EGNSS Centre of Excellence

Eindrapport IKUS-II

Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie

21 november 2022

CGI s[&]t nlr

Inhoudsopgave

Managementsamenvatting

Global Navigation Satellite Systems (GNSS); we vertrouwen er allemaal op. Niemand heeft nog een stratenboek; het bepalen van de beste route naar onze vakantiebestemming is nu simpel het intoetsen van het adres van onze favoriete camping in ons navigatiesysteem. Maar ook wetenschappers die op zoek zijn naar een zwart gat gebruiken GNSS; radarsystemen die het scheepvaartverkeer in goede banen leiden ook; en financiële instellingen vertrouwen op de tijdinformatie van GNSS voor hun internationale transacties.

De maatschappij vertrouwt op goedwerkende GNSS, zoals het Amerikaanse GPS en het Europese Galileo. Met behulp van GNSS kan Plaatsbepaling, Navigatie en Tijdsbepaling (PNT) gemakkelijk gedaan worden, zodoende is GNSS in veel systemen toegepast; ook binnen de vitale processen[1]. Al ruim twee decennia geleden[2] realiseerde men zich in de Verenigde Staten (VS) dat de afhankelijkheid van GNSS aan het toenemen is. Bij een verstoring in een GNSS kunnen er geen garanties gegeven worden dat de juiste uitvoering van processen voor allerlei basisvoorzieningen gewaarborgd is. In het Verenigd Koninkrijk[3] is de economische impact bepaald voor de situatie dat men voor vijf dagen niet over GNSS kan beschikken; deze schade kan tot 5.2 miljard Britse ponden (tegen de huidige koers bijna 6 miljard euro) oplopen.

GNSS-storingen komen regelmatig voor

Recent heeft zich op de luchthaven van Denver in de VS een verstoring van GNSS voorgedaan. Het volgende enigszins cryptische bericht werd op 21 januari 2022 uitgezonden naar al het vliegverkeer.

Notice To Airmen 21 January 2022

NAV GPS UNREL(INCLUDING WAAS, GBAS, AND ADS-B) MAY NOT BE AVBL WI A 50NM RADIUS CENTERED AT 394900N1044000W OR ALL QUADRANTS OF THE DEN VOR SFC-FL400. 22 JAN 05:00 2022 UNTIL 01 FEB 05:00 2022. CREATED: 22 JAN 05:33 2022

Binnen een straal van 75 km vanaf de luchthaven van Denver is het GNSS signaal onbetrouwbaar voor het vliegverkeer. (Ter vergelijking, dit gebied is ongeveer 40% van de totale oppervlakte van Nederland). Het vliegverkeer had hier op verschillende manieren last van, inclusief dat een *collision avoidance system* verkeerde informatie aan de piloot gaf. Niet alleen het vliegverkeer had last van deze storing, maar ook mobiele telefoonproviders. Zij konden naar een back-up systeem overschakelen, andere vormen van communicatie konden dat niet en hadden last van deze storing. Dit event duurde 33.5 uur en de precieze oorzaak wordt nog onderzocht.

Dit voorbeeld geeft aan dat GNSS-storingen in de praktijk voorkomen, dat deze verstoringen ook niet zomaar worden opgelost en dat er omvangrijke keteneffecten kunnen ontstaan. Het voorbeeld laat ook zien dat men zich wel degelijk kan wapenen tegen dit soort verstoringen.

[1] Bepaalde processen zijn zo essentieel voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen vormen de Nederlandse vitale infrastructuur. Drinkwater, elektriciteit, toegang tot internet en betalingsverkeer zijn voorbeelden van vitale processen.

[2] John A. Volpe National Transportation Systems Center. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. 29 Aug 01.

[3] Government office for Science, Satellite-derived Time and Position, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/676675/satellite-derived-time-and-position-blackett-review.pdf

De situatie in Nederland

Het ministerie van Infrastructuur en Waterstaat (IenW) is nationaal beleidsverantwoordelijk voor plaats- en tijdbepaling met behulp van GNSS dat is aangemerkt als vitaal B proces en heeft opdracht gegeven voor de uitvoering van het project Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie II (IKUS-II). IKUS-II is een vervolg op de studie IKUS-I uit 2016 en heeft als doel om inzicht te krijgen in de weerbaarheid tegen verstoringen van PNT middels GNSS in Nederland. IKUS-II is uitgevoerd in samenwerking met het Netherlands Space Office, European Space Agency en de begeleidingsgroep met afgevaardigde vanuit diverse ministeries, waarvan ook het IenW. De studie is uitgevoerd door het EGNSS Centre of Excellence. IKUS-II is uitgevoerd met behulp van een vragenlijst en verdiepende risicoanalyses op organisatieniveau. Voorafgaand aan de daadwerkelijke studie zijn er masterclasses en een awareness campagne georganiseerd met als doel het kennisniveau onder de deelnemende organisaties te verhogen om daarmee de betrouwbaarheid van het onderzoek te vergroten. De masterclasses en de awareness campagne waren een nieuw onderdeel in vergelijking met IKUS-I. Daarnaast heeft IKUS-II ook verdieping aangebracht ten opzichte van IKUS-I en is de scope verbreed. In IKUS-II is namelijk zowel naar de vitale processen als naar de niet vitale processen gekeken. In IKUS-II staan vier onderzoeksthema's centraal: kennis en bewustzijn, gebruik, weerbaarheid en keteneffecten.

Het beeld dat uit deze studie komt is zeker niet alleen positief. Er zijn zeker goede voorbeelden van organisaties te geven waar risico's in beeld zijn en bewust beoordeeld worden. Echter, een organisatie waar nagedacht wordt over de consequenties van een GNSS-verstoring op de eigen systemen, waar alternatieven voor GNSS aanwezig zijn en waar de weerbaarheid voor GNSS-verstoringen onderdeel is van het beleid, is eerder een uitzondering dan regel.

Bovenstaande geeft een zeer zorgelijk beeld van de potentiële risico's die breed in de verschillende gebruikerssectoren kunnen bestaan. Deze situatie vergt naar onze mening urgente aandacht van het beleidsverantwoordelijke ministerie en gerelateerde overheden. Onderstaande conclusies dienen dan ook in dit licht te worden gelezen.

De belangrijkste conclusies van deze studie zijn:

Kennis en bewustzijn

- Het kennisniveau ten aanzien van bewust gebruik en weerbaarheid verschilt sterk per organisatie. Over het algemeen kan geconcludeerd worden dat er nog veel ruimte voor verbetering is op het gebied van kennis en bewustzijn;
- Kwetsbaarheidsstudies zoals IKUS-I en IKUS-II zorgen voor een bewustwordingsimpuls aangaande het gebruik van PNT middels GNSS maar leiden niet perse tot het duurzaam vergroten van de weerbaarheid;
- De grote belangstelling voor de masterclasses toont aan dat er veel behoefte is aan het verkrijgen van kennis en kunde over PNT middels GNSS.

Gebruik

- PNT middels GNSS wordt veelvuldig (al dan niet bewust) ingezet in diverse (vitale) processen van de onderzochte sectoren. Zowel van positie- als van tijdsbepaling wordt gebruik gemaakt. Uitval kan zodoende verstrekkende gevolgen hebben voor de Nederlandse maatschappij[4];
- Zes, waarvan vier vitale sectoren, van de 24 aangeschreven sectoren hebben niet of nauwelijks geparticipeerd in IKUS-II waaronder ook sectoren die in IKUS-I, alsook in internationale kwetsbaarheden studies als kwetsbaar worden aangemerkt.

Weerbaarheid

- Er is geen actief beleid binnen sectoren en organisaties dat zich richt op het vergroten van de weerbaarheid van processen en systemen welke afhankelijk zijn van PNT middels GNSS. De verantwoordelijkheid voor het gebruik van PNT middels GNSS is daarnaast bij de meeste organisaties niet duidelijk belegd;

[4] De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft plaats- en tijdsbepaling door middel van GNSS in Nederland als een categorie B vitaal proces geïdentificeerd. In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de drie impactcriteria voor categorie B raakt:

- Economische gevolgen: > ca. 5 miljard euro schade of ca. 1,0% daling reëel inkomen
- Fysieke gevolgen: meer dan 1.000 personen dood, ernstig gewond of chronisch ziek
- Sociaal maatschappelijke gevolgen: meer dan 100.000 personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen

- Gericht risicomanagement met betrekking tot PNT middels GNSS ontbreekt bij veel organisaties en zodoende worden geen acties ondernomen en/of geïdentificeerd om risico's te reduceren zoals het onderzoeken van alternatieven voor GNSS. Het inrichten van risicomanagement en het onderzoeken van alternatieven was een aanbeveling vanuit IKUS-I, waar dus onvoldoende invulling aan gegeven is;
- Kennis over de (technische) weerbaarheid is zeer beperkt.

Keteneffecten

- Internationale onderzoeken en het gegeven dat PNT middels GNSS in Nederland een vitaal proces is, tonen aan dat er bij GNSS-verstoringen maatschappij ontwrichtende keteneffecten kunnen ontstaan. Deze studie schetst een beeld van de te verwachte keteneffecten als gevolg van GNSS-verstoringen in Nederland. Een diepgaande analyse was geen onderdeel van dit onderzoek.

Dit rapport bevat de volgende aanbevelingen om inzicht in, en de actuele toestand van, de weerbaarheid binnen de verschillende sectoren in Nederland sterk te verbeteren.

Aanbevelingen IKUS-II:

Kennis en bewustzijn

- Zorg als overheid dat het kennisniveau op peil komt en blijft door het laagdrempelig, centraal en continu beschikbaar te stellen van actuele kennis en kunde.

Gebruik

- Ga als beleidsverantwoordelijk ministerie in gesprek met sectoren over het verantwoord gebruik van GNSS, vooral met de sectoren die niet hebben deelgenomen aan IKUS-II;
- Identificeer als PNT-gebruikende organisatie in welke processen er gebruik wordt gemaakt van GNSS en of dit tijd- en/of plaatsbepaling betreft.

Weerbaarheid

- Beleg als PNT-gebruikende organisatie de verantwoordelijkheid voor het gebruik van GNSS duidelijk en centraal binnen de organisatie.
- Neem het gebruik van PNT middels GNSS op in bestaande crisis en- risicomanagement processen op zowel nationaal niveau (zoals de rijksbrede risicoanalyse) als op organisatieniveau.
- Vergroot als PNT-gebruikende organisatie de (technische) weerbaarheid tegen verstoring van PNT middels GNSS.
- Stel als PNT-gebruikende organisatie beleid op voor het gebruik van GNSS binnen de organisatie.
- Onderzoek als overheid op welk niveau kaders nodig zijn om te helpen bij weerbaarheids- en continuïteitsmaatregelen voor sectoren[5].

Keteneffecten

- Doe als overheid in samenwerking met PNT-gebruikende organisaties nader onderzoek om de keteneffecten als gevolg van GNSS-verstoringen in Nederland beter in beeld te krijgen.

De aanbevelingen van IKUS-I hebben niet geleid tot een zichtbare vergroting van het bewustzijn en de weerbaarheid. Dit is zorgwekkend, temeer daar de afhankelijkheid zoals is vastgesteld alleen maar toeneemt en eerder GNSS al geïdentificeerd is als een categorie B vitaal proces. Dit vraagt een nog (pro)actievere rol van het ministerie van IenW vanuit haar nationale beleidsverantwoordelijkheid voor plaats- en tijdsbepaling met behulp van GNSS.

[5] Deze kaders zorgen voor uniformiteit en geeft richting aan maatregelen die organisaties zelf kunnen oppakken om een gewenst (minimaal) niveau van weerbaarheid te realiseren. Dergelijke kaders zorgen ook voor de afbakening en begrenzing tussen overheden en organisaties om dit in goed samenspel op te pakken.

Management summary

Global Navigation Satellite Systems (GNSS); we all rely on it. No one is using maps anymore; planning the best route to our holiday destination is now simply entering the address of our favorite campsite into our navigation system. But also scientists searching for a black hole use GNSS; radar systems used for vessel traffic management and financial institutions rely on GNSS timing information for their international transactions.

Without realizing society relies on operational Global Navigation Satellite Systems (GNSS), such as the American GPS and the European Galileo. Using GNSS Positioning, Navigation and Timing (PNT) can be done easily, as a result GNSS has been applied in many systems including in vital processes[6]. Already more than two decades ago[7] people realised in the United States (US) that dependence on GNSS is increasing. In the event of a disruption in a GNSS the proper execution of processes for all kinds of basic services is not guaranteed. In the United Kingdom[8] the economic impact of malfunctioning of GNSS for five days has been valued to £5.2 billion (at the current exchange rate nearly €6 billion).

GNSS failures occur regularly

Recently, GNSS outage occurred at Denver airport in the US. The following somewhat cryptic message was broadcasted to all air traffic on 21 January 2022.

Notice To Airmen 21 January 2022

NAV GPS UNREL(INCLUDING WAAS, GBAS, AND ADS-B) MAY NOT BE AVBL WI A 50NM RADIUS CENTERED AT 394900N1044000W OR ALL QUADRANTS OF THE DEN VOR SFC-FL400. 22 JAN 05:00 2022 UNTIL 01 FEB 05:00 2022. CREATED: 22 JAN 05:33 2022

Within a radius of 75 km from Denver airport, the GNSS signal is unreliable for air traffic. (By comparison, this area covers about 40 percent of the total of the Netherlands). Air traffic was affected in several ways, including that one *collision avoidance system* provided wrong information to pilots. Not only did air traffic suffer from this failure, but also mobile phone providers. They could switch to a back-up system but other forms of communication could not and suffered from this failure. This event lasted 33.5 hours and the exact cause is still under investigation.

This example shows that GNSS disruptions do occur and that these disruptions are also not simply resolved and extensive chain effects can occur. The example also shows that it is possible to guard against such disruptions.

The situation in the Netherlands

The Ministry of Infrastructure and Water Management (IenW) is in the Netherlands responsible for positioning and timing using GNSS which has been identified as a vital B process and has launched the Vulnerability Assessment on failure of Satellite Navigation (IKUS-II) project. IKUS-II is a

[6] Certain processes are so essential to Dutch society that failure or disruption leads to serious social disruption and threatens national security. These processes constitute the Netherlands' vital infrastructure. Drinking water, electricity, internet access and payments are examples of vital processes.

[7] John A. Volpe National Transportation Systems Center. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. 29 Aug 01.

[8] Government office for Science, Satellite-derived Time and Position, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/676675/satellite-derived-time-and-position-blackett-review.pdf

follow-up to the 2016 study IKUS-I and aims to create insight into the resilience to PNT disruptions via GNSS in the Netherlands. IKUS-II was carried out in collaboration with the Netherlands Space Office, European Space Agency and the guidance group with representatives from various ministries, including the IenW. The study was carried out by the EGNSS Centre of Excellence. IKUS-II was performed using a questionnaire and in-depth risk analyses at organisational level. Prior to the actual study, GNSS master classes and an awareness campaign were organised with the aim of raising the level of knowledge among participating organisations to increase the reliability of the study. The master classes and awareness campaign were new developed tools in comparison to IKUS-I. In addition, IKUS-II added more detail compared to IKUS-I and broadened the scope with respect to invited organisations. IKUS-II focused on both vital processes and non-vital processes. IKUS-II identified four research topics: knowledge and awareness, use, resilience and chain effects.

The final conclusions from this study are certainly not only positive. There are certainly good examples of organisations where risks are known and consciously assessed. Ideally an organisation considers the consequences of GNSS interference on its own systems, has prepared for alternatives to GNSS and made resilience to GNSS interference part of their policy and decision making. Unfortunately this situation is more the exception than the rule.

The above paints a very worrying picture of the potential risks that may exist broadly across user sectors. In our view, this situation requires urgent attention from the policy-making ministry and related authorities. The conclusions below should therefore be read in this light.

The main conclusions of this study are:

Knowledge and awareness

- The level of knowledge with regard to conscious use and resilience varies greatly between organisations. In general, it can be concluded that there is still much room for improvement in terms of knowledge and awareness;
- Vulnerability studies such as IKUS-I and IKUS-II help to raise awareness of the use of PNT through GNSS but do not necessarily lead to a sustainable increase in resilience;
- The high participation rate in the master classes demonstrated that there is a great interest in getting knowledge and skills about PNT through GNSS.

Usage

- PNT through GNSS is frequently used (consciously or unconsciously) in various (vital) processes of the sectors in scope. Both positioning and timing are used. Failure could therefore have far-reaching consequences for Dutch society[9];
- Six, including four vital sectors, of the 24 sectors contacted did not participate in IKUS-II or participated limited including sectors identified as vulnerable in IKUS-I, as well as in international vulnerability studies.

Resilience

- There is no active policy within sectors and organisations aimed at increasing the resilience of processes and systems that depend on PNT through GNSS. Furthermore, the responsibility for the use of PNT through GNSS is not clearly assigned in most organisations;
- Targeted risk management with regard to PNT through GNSS is lacking in many organisations and thus no actions are taken and/or identified to reduce risks, such as investigating alternatives to GNSS. Setting up risk management and investigating alternatives was a recommendation from IKUS-I, which has therefore not been adequately implemented;
- Knowledge of (technical) resilience is very limited.

[9] The National Coordinator for Counterterrorism and Security (NCTV) has identified location and timing through GNSS in the Netherlands as a category B vital process. This category includes infrastructure that, in the event of disruption, degradation or failure, hits the lower limits of at least one of the three impact criteria for category B:

- Economic impact: > ca. €5 billion damage or ca. 1.0% drop in real income
- Physical consequences: more than 1,000 people dead, seriously injured or chronically ill
- Social impact: more than 100,000 people experience emotional distress or severe social survival problems

Chain effects
- International studies and the fact that PNT through GNSS is a vital process in the Netherlands show that society can experience disruptive chain effects in case of GNSS disruptions. This study paints a picture of the expected chain effects due to GNSS disruptions in the Netherlands. In-depth analysis was not part of this study.

This report contains the following recommendations to greatly improve the understanding and current state of resilience within different sectors in the Netherlands.

Recommendations IKUS-II:

Knowledge and awareness
- As a government, ensure that the level of knowledge is and remains up to standard by making up-to-date knowledge and expertise centrally available, easily accessible and continuously available.

Usage
- As the responsible ministry, engage with sectors on the responsible use of GNSS, especially those that have not participated in IKUS-II;
- As a PNT-using organisation, identify in which processes GNSS is used and whether this involves time and/or positioning.

Resilience
- As a PNT-using organisation, delegate responsibility for GNSS use clearly and centrally within the organization;
- Incorporate the use of PNT through GNSS into existing crisis and risk management processes at both national level (such as the government-wide risk analysis) and organisational level;
- As a PNT-using organisation, increase (technical) resilience to PNT disruption failures through GNSS;
- As a PNT-using organisation, set policies for the use of GNSS;
- As a government, examine at what level frameworks are needed to help with resilience and continuity measures for sectors[10].

Chain effects
- As a government, conduct further research in cooperation with PNT-using organisations to better understand the chain effects due to GNSS interference in the Netherlands.

IKUS-I's recommendations have not resulted in a visible increase in awareness and resilience. This is worrisome, especially as dependency as identified is only increasing and GNSS has previously been identified as a category B vital process. This calls for an even more (pro)active role of the Ministry of IenW from its national policy responsibility for place and time determination using GNSS.

[10] These frameworks ensure uniformity and give direction to measures that organisations themselves can take to achieve a desired (minimum) level of resilience. Such frameworks also provide demarcation and boundaries between governments and organisations to address this in good cooperation.

Hoofdstuk 1 Introductie

1.1 Aanleiding en doel

GNSS staat voor Global Navigation Satellite System en is een verzamelterm voor verschillende satellietnavigatiesystemen. Het doel van GNSS is om gebruikers altijd en overal ter wereld te kunnen voorzien van gedetailleerde positie- en tijdinformatie. Diverse sectoren maken gebruik van GNSS. De transportsector bijvoorbeeld voor navigatie en de energiesector voor het koppelen van energienetwerken met behulp van tijdsynchronisatie. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft plaats- en tijdsbepaling door middel van GNSS in Nederland als een categorie B vitaal proces geïdentificeerd. Dit betekent dat verstoring van het proces kan leiden tot ernstige maatschappelijke ontwrichting[11] en een bedreiging voor de nationale veiligheid vormt.

Omdat verstoring van GNSS ernstige gevolgen kan hebben, is het van belang te weten wat de kwetsbaarheden van plaats-, navigatie en tijdbepaling (PNT) door middel van GNSS zijn. Dan kan worden afgewogen welke kwetsbaarheden er gemitigeerd moeten worden en welke risico's acceptabel zijn. In Nederland is het ministerie van Infrastructuur en Waterstaat (IenW) beleidsverantwoordelijk voor het vitale proces PNT door middel van GNSS. Vanuit deze verantwoordelijkheid inventariseert het ministerie de kwetsbaarheden in het gebruik van GNSS voor verschillende sectoren. Het doel hiervan is om inzicht te krijgen in de weerbaarheid van sectoren tegen verstoring van PNT middels GNSS.

Met het onderzoek Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie IKUS-I[12] is in 2016 een analyse gemaakt van de afhankelijkheden en kwetsbaarheden van GNSS voor de vitale sectoren. Het onderzoek heeft geleid tot meer bewustzijn over de kwetsbaarheden en richting gegeven aan te nemen maatregelen in de vitale sectoren. De behoefte aan een vervolgonderzoek naar de keteneffecten van GNSS-verstoring is onder andere[13] voortgekomen uit dit onderzoek. Ook kregen de sectoren het advies om het scenario van GNSS-verstoring op te nemen als terugkerend onderwerp binnen de sectorspecifieke (continuïteits-)overleggen en in de risicoanalyses en crisismanagementmaatregelen van organisaties. Ten slotte was er het advies om alternatieven voor PNT middels GNSS te onderzoeken.

IKUS-I concludeerde al dat het gebruik van GNSS blijft toenemen. Het marktrapport uit 2022 van The European Union Agency for the Space Programme (EUSPA)[14] bevestigt dit beeld. De integratie van PNT door middel van GNSS in processen en systemen is op een dusdanige schaal dat veel gebruikers zich niet eens realiseren dat ze een gebruiker zijn. Het is dus van belang om een actueel inzicht in het gebruik en de eventuele risico's ervan te hebben. Dit geldt in het bijzonder voor de vitale sectoren.

IenW besloot in 2021 tot een vervolgonderzoek, IKUS-II. Naast het creëren van meer bewustzijn en het verkrijgen van inzicht in keteneffecten als gevolg van verstoring van GNSS, ligt in dit onderzoek de nadruk op kennisoverdracht. Om de (uitkomsten van) vergelijkbare onderzoeken in Europees verband mee te kunnen nemen is dit onderzoek uitgevoerd binnen het NAVISP[15] programma van de European Space Agency (ESA).

---

[11] In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de drie impactcriteria voor categorie B raakt:
- Economische gevolgen: > ca. 5 miljard euro schade of ca. 1,0% daling reëel inkomen
- Fysieke gevolgen: meer dan 1.000 personen dood, ernstig gewond of chronisch ziek
- Sociaal maatschappelijke gevolgen: meer dan 100.000 personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen

[12] IKUS Inventarisatie Kwetsbaarheid Uitval Satellietnavigatie, 11-03-2016
https://www.eerstekamer.nl/overig/20121113/bijlage_9_synthese_rapport/document3/f=/vkh7ivszouz2.pdf

[13] Daarnaast ook in de Risico Inventarisatie Cyber Security IenW totaalrapportage, maart 2020

[14] EUSPA EO and GNSS Market Report 2022/Issue 1

[15] ESA Navigation and Innovation Support Programme

In de uitvoering van het project heeft het Centre of Excellence voor Europese GNSS (EGNSS CoE)[16] de opdracht gekregen om:

1. Onderzoek te doen naar het gebruik van PNT middels GNSS in Nederland om de kwetsbaarheden in beeld te brengen en het inzicht in de risico's te vergroten.
2. Een toolbox van onderzoeksinstrumenten te ontwikkelen, waarmee de kwetsbaarheid van het gebruik van GNSS kan worden beoordeeld. Deze maakt het mogelijk de gehele studie in de toekomst consistent te herhalen.

Het project is uitgevoerd langs vier onderzoeksthema's met bijbehorende onderzoeksvragen:

- Kennis en bewustzijn: hoeveel kennis heeft een organisatie over GNSS(-verstoringen) en is een organisatie zich bewust van bijbehorende kwetsbaarheden en risico's?
- Gebruik: hoe gebruikt een organisatie GNSS en welke processen zijn ervan afhankelijk?
- Weerbaarheid: hoe kijken organisaties naar weerbaarheid tegen GNSS-verstoringen en hoe weerbaar zijn organisaties?
- Keteneffecten: als er GNSS-verstoringen optreden, welke keteneffecten kunnen dan verwacht worden en wanneer treden ze op?

Het onderzoek is geïnitieerd vanuit het Nederlandse belang en richt zich zodoende ook op de Nederlandse situatie.

1.2 Onderzoeksopzet

De eerste stap in het onderzoek was het identificeren van potentiële GNSS-gebruikers in zowel de vitale als de niet-vitale sectoren die konden worden aangeschreven om aan dit onderzoek deel te nemen. De gebruikers uit de niet-vitale sectoren zijn geïdentificeerd op basis van deskresearch naar toepassingen van GNSS. Een overzicht van organisaties die aangeschreven zijn om deel te nemen aan de kwetsbaarheidsbeoordeling is opgenomen in Bijlage A. De organisaties zijn uitgenodigd om te reageren op een online vragenlijst (zie Bijlage C) om inzicht te krijgen in kennis en bewustzijn, gebruik en weerbaarheid van een organisatie en inzicht te krijgen in keteneffecten als gevolg van GNSS-verstoringen. Daarnaast zijn de organisaties ook uitgenodigd om een masterclass over GNSS bij te wonen met als doel het kennisniveau binnen de organisatie te verhogen zodat het gebruik, de weerbaarheid en potentiële keteneffecten beter beoordeeld kunnen worden. Organisaties die dat desgevraagd in de online vragenlijst of masterclass hebben aangegeven zijn vervolgens uitgenodigd tot een meer diepgaande risicoanalyse van het gebruik van PNT middels GNSS binnen de specifieke organisatie. De verdiepende risicoanalyse is uitgevoerd voor vier organisaties conform de Information Risk Assessment Methodology (IRAM2) methode. Om het gebruik van PNT middels GNSS en de bijbehorende risico's goed bij de organisaties onder de aandacht te brengen is er een awareness campagne opgezet. De awareness campagne diende daarnaast ook om het bewustzijn over verschillende soorten GNSS-storingen te vergroten. Deze bestond uit nieuwsbrieven en een demonstratie en impliciet waren ook de masterclasses hier onderdeel van. Tenslotte zijn de vragenlijst en de masterclass vastgelegd in een toolbox om de uitvoering van toekomstige kwetsbaarhedenanalyses te vergemakkelijken.

Een door het ministerie van Infrastructuur en Waterstaat samengestelde commissie begeleidde het onderzoek (zie Bijlage J). Deze begeleidingscommissie speelde een actieve rol in:

- het beoordelen van de onderzoeksopzet;
- de identificatie en het verzamelen van deelnemende organisaties;
- deelname aan de masterclass en discussie;
- het reflecteren op de tussenresultaten, conclusies en aanbevelingen.

In het onderzoek is ook nadrukkelijk naar de ontwikkelingen in andere landen gekeken. Omdat het onderzoek is uitgevoerd binnen het NAVISP van ESA, is er via deze route ook contact gelegd met organisaties die betrokken zijn bij vergelijkbare studies in andere ESA-lidstaten.

1.3 Vertrouwelijkheid

De informatie die de basis vormt voor het onderwerp van deze studie geeft inzicht in potentiële kwetsbaarheden en afhankelijkheden. De informatie kan voor deelnemende organisaties leiden tot

[16] Het EGNSS CoE is een samenwerking tussen organisaties met specialistische kennis over GNSS: CGI, S[&]T en het Nederlands Lucht- en Ruimtevaartcentrum (NLR). https://gnss-coe.eu

een commercieel of veiligheidsrisico. Daarom is er in deze studie extra aandacht besteed aan het thema vertrouwelijkheid. Er is een black box-principe gehanteerd, waarbij detailinformatie alleen bekend was bij de onderzoekers. De data is niet herleidbaar en enkel op een hoger abstractieniveau gedeeld met het ministerie van IenW (en andere betrokken vakdepartementen en deelnemers). De gemeenschappelijke thema's en inzichten van het kwetsbaarheidsonderzoek worden in dit rapport gepresenteerd.

1.4 EGNSS Centre of Excellence

Het EGNSS CoE is een samenwerking tussen organisaties met specialistische kennis over GNSS: CGI[17], S[&]T[18] en het Nederlands Lucht- en Ruimtevaartcentrum (NLR). Het CoE werkt samen met Netherlands Space Office (NSO), het ministerie van IenW, ESA, EUSPA en NL Space Campus. Het CoE adviseert organisaties over het veilig implementeren en gebruiken van GNSS-signalen. Het CoE kan een risicobeoordeling uitvoeren over gekozen GNSS-implementaties en kan adviseren over mitigerende maatregelen voor GNSS-kwetsbaarheden.

1.5 Leeswijzer

Dit document begint met een introductie van het onderzoek en de onderzoeksopzet en achtergrondinformatie omtrent GNSS en het gebruik van GNSS respectievelijk de hoofdstukken 1 en 2. Hoofdstuk 3 geeft een overzicht van GNSS-storingen en beschrijft scenario's die als referentie dienen voor de kwetsbaarheidsbeoordeling. De resultaten daarvan worden in hoofdstuk 4 gepresenteerd. Hoofdstuk 5 betreft de conclusie van dit onderzoek; in hoofdstuk 6 worden een aantal aanbevelingen gedaan. Dit rapport bevat de volgende bijlagen:

A. Aangeschreven organisaties
B. Vragenlijst, masterclass en awareness campagne
C. Questionnaire
D. Methode kwetsbaarheden analyse
E. Kwetsbaarheden per sector (vertrouwelijk)
F. Technische diepgang GNSS
G. Toelichting dreigingen betreffende GNSS gebruik
H. Potentieel kwetsbare systemen zoals genoemd in de deep-dives
I. Voorbeelden mitigerende maatregelen
J. Samenstelling van de interdepartementale begeleidingsgroep
K. Begrippen en afkortingen
L. Nieuwsbrieven

[17] www.cgi.com

[18] www.stcorp.nl

Hoofdstuk 2 Achtergrondinformatie GNSS

Dit hoofdstuk beschrijft op hoofdlijnen de technologie en het gebruik hiervan en gaat in op ontwikkelingen in andere landen met betrekking tot weerbaarheid en keteneffecten bij verstoringen van PNT middels GNSS. Deze achtergrondinformatie geeft de noodzakelijke context en kennis om vervolgens op de dreigingen en de kwetsbaarheden in te kunnen gaan.

2.1 Verantwoordelijkheden

Het ministerie van IenW heeft nationale beleidsverantwoordelijkheid voor PNT middels GNSS. Dit laatste is in de nationale systematiek van vitale infrastructuur geïdentificeerd als een categorie B vitaal proces. Daarnaast bereidt IenW momenteel het beheer en gebruik voor van de Galileo-dienst *Public Regulated Service (PRS).* PRS is een een robuuste dienst voor tijd- en plaatsbepaling. PRS biedt bescherming tegen verstoringen (jamming) of manipulatie (spoofing). Om het beheer en gebruik van PRS in lidstaten van de EU mogelijk te maken moeten lidstaten een *Competent PRS Authority (CPA)* inrichten. De CPA voor Nederland is belegd bij IenW. Op basis van de Telecommunicatiewet houdt het Agentschap Telecom (AT) toezicht op het gebruik van het frequentiespectrum en heeft het een meldpunt voor radio-interferentie. Het AT is een onderdeel van het ministerie van Economische Zaken en Klimaat (EZK).

Het ministerie van EZK heeft een coördinerende verantwoordelijkheid voor het ruimtevaartbeleid dat door een aantal ministeries (onder andere IenW) wordt gemaakt en wordt uitgevoerd door het NSO.

De sectoren zijn zelf verantwoordelijk voor het identificeren, beoordelen en mitigeren van kwetsbaarheden.

2.2 GNSS

GNSS staat voor Global Navigation Satellite System en is een verzamelterm voor de verschillende satellietconstellaties en bijbehorende grondinfrastructuur waarvan de signalen wereldwijd te ontvangen zijn. Het doel van GNSS is om gebruikers altijd en overal ter wereld te kunnen voorzien van gedetailleerde positie- en tijdinformatie (PNT-informatie). Op dit moment zijn er meerdere GNSS'en operationeel, waarvan het oudste en bekendste GPS is. GPS werd als eerste constellatie geïntroduceerd en is eigendom van de VS, die het ook beheren. Niet lang na de introductie van GPS kwam Rusland met een eigen systeem genaamd GLONASS. Meer recent hebben ook Europa (Galileo) en China (BeiDou) hun eigen systemen geïntroduceerd. Naast de vier genoemde Global Navigation Satellite Systems bestaan er een aantal regionale systemen. Zo heeft India NavIc en beschikt Japan over QZSS, een systeem dat geostationaire satellieten[19] gebruikt voor de informatieverstrekking naar de gebruiker. Zoals aangegeven wordt GNSS ook gebruikt om een nauwkeurig tijdsignaal aan applicaties te leveren. Voor deze toepassing worden vaak gespecialiseerde Timing-ontvangers gebruikt. Deze Timing-ontvangers leveren zowel een nauwkeurig tijdsindicatie als een stabiel frequentiesignaal. Het GNSS-signaal wordt door de Timing-ontvanger gebruikt om de stabiliteit van een lokale oscillator binnen zeer strenge grenzen te houden. Dit betekent dat als het GNSS-signaal wegvalt, de stabiliteit van de klok niet direct teniet is gedaan maar dat deze terugvalt naar die van de lokale oscillator. De politieke behoefte om voor PNT-informatie onafhankelijk te zijn van andere landen of mogendheden motiveert in de basis de wens om over eigen satellietnavigatiesystemen te beschikken. Maar ook de mogelijkheid om meerdere constellaties te gebruiken biedt voordelen. Het komt namelijk de robuustheid van een applicatie die PNT-informatie gebruikt ten goede. Bovendien introduceert het robuustheid tegen het falen van één van de constellaties. Niet elke ontvanger kan gebruikmaken van meerdere constellaties. Dit hangt af van de mate van beschikbaarheid van het signaal op de locatie en de specificaties van de ontvanger.

[19] Een geostationaire satelliet is een satelliet in een circulaire baan boven de aarde, waarbij de satelliet met dezelfde hoeksnelheid om de aarde draait als de aarde om haar eigen as. Hierdoor lijkt de satelliet op dezelfde positie (stationair) boven de gebruiker te staan.

Vrijwel alle GNSS-ontvangers maken gebruik van de open signalen die de verschillende GNSS aanbieden. Naast de open signalen bestaan er ook speciale signalen met verdergaande prestatiegaranties. Eén van de bekendste is het militaire M-code-signaal van GPS, dat garanties biedt tegen bepaalde verstoringen. Dit M-code-signaal is echter alleen beschikbaar voor een zeer beperkte, militaire doelgroep. Met de komst van het Europese Galileo-systeem is een dergelijk signaal behalve voor militaire organisaties ook voor een Europese, door een autoriteit goedgekeurde, civiele organisatie beschikbaar[20]. Deze gereguleerde Europese service wordt Public Regulated Service (PRS) genoemd.

In Bijlage F is meer informatie te vinden over onder andere de verschillende elementen van een GNSS-constellatie, de gebruikte signalen, het bepalen van de positie-snelheid-tijdoplossing, en het gebruik van augmentatie systemen.

2.3 GNSS-kwetsbaarheden

Zoals beschreven in Hoofdstuk 1 is dit onderzoek uitgevoerd langs vier onderzoeksthema's: kennis en bewustzijn, gebruik, weerbaarheid en keteneffecten. Deze paragraaf gaat in op relevante literatuur over deze vier thema's.

2.3.1 Kennis en bewustzijn

In Nederland is in 2016 de eerste IKUS studie uitgevoerd waaruit geconcludeerd werd dat de kennis over GNSS en bijbehorende risico's beperkt is onder PNT-gebruikende organisaties. Het NLR heeft in 2019 een studie[21] uitgevoerd over de gevaren van spoofing (dit leidt tot GNSS-verstoringen, zie verdere uitleg hierover in Hoofdstuk 3). Het NLR rapport concludeert ook dat er weinig bewustzijn is over het gebruik en kwetsbaarheid van GNSS onder PNT-gebruikende organisaties.

Hoewel PNT middels GNSS geïdentificeerd is als een vitaal B proces worden in de Rijksbrede risicoanalyse (RbRa) nationale veiligheid 2022 van het Analistennetwerk Nationale Veiligheid[22] GNSS-verstoringen niet genoemd als dreiging met een mogelijk ontwrichtend effect op het Koninkrijk der Nederlanden[23]. Terwijl in bijvoorbeeld Amerikaanse of Britse literatuur wordt wel wordt gesproken over een mogelijk ontwrichtend effect van GNSS-verstoringen. In Amerika lijkt de dreiging van GNSS-kwetsbaarheden wel onderkend maar in een Britse kwetsbaarheden studie[24] wordt daarentegen benoemd dat het bewustzijn over afhankelijkheden van GNSS ook laag is.

In de themarapportage bedreiging vitale infrastructuur 2022 behorend bij de RbRa is wel het scenario ruimteweer meegenomen waarbij wordt beschreven dat dit kan leiden tot GNSS-verstoringen wat vervolgens kan leiden tot verstoringen in de luchtvaart. In de beschouwing wordt aangegeven dat er meerdere studies zijn gedaan naar de mogelijke gevolgen van satellietuitval, maar dat de daadwerkelijke impact op het functioneren van vitale processen (en de Nederlandse maatschappij in het algemeen) veelal onzeker blijft. De Britse kwetsbaarheden studie merkt ook op dat het scenario van GNSS-verstoringen op zichzelf opgenomen zou moeten worden in de Britse Nationale Risicobeoordeling en niet enkel als een gevolg van ruimteweer.

Er is dus nog weinig kennis en bewustzijn over de mogelijke gevolgen van GNSS-verstoringen. Het gebruik van GNSS is veelal onzichtbaar omdat de functionaliteit vaak standaard in apparatuur aanwezig is en ook diep in deze apparatuur verborgen kan zitten. Daarnaast vereist de beoordeling van kwetsbaarheden en bijbehorende kwetsbaarheden specialistische kennis die schaars is.

---

[20] Decision 2011/1104 - Decision 1104/2011/EU on the rules for access to the public regulated service provided by the global navigation satellite system established under the Galileo programme

[21] GNSS spoofing revised edition NLR-CR-2019-001-PT-1-RevEd-1| June 2019

[22] https://www.nctv.nl/documenten/publicaties/2022/09/26/rijksbrede-risicoanalyse-nationale-veiligheid

[23] ANV (2022), Rijksbrede Risicoanalyse Nationale Veiligheid, Analistennetwerk Nationale Veiligheid.

[24] Government office for Science, Satellite-derived Time and Position, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/676675/satellite-derived-time-and-position-blackett-review.pdf

2.4 GNSS-gebruik en toepassingen

IKUS-I heeft geconstateerd dat het gebruik van GNSS verschilt per sector en per organisatie binnen de sectoren. Organisaties gebruik PNT middels GNSS voor zowel plaats- en tijdsbepaling. Tijdsbepaling middels GNSS is de meest gebruikte vorm van tijdsbepaling in de vitale infrastructuur en tegelijkertijd ook de meest kwetsbare vorm van tijdsbepaling[25].

GNSS is uitgegroeid tot de standaardbron van PNT-informatie, omdat deze voorhanden is en eenvoudig geïntegreerd kan worden. EUSPA verwacht dat het aantal geïnstalleerde apparaten dat wereldwijd gebruik maakt van GNSS toeneemt van 6,5 miljard eenheden in 2021 tot 10,6 miljard eenheden in 2031[26]. Het toenemende gebruik wordt gedreven vanuit enerzijds de behoefte aan continue en betrouwbare PNT-informatie en anderzijds het streven naar steeds betere prestaties in termen van bijvoorbeeld nauwkeurigheid, kosten of autonomie. Tegelijkertijd maakt technologische innovatie in bijvoorbeeld ontvangertechnologie ook steeds meer toepassingen van PNT middels GNSS mogelijk. Opkomende toepassingsgebieden zijn bijvoorbeeld autonome systemen, het internet der dingen en 5G. In Tabel 1 worden ter illustratie (niet uitputtend) enkele voorbeelden gegeven van toepassingen van GNSS in diverse sectoren.

In een Britse kwetsbaarhedenstudie[27] wordt beschreven dat alle kritieke nationale infrastructuren tot op zekere hoogte afhankelijk van PNT middels GNSS zijn. Telecom, noodhulpdiensten, energie, landbouw, financiën en transport worden als bijzonder intensieve gebruikers aangemerkt.

Tabel 1 Voorbeelden van GNSS-toepassingen (niet uitputtend) per sector

Digitale overheidsprocessen - Tijdsbepaling door middel van GNSS wordt over het algemeen gebruikt in digitale processen. Zodoende is het aannemelijk dat binnen de digitale overheidsprocessen voor het garanderen van de beschikbaarheid van de basisregistraties van personen en organisaties, de uitwisseling van deze basisinformatie en de beschikbaarheid van de datasystemen waarvan diverse (overheids)organisaties afhankelijk zijn in hun functioneren gebruik maken van GNSS.	Tijd
Openbare orde, veiligheid en defensie - Plaats- en tijdsbepaling door middel van GNSS zijn een waardevol instrument voor de nooddiensten zoals politie, brandweer en medische diensten om de reactie op noodsituaties en de humanitaire hulp te coördineren. Het maakt het mogelijk de locatie van slachtoffer of incident nauwkeurig te bepalen en ook de beschikbare nooddiensten met inachtneming van de geldende responstijden adequaat te leiden naar deze locatie. Voor defensie is PNT middels GNSS belangrijk voor haar operationele activiteiten; data link, GPS guided ammo, logistieke droppings, plaatsbepaling van troepen, tracking van mensen en objecten et cetera.	Tijd en Positie
Luchtvaart - De luchtvaart gebruikt PNT middels GNSS voor het veilig navigeren en laten landen van vliegtuigen. Zo zorgt de toepassing van plaatsbepaling middels GNSS voor veiligere vliegroutes door bijvoorbeeld precies aan te geven waar er aswolken zijn of waar de grenzen van een conflictgebied zijn ten opzichte van de eigen locatie, zodat er dan omheen kan worden genavigeerd. Op basis van PNT-data middels GNSS kunnen nauwkeurig tijd en plaats worden bepaald en worden toepassingen als geo-fencing en geo-caging mogelijk die helpen om de regels voor drones te reguleren zoals, waar wel en niet gevlogen mag worden.	Tijd en Positie

[25] "Time – The Invisible Utility," Cybersecurity and Infrastructure Security Agencyhttps://us-cert.cisa.gov/sites/default/files/documents/Technical-Level_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdfhttps://us-cert.cisa.gov/sites/default/files/documents/Corporate_Leadership_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf

[26] EUSPA EO and GNSS Market Report 2022/Issue 1

[27] London-Economics-Economic-impact-to-the-UK-of-a-disruption-to-GNSS-2017.pdf (ursanav.com)

Geografische diensten – Met GNSS-data worden in de landmeetkunde en cartografie, nauwkeurige plaatsbepalingen en metingen gedaan die gebruikt worden voor geografische informatiesystemen, de productie van kaarten en voor topografische opmetingen.	Positie
Energieproductie - GNSS wordt gebruikt voor onder meer de plaatsbepaling van booreilanden en voor de olie- en gasexploratie wordt plaats- en tijdsbepaling gebruikt bij het doen van seismisch onderzoek.	Tijd en Positie
Energiedistributie - Monitoring en beheer van elektriciteitsnetwerken zijn sterk afhankelijk van GNSS-timing en –synchronisatie ondermeer als tijdsbasis voor control systems en event logging systemen van de energienetwerken. Op het gebied van grondstoffen ondersteunt GNSS bij de selectie, planning en monitoring van locaties, maar ook bij toezicht op mijnbouwactiviteiten en begeleiding van mijnbouwmachines.	Tijd en Positie
Scheepvaart - De toepassing van GNSS in de scheepvaart is breed. Onder meer het berekenen van veilige en efficiënte vaarroutes via toepassingen zoals VMS (Vessel Monitoring System) en AIS (Automatic Identification System) gebeurt met behulp van plaatsbepaling middels GNSS. Maar ook voor de voorspelling van benodigde ruimte voor opslag van lading en vaartuigen in havens en voor de veiligheid van vaarroutes of bij de aanleg van windparken wordt gebruik gemaakt van GNSS. Denk hierbij aan situational awareness en collision avoidance systemen.	Positie
Wegvervoer - GNSS wordt in de vervoerssector gebruikt voor navigatie, efficiëntieberekeningen en fleetmanagement voor bussen, auto's en fietsen- en scooterverhuur. Ook voor systemen als rekeningrijden en data van tachografen is GNSS van belang. Hetzelfde geldt voor berekeningen van verkeerscongestie en aankomsttijden van wegtransporten. Waarschijnlijk gaat GNSS ook een rol spelen in (regelgeving voor) autonoom vervoer.	Positie
Watermanagement - GNSS wordt gebruikt bij de aanleg en bewaking van dijken, bruggen en andere waterwerken. Denk hierbij aan toepassingen voor de nivellering (grondwerken), controle op verzakkingen, positiebepaling baggerwerkzaamheden, peilbeheer et cetera.	Positie
Onderwijs en wetenschap - Positie- en tijdsbepaling door middel van GNSS is essentieel voor het doen van metingen. Het wordt gebruikt in modellen in algemene zin en voor wetenschappelijke toepassingen, zoals de schatting van de magnitude van aardbevingen, meteorologie, et cetera.	Tijd en Positie
Bouw – Toepassingen die gebruikmaken van plaatsbepaling middels GNSS met hoge nauwkeurigheid maakt veilige en tijdige voltooiing van bouwwerkzaamheden op het gebied van onze infrastructuur mogelijk.	Positie
ICT/Telecom - Tijdsbepaling middels GNSS speelt een steeds kritiekere rol bij de synchronisatie en exploitatie van telecommunicatienetwerken. Hierbij gaat het om mobiele netwerken, vaste telefoonlijnen (inclusief internet), professionele radio maar ook het C2000 netwerk voor nooddiensten.	Tijd
Klimaatdiensten - GNSS heeft beperkte maar belangrijke toepassingen voor het klimaatdienstendomein. De technologie ondersteunt een reeks geodetische toepassingen die eigenschappen van de aarde (magnetisch veld, atmosfeer) meten die directe gevolgen hebben voor het klimaat. In toenemende mate speelt GNSS een rol in klimaatmodellen.	Tijd en Positie
Spoorvervoer – Plaats- en tijdsbepaling middels GNSS wordt gebruikt in systemen voor de advisering van de machinist, het beheer van assets maar ook in koppelingen met partnersystemen voor het doorgeven van aankomsttijden voor passagiers bijvoorbeeld.	Tijd en Positie

Landbouw en bosbouw - De landbouwsector gebruikt GNSS-data voornamelijk in landbouwvoertuigen voor een efficiëntere inzet van besproeiingsmiddelen en voor de rijbewegingen van de voertuigen. Maar ook voor het monitoren van de veestapel: zo zijn voor GNSS geschikte wearables voor vee in opkomst. Dit past in de trend om het dierenwelzijn te verbeteren. In de bosbouw wordt GNSS-data gebruikt in toepassingen voor de bewaking en instandhouding van de duurzaamheid van bossen. Naast precisiebosbeheer is een belangrijke opkomende trend het gebruik van drones en volgapparatuur om de gezondheid van bomen en de efficiëntie van houtvoorzieningsketens te bewaken. Ook wordt plaatsbepaling middels GNSS gebruikt voor de navigatie en inzet van zwaar materieel en voertuigen in de bosbouw.	Positie
Gezondheidszorg - De zorg gebruikt GNSS-data ondermeer voor het op afstand volgen van kwetsbare mensen zoals bijvoorbeeld patiënten met Alzheimer, het lokaliseren van patiënten indien gebruik gemaakt wordt van een draagbare SOS-button of het delen van gezondheidsgegevens zoals de glucosestatus voor een patiënt met diabetes. Bovendien is het gebruik van GNSS-data niet meer weg te denken in het dagelijks leven en preventieve zorg ter ondersteuning van gezondheid en sportactiviteiten, bijvoorbeeld in wearables, fitness trackers en horloges. Hierbij speelt navigatie en plaatsbepaling een vitale rol.	Tijd en Positie
Chemie - GNSS wordt gebruikt voor het volgen van het vervoer, de opslag en de productie/verwerking van chemische stoffen.	Positie
Voedselketen – GNSS-data wordt gebruikt in toepassingen voor het volgen van goederen en voertuigen. Dit kan de levering van voedsel versnellen en de kwaliteit helpen handhaven. Met positie- en tijdlabels wordt ook de documentatie over voedselveiligheid mede getraceerd.	Tijd en Positie
Nucleair - GNSS wordt gebruikt voor het volgen van het vervoer, de opslag en de productie/verwerking van nucleaire stoffen.	Tijd en Positie
Drinkwater – Plaatsbepaling middels GNSS wordt in beperkte mate gebruikt bijvoorbeeld voor het inmeten en begrenzen van waterwingebieden.	Positie
Visserij – Plaatsbepaling middels GNSS speelt een vitale rol voor het efficiënt en effectief toezicht op visserijactiviteiten via toepassingen als VMS (Vessel Monitoring System) en AIS (Automatic Identification System). Denk hierbij aan de beveiliging en begeleiding van schepen maar ook aan het opsporen van illegale visserij.	Positie
Verzekeringen en financiën - De financiële wereld vertrouwt op GNSS-timing en –synchronisatie voor de nauwkeurige tijdregistratie van financiële transacties. Ook bij de beveiliging van financiële transacties speelt GNSS een rol. Zo wordt bij een mobiele pintransactie middels GNSS de plaats bepaalt van de mobiele telefoon waarmee de transactie wordt verricht. Dit om te voorkomen dat er transacties met hetzelfde rekeningnummer binnen korte tijd in verschillende landen plaatsvinden.	Tijd
Ruimtevaart – GNSS-data wordt in allerlei ruimtevaarttoepassingen gebruikt, van het gebruik van real-time GNSS-gegevens voor absolute en relatieve navigatie van ruimtevaartuigen tot de ondersteuning van specifieke wetenschappelijke of operationele satellietmissies en het afleiden van aardobservatiemetingen.	Tijd en Positie

2.4.1 Weerbaarheid

De term weerbaarheid staat voor het vermogen van een organisatie om zich voor te bereiden en te reageren op veranderende condities en het kunnen weerstaan en snel herstellen van

verstoringen. Weerbaarheid betreft niet enkel preventie maar ook respons en herstel. Detectie is een integraal onderdeel van preventie, reactie en herstel hoewel sommige preventietechnieken geen detectie vereisen. Belangrijk is dat weerbaarheid hier niet geïnterpreteerd moet worden als het meten van prestaties zoals nauwkeurigheid, integriteit, continuïteit, dekking etc.

Doordat IKUS-II onderdeel is van 'NAVISP element 3' kon er via die weg ook contact gelegd worden met andere ESA lidstaten om een beeld te krijgen van de ontwikkelingen omtrent GNSS-kwetsbaarheden.

Het Verenigd Koninkrijk werkt aan een zogenaamde GNSS Event Notification Service (GENS). Dit is een detectie- en monitoringcapaciteit die doeltreffende rapportage en registratie van GNSS-verstoringen mogelijk maakt. In de Tsjechische Republiek wordt in een studie[28] een aantal experimenten uitgevoerd waarbij het effect van GNSS-verstoringen op een aantal applicaties van de vitale infrastructuur wordt gemeten. In Noorwegen wordt, als gevolg van gedetecteerde verstoringen, gewerkt aan een concept voor een alternatieve bron van PNT-informatie (anders dan GNSS) voor de maritieme navigatie. Met het oog op de impact van verstoringen op de veiligheid en operaties voor de luchtvaart, wordt in Roemenië gemonitord op verstoringen met als doel minimale en verplichte vereisten voor een GNSS-prestatiemonitoringsysteem te ontwikkelen. Roemeense luchthavens die commerciële vluchten aanbieden moeten zich aan deze vereisten gaan houden. Het algemene beeld is dat verschillende landen werken aan detectiemogelijkheden en mitigerende maatregelen om beter inzicht te krijgen in de verstoringen. Door vroegtijdig te kunnen handelen willen ze de impact van GNSS-verstoringen beperken.

In Nederland zijn in de Kennis Innovatie Agenda (KIA) Veiligheid de afhankelijkheden en kwetsbaarheden van GNSS onderkend en is er door overheid en industrie gezamenlijk een agenda opgesteld voor het komen tot een robuuste PNT-oplossing in uiterlijk 2030.

In de studie naar spoofing, uitgevoerd door NLR is aanbevolen dat het toepassen van mitigerende maatregelen, in het bijzonder voor tijdsbepaling middels GNSS wordt afgedwongen door autoriteiten. Daarnaast wordt ook aanbevolen om de monitoring nabij vitale processen uit te breiden zodat detectie beter plaats kan vinden.

Er zijn in diverse sectoren standaarden voor het gebruik van PNT die de weerbaarheid moeten verbeteren, maar een centraal overzicht van waar wel en niet al standaarden zijn, waar ze op gebaseerd zijn en wat de standaarden precies voorschrijven, ontbreekt momenteel. Het Amerikaanse Resilient PNT Conformance Framework is o.a. opgesteld om richting te geven aan organisaties die standaarden ontwikkelen. Het framework is opgesteld in samenwerking tussen overheid en industrie met als doel:

- Het faciliteren van de ontwikkeling en adoptie van weerbare PNT-oplossingen
- Stimuleren van innovatie voor weerbare PNT-oplossingen
- Richting geven aan organisaties die standaarden ontwikkelen
- Het fungeren als een brug tussen bestaande kwetsbaarheden en tegelijkertijd bouwen aan toekomstige weerbare PNT-oplossingen.

Het Amerikaanse framework beschrijft vier niveaus van weerbaarheid en geeft eindgebruikers handvaten op basis waarvan zij kunnen besluiten welk niveau zij geschikt achten afhankelijk van hun risico inschatting, budget en belang van de toepassing. Er is geen Europese variant van een dergelijk framework. Wel worden in het kader van de nieuwe Europese CER- en NIS-richtlijnen[29] aanbieders van vitale sectoren in de toekomst verplicht een risicobeoordeling te doen op risico's die de continuïteit, integriteit of vertrouwelijkheid van hun vitale proces kunnen schaden.

2.4.2 Keteneffecten

Processen in verschillende sectoren zijn soms onderling van elkaar afhankelijk. Hierdoor kunnen verstoringen in de ene sector de bedrijfsvoering in een andere sector beïnvloeden. Vertragingen op de weg, al dan niet door GNSS-verstoringen, leiden bijvoorbeeld tot een grotere kans op aanrijtijdoverschrijdingen voor hulpdiensten.

[28] GNSS Vulnerability & mitigation in Czech Republic

[29] https://www.rijksoverheid.nl/actueel/nieuws/2022/07/22/nieuwe-europese-richtlijn-moet-veiligheid-verhogen

De Britse kwetsbaarhedenstudie schat de economische impact van een vijfdaagse GNSS-uitval in het Verenigd Koninkrijk op 5,2 miljard Britse ponden als gevolg van directe en indirecte effecten (keteneffecten). Keteneffecten zullen altijd contextafhankelijk zijn (bijvoorbeeld voor wat betreft aard van de verstoring, duur) en zijn niet statisch. Met de introductie van nieuwe apparatuur kunnen bijvoorbeeld nieuwe GNSS-kwetsbaarheden ontstaan. Het bijhouden van een actueel overzicht van alle apparatuur binnen omvangrijke processen is zeer arbeidsintensief. Het is dus per definitie niet haalbaar om een uitputtend overzicht te geven van keteneffecten als gevolg van GNSS-verstoringen. Wel is het haalbaar om op hoofdlijnen inzicht te geven in te verwachten keteneffecten.

De Britse kwetsbaarhedenstudie en het rapport Cascading Effects of Global Positioning and Navigation Satellite Service Failures van UCL[30] geven wel veel voorbeelden van keteneffecten.

Het rapport van UCL geeft daarnaast aan dat keteneffecten veroorzaakt door GNSS-verstoringen gerelateerd zijn aan de noodzaak om terug te schakelen op back-up systemen of bufferingoplossingen die doorgaans low-tech zijn. Dit leidt volgens het rapport tot de volgende uitdagingen:

- De huidige maatschappij draait op een 'just-in-time' economie waardoor vertragingen door low-tech oplossingen direct ontwrichtend werken.
- Er is weinig beschikbaarheid van bufferingoplossingen en back-ups doordat hier weinig financiële ruimte voor is of gemaakt wordt en wat een terugkomend probleem in het veld van risico- en crisismanagement is.
- Er is weinig kennis over de routines en procedures van de low-tech back-up en bufferoplossingen doordat veel van het ervaren personeel inmiddels gepensioneerd is en kennisoverdracht moeilijk te realiseren is met de huidige arbeidsmarkt die gekenmerkt wordt door snelle doorstroom van personeel.

Het rapport van UCL beschrijft dat er weinig literatuur is over keteneffecten als gevolg van GNSS-verstoringen en benadrukt dat de onzekerheid over keteneffecten groot is.

In het algemeen kan gesteld worden dat de volgende keteneffecten in de lijn der verwachting liggen:

- Verstoring van PNT middels GNSS zal direct effect hebben op de operationele slagkracht van de nooddiensten terwijl het aantal ongevallen als gevolg van minder nauwkeurige PNT zal toenemen. Dit zal tot meer slachtoffers en gewonden leiden.
- Alle transportmodaliteiten zullen sterk gehinderd worden, wat naast gestrande personen en goederen ook supply chain ontwrichting zal veroorzaken en daarmee de voedselketen zal ontwrichten.
- Financiële diensten zullen, wanneer ze niet geïnvesteerd hebben in weerbaarheid, naar verwachting verstoord worden omdat ze afhankelijk zijn van tijdsbepaling middels GNSS.
- Wanneer de energiesector geïnvesteerd heeft in weerbaarheid zal de impact beperkt kunnen blijven maar toch zullen lokale black-outs niet ondenkbaar zijn. Wel zal de levering van olie, gas en brandstof waarschijnlijk onder druk komen te staan.
- De continuïteit van vitale processen zal onder druk komen te staan doordat er overgeschakeld moet worden op back-up-oplossingen die doorgaans slecht onderhouden zijn, niet langdurig vol te houden zijn en waarover kennis beperkt is. Daarnaast zal de continuïteit van de vitale processen onder druk komen te staan voor zover zij afhankelijk zijn van transportmodaliteiten die sterk gehinderd zullen worden.

[30] Pescaroli, G., Green, L.M., Wicks, R., Bhattarai, S. and Turner, S. Cascading effects of global positioning and navigation satellite service failures. UCL IRDR and Mullard Space Science Laboratory Special Report 2019-02, University College London. DOI: 10.14324/000.rp.10076568

Hoofdstuk 3 Het GNSS, dreigingen & scenario's

Naast het toenemende gebruik van GNSS is er ook een voortdurende stijging van het aantal gevallen van GNSS-verstoringen. Hoewel GNSS-verstoringen soms lastig inzichtelijk te maken zijn – zeker wanneer hier niet proactief op gemonitord wordt – verschijnen in de media steeds vaker berichten over gedetecteerde verstoringen. In 2020 is een lijst met duizenden GNSS-verstoringen gepubliceerd[31]. Bij conflicten wordt steeds vaker elektronische oorlogsvoering ingezet; het verstoren van GNSS is daar een voorbeeld van. Als onderdeel van de awareness campagne van deze studie zijn berichten over gedetecteerde verstoringen opgenomen in de nieuwsbrieven (Bijlage L). Dit hoofdstuk gaat in op het GNSS zodat inzichtelijk gemaakt wordt waar dreigingen kunnen aangrijpen. Tenslotte bevat dit hoofdstuk een aantal scenario's waar GNSS-verstoringen een rol spelen.

3.1 Het GNSS

Een GNSS is opgebouwd uit een aantal operationale segmenten en het signaal in de tussenliggende ruimte. De drie GNSS-segmenten en het GNSS-signaal propagerende richting gebruiker, worden hieronder geïntroduceerd. Meer details over GNSS zijn te vinden in Bijlage F.

Het **gebruikerssegment:** dit segment bestaat uit de apparatuur, de ontvangers, antennes et cetera, dat de signalen, uitgezonden door GNSS satellieten, omzet in positie- en tijdinformatie, en is het gedeelte waar je als gebruiker van GNSS zelf invloed op uit kunt oefenen. Bij onbetrouwbaarheid van de GNSS-positie en tijd is het daarom nuttig te kijken of er in de eigen apparatuur oorzaken zijn te identificeren die je zelf kunt mitigeren. Zo zal een ontvanger die werkt op basis van meerdere satellietnavigatiesystemen in veel gevallen robuuster zijn dan een ontvanger die van een enkele GNSS gebruikmaakt. Een ander voorbeeld van een randvoorwaarde waar de gebruiker invloed op kan uitoefenen is de antenne plaatsing. Omdat een directe ontvangst van GNSS signalen essentieel is voor een nauwkeurige meting, is het van belang rekening te houden met omgevingsfactoren en te voorkomen dat GNSS-signalen van satelliet naar ontvanger voor ontvangst geblokkeerd of weerkaatst worden.

Het **ruimtesegment:** dit segment bestaat uit de satellieten die de GNSS-signalen uitzenden. Hier is ruimteweer een dreiging. Ruimteweer kan niet alleen propagatie van het signaal verstoren, maar kan in uitzonderlijke situaties ook een bedreiging vormen voor de satellieten zelf. Zo kan ruimteweer elektronica aan boord van een satelliet beschadigen. Hierdoor kan deze satelliet onbruikbaar worden. Ook technisch falen is een risico in het ruimtesegment. Satellieten zijn weliswaar ontworpen om mogelijke defecten zo goed mogelijk op te vangen (bijvoorbeeld door het aan boord hebben van reserveapparatuur). Toch kan technisch falen de oorzaak zijn dat een satelliet (tijdelijk) niet werkt.

Het **signaal in de ruimte:** het GNSS signaal legt een grote afstand af om van een satelliet in de ruimte naar de ontvanger op de grond te komen. Door onder andere de relatief lage zendsterkte, de grote af te leggen afstand en de gedeeltelijke absorptie van het signaal in de atmosfeer en ontvangst apparatuur is het ontvangen signaal erg zwak. Dit maakt het Signal in Space (SiS, de term voor het signaal dat van een satelliet naar gebruiker propageert) gevoelig voor verschillende soorten verstoringen. Verstoringen van het SiS zijn op te splitsen in drie oorzaak-categorieën: moedwillig, onbedoeld en natuurfenomenen. Omdat de intentie van de verstoring bij deze drie oorzaken anders is, is het nuttig dit onderscheid te maken. Dit kan helpen bij het oplossen van de verstoring of dreiging. Moedwillige fouten omvatten *jamming* en *spoofing*. Bij jamming wordt het satellietsignaal overstemd; bij spoofing wordt een vals signaal ontvangen. Jamming en spoofing worden in paragraaf 3.3 Scenario's en in Bijlage G verder beschreven. Ook natuurfenomenen zoals ruimteweer beschreven in paragraaf 3.3.1. kunnen het ruimtesignaal verstoren.

Het **grondsegment:** dit segment bestaat uit de apparatuur en faciliteiten om de satellieten te controleren en te besturen en om correctie informatie, nodig om nauwkeurige positie- en tijdsbepaling te kunnen maken, te bepalen. Fouten in het grondsegment kunnen een negatief effect hebben op het SiS. Fouten in het grondsegment kunnen ontstaan door menselijke fouten in de operatie, technisch falen of cyberaanvallen.

[31] Guy Beusnel, zie bijvoorbeeld: Thousands of GNSS jamming and spoofing incidents reported in 2020 , en Roi Mit, Top 10 GPS Spoofing, Events Threat Technology,, https://threat.technology/top-10-gps-spoofing-events-in-history/

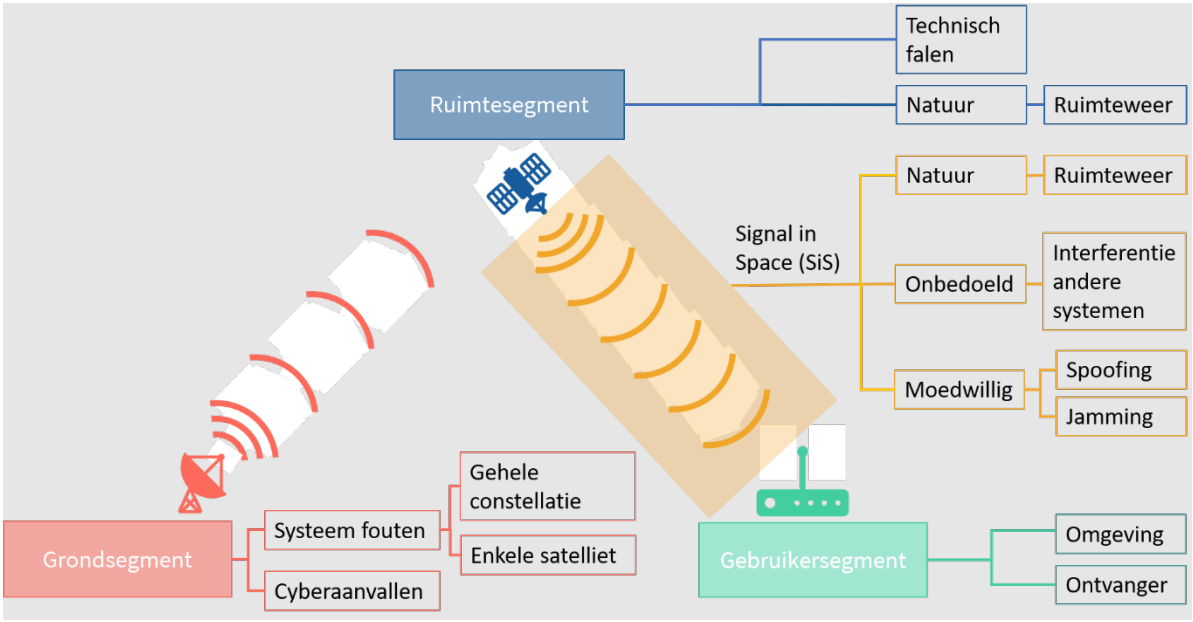
3.2 Dreigingen

Om de kwetsbaarheid van systemen voor uitval van satellietnavigatie in te kunnen schatten, is het belangrijk een overzicht te hebben welke dreigingen een rol kunnen spelen. In de schematische weergave in Figuur 1 is het GNSS opgesplitst in vier verschillende onderdelen:

1. het gebruikerssegment
2. het signaal in de ruimte, ofwel Signal in Space (SiS)
3. het ruimtesegment
4. het grondsegment.

Per onderdeel worden de dreigings- en verstoringstypen die van invloed kunnen zijn weergegeven en benoemd. Meer informatie over deze dreigingen en verstoringstypes is te vinden in Bijlage G.

De continuïteit en weerbaarheid van het grondsegment en het ruimtesegment zijn de verantwoordelijkheid van de GNSS-aanbieder. Als het grondsegment of het ruimtesegment faalt dan probeert de aanbieder de oorzaak van het probleem te vinden en te verhelpen. Alle fouten die het gebruikerssegment introduceert, kan de GNSS-aanbieder niet beïnvloeden. Het adresseren van deze fouten is dan ook de verantwoordelijkheid van de gebruiker.



Figuur 1 Schematische weergave dreiging en verstoringstypen op de verschillende onderdelen van het GNSS

3.3 Scenario's

Voor dit onderzoek worden drie verschillende representatieve gebeurtenissen beschouwd die de nominale ontvangst van GNSS-signalen verstoren. Deze gebeurtenissen hebben verschillende oorzaken (moedwillig, onbedoeld, natuurfenomeen, technisch falen), hebben een verschillende geografische omvang (van lokaal tot wereldwijd) en hebben verschillende looptijden (van uren tot weken). Meer details over de technische aard van deze gebeurtenissen zijn te vinden in Bijlage G. De scenario's die beschouwd worden, zijn:

- **Ruimteweer:** De activiteit van de zon is variabel. Een aantal natuurfenomenen die samenhangen met de zonneactiviteit worden samengevat met de term ruimteweer. In Bijlage G staan de hoofdcategorieën die vallen onder ruimteweer beschreven. Ruimteweer kan, afhankelijk van het type fenomeen en de intensiteit, het gebruik van GNSS op meerdere manieren beïnvloeden. Ruimteweer kan ervoor zorgen dat de kwaliteit van het signal in space degradeert. Het gebruik van gedegradeerde GNSS signalen voor het verkrijgen van een positie- en tijdoplossing heeft een negatief effect op de kwaliteit ervan. In sommige gevallen kan ruimteweer ook ruimte-infrastructuur onbruikbaar maken of verwoesten.

- **Jamming**: Bij jamming wordt de correcte ontvangst van het GNSS-signaal moedwillig geblokkeerd door het uitzenden van een stoorsignaal op dezelfde frequentie als (een van) de GNSS-frequenties. Door dit extra signaal wordt het voor een ontvanger moeilijk of onmogelijk om de toch al zwakke GNSS signalen te detecteren, en de informatie van de GNSS signalen te kunnen extraheren.
- **Spoofing:** Bij spoofing wordt een vals GNSS signaal uitgezonden. Dit signaal lijkt op een echt GNSS signaal en heeft dezelfde kenmerken en modulaties, maar kan verkeerde informatie bevatten. Als een gebruiker een spoofsignaal ontvangt en gebruikt kan dit leiden tot een valse positie- en tijdoplossing. Dergelijke vervalste signalen zijn lastig te detecteren.
- **Systeemfout grondsegment:** Een systeemfout in het controlecentrum van een GNSS kan er voor zorgen dat verkeerde informatie met het SiS wordt verzonden, met als gevolg dat een GNSS-ontvanger verkeerde PNT-informatie naar de gebruikersapplicatie verstuurt Een systeemfout is een onbewuste menselijke fout.

Deze vier scenario's zijn gebruikt om de kwetsbaarheid van de verschillende organisaties binnen de sectoren te analyseren.

3.3.1 Ruimteweer

De zon beïnvloedt onze aarde en haar atmosfeer op verschillende manieren en die kunnen het gebruik van GNSS mogelijk verstoren. De belangrijkste fenomenen zijn a) variaties in het electronengehalte van de ionosfeer en ionosferische scintillaties, b) geomagnetische stormen, c) solar radiation stormen, d) radio black-outs[32]. In het scenario wordt het fenomeen waarin een radio black-out plaatsvindt meegenomen. Tijdens een radio black-out wordt er door de zon een hoeveelheid elektromagnetisch straling in het radio spectrum uitgezonden. Deze emissies hebben een groot bereik (gebied van de Noordpool naar de Zuidpool dat door de zon beschenen wordt) en mogelijk een lange duur (zolang de zon zichtbaar is), zie ook Bijlage G.

Tabel 2 Ruimteweer-event, fenomeen Solar radio blackout

Type event	**Subtype**	**Frequentie van optreden**	**Duur**	**Geografisch gebied**	**Effect op ontvangers-niveau**	**Potentieel betrokken toepassingen**
Solar radio blackout	Extreem	Te weinig informatie aanwezig	Meerdere uren per event	Gehele door de zon verlichte deel van de aarde	Verlies van positie- en tijdsignaal	Alle niet-redundante positie- of tijdsbepalings-toepassingen (synchronisatie)
	Ernstig	8 keer per cyclus	1 – 2 uur per event	Meeste van het door de zon verlichte deel van de aarde	Verlies van positie- en tijdsignaal	Alle niet-redundante positie- of tijdsbepalings-toepassingen (synchronisatie)
	Sterk	Elke 140 dagen	Ongeveer 1 uur	'Uitgebreid gebied' op het door de zonverlichte deel van de aarde	Verlies van positie- en tijdsignaal	Alle niet-redundante positie- of tijdsbepalings-toepassingen (synchronisatie)

[32] Referentie: Solar radio emission as a disturbance of aeronautical radionavigation https://www.swsc-journal.org/articles/swsc/full_html/2018/01/swsc170090/swsc170090.html#:~:text=Between%201000%20and%20%E2%88%BC1200,the%20cause%20of%20these%20disturbances

3.3.2 Jamming en spoofing

Ruimteweer is een natuurlijk fenomeen. Jamming en spoofing zijn echter altijd een direct of indirect gevolg van menselijk handelen. Uitgaande van de beschrijving in detail in Bijlage G zijn de volgende vormen meegenomen in de analyse:

- Hoogvermogen jamming
- Gecoördineerde jamming
- Spoofing

Afhankelijk van de plaatsing en de sterkte van de storingsapparatuur zal het gebied dat last heeft van een aanval in grootte variëren. Grote, bijvoorbeeld militaire, jammers zijn vaak zeer krachtig. Hierdoor kun je deze stoorzenders in het algemeen redelijk goed detecteren en lokaliseren.

Via het internet aan te schaffen jammers zijn juist klein en van beperkt vermogen. Dit soort jammers worden vaak gebruikt om eigen systemen om de tuin te leiden. Andere naburige GNSS-ontvangers kunnen echter wel hinder ondervinden door het gebruik van dit type jammer.

Door één of meerdere jammers strategisch te plaatsen, kan een groot gebied te maken hebben met aanwezige stoorsignalen. Hierdoor kan er een landelijk of regionaal effect ontstaan. Met behulp van meerdere jamming/ spoofing-apparaten kan een gecoördineerde aanval georganiseerd worden. Zo'n gecoördineerde aanval is mogelijk op afstand te bedienen en naar believen in- en uit te schakelen. Op deze manier wordt het getroffen gebied sterk uitgebreid. Omdat met relatief laag vermogen wordt uitgezonden en de jammers / spoofers niet altijd aan hoeven te staan wordt het lokaliseren naar de storingsbronnen gehinderd.

Om spoofing-aanvallen het meest effectief te maken kan ervoor gekozen worden de nepsignalen specifiek te richten op de locatie van het doelwit. Dit type aanval zal minder effectief zijn voor ontvangers op een andere locatie, desalniettemin kunnen ontvangers op andere locaties wel last ondervinden van deze aanval.

De effecten van de verschillende jamming / spoofing-strategieën zijn samengevat in Tabel 3. Hierbij is de verwachte duur van de storing afgeleid van de complexiteit om zo'n stoorsignaal te detecteren en te lokaliseren.

Tabel 3 Effecten van de verschillende jamming / spoofing-strategieën

Type event	**Subtype**	**Frequentie van optreden**	**Duur**	**Geografisch gebied (zie ook Brown, Reynolds, Roberts and Series 1999)[33]**	**Effect op ontvangers-niveau**	**Potentieel betrokken toepassingen**
Jamming en spoofing	Gerichte aanval met laag vermogen (gecoördi-neerd storen)	Onbekend; er is vrij weinig bekend van het daadwerkelijk optreden van dit type storingen.	Kan dagen duren; deze inschatting is gemaakt omdat de detectie en lokalisatie moeilijk is.	Enkele honderden m^2 tot 10 km^2.	Verlies van positie- en tijdsignaal	Alle niet-redundante positie- of tijdsbepalings-toepassingen (synchronisatie van applicatie-apparatuur).

[33] Alison Brown, Dale Reynolds, Capt. Darren Roberts, Major Steve Serie, Jammer and Interference Location System – Design And Initial Test Results, Proceedings of the ION GPS '99, Sept 99, Nashville, TN

Type event	Subtype	Frequentie van optreden	Duur	Geografisch gebied (zie ook Brown, Reynolds, Roberts and Series 1999)[33]	Effect op ontvangers-niveau	Potentieel betrokken toepassingen
Jamming	Aanval met hoog vermogen	Vaak (frequent gebruik in oorlogs-situaties)		Afhankelijk van de sterkte van het stoor-signaal. Het beïnvloede gebied kan variëren van 100m^2 tot honderden km^2.	Verlies van positie- en tijdsignaal	Alle niet-redundante positie- of tijdsbepalings-toepassingen (synchronisatie van applicatie-apparatuur). Merk op: Bij jamming zal de stabiliteit van klokfrequentie van de Timing ontvangers terugvallen naar de stabiliteit van de lokale oscillator (zie ook 2.2). Bij spoofing zal de stabiliteit wel kunnen worden beïnvloed door de spoofer.
Jamming	Verstoren van eigen systemen (laag vermogen)	Dagelijks [34]	Uren, dit type jamming wordt vaak gebruikt gedurende transport.	<=25 m^2	Verlies van positie en tijdsignaal op eigen systeem Tijdelijk lagere kwaliteit (<= 1 minuut) van positie en tijdsignaal voor passanten	Eigen systemen
Spoofing	Spoofing aanval	Onbekend	Kan dagen duren	Vele honderden m^2 tot 10 km^2.	Verkeerde informatie van positie- en tijdsignaal	Alle niet-redundante positie- of tijdsbepalings-toepassingen (synchronisatie van applicatie-apparatuur).

3.3.3 Systeemfouten in het grondsegment

Binnen het grondsegment van een GNSS kunnen zich fouten voordoen die er uiteindelijk toe leiden dat verkeerde status- of correctiedata wordt geüpload naar de satellieten. Deze status- en correctiedata is onderdeel van de satellietsignalen en is essentieel voor een juiste bepaling van positie en tijd door de ontvanger. Dit soort systeemfouten worden, dankzij de vele referentiestations op de grond, meestal snel opgespoord en opgelost. Een voorbeeld van zo'n systeemfout deed zich in januari 2016 voor in het GPS-systeem. Deze fout werd snel gedetecteerd en werd binnen 6 uur op GNSS-niveau opgelost. Het komt soms voor dat een fout leidt tot het verlies van een geheel GNSS voor een korte of langere periode (in één geval betrof het een week, zie Inside GNSS, 2019). De kans dat systeemfouten parallel in verschillende systemen optreden is

[34] Dozens of Jammers at Amsterdam Office Every Day - Dutch Aerospace Center - RNTF (rntfnd.org)

GNSS monitoring LVNL Schiphol-Oost (navnin.nl)

klein. Hierdoor blijft PNT beschikbaar als een ontvanger gebruik maakt van meerdere GNSS. In het geval van een volledig GNSS-verlies heeft dit ook direct gevolgen voor toepassingen met strenge veiligheidseisen waarbij een voldoende aantal zichtbare GNSS-satellieten van belang is. De effecten van een grondsegmentfout zijn samengevat in Tabel 4.

Tabel 4 Effecten van een grondsegmentfout

Type event	**Subtype**	**Frequentie van optreden**	**Duur**	**Geografisch gebied**	**Effect op ontvangers-niveau**	**Potentieel betrokken toepassingen**
Fout in het grond-segment	-	-	Van uren tot (sporadisch) dagen of weken	Aarde	Verlies van één GNSS	Alle gebruikers van desbetreffende GNSS

Hoofdstuk 4 Kwetsbaarhedenanalyse

De kwetsbaarhedenanalyse is gebaseerd op de resultaten verkregen vanuit de questionnaire, de discussies tijdens de masterclasses en de verdiepende risicoanalyse ('deep-dive'). Daar waar dit relevant is, zijn resultaten ook vergeleken met de beschikbare literatuur. Er zijn 159 vertegenwoordigers van 90 verschillende organisaties aangeschreven om te reageren op de questionnaire en deel te nemen aan de masterclasses. Zij vertegenwoordigden zowel vitale als niet-vitale sectoren, waaronder ook sector- en brancheverenigingen. Een overzicht van de aangeschreven organisaties staat in Bijlage A. Daarnaast zijn alle respondenten van de questionnaire en deelnemers uit de masterclasses uitgenodigd voor een verdiepende risicoanalyse. De resultaten van de kwetsbaarhedenanalyse worden hieronder nader toegelicht aan de hand van de vier onderzoeksthema's: kennis en bewustzijn, gebruik, weerbaarheid en keteneffecten. Ook wordt ingegaan op de bereikbaarheid van de doelgroep van deze studie. Bij elk van de thema's worden relevante observaties benoemd.

4.1 Doelgroep

In IKUS-I werd geconstateerd dat de kennis over het gebruik en kwetsbaarheid van GNSS binnen organisaties beperkt is. Het is zodoende niet bekend of en waar de kennis binnen een organisatie geborgd is. Tijdens deze studie is dat nog steeds het geval. Dit maakt het identificeren van de juiste vertegenwoordigers niet eenvoudig. Er is voor gekozen om zowel vertegenwoordigers aan te schrijven die naar verwachting eindverantwoordelijk zijn zoals een directeur, voorzitter of een Chief Information Officer als vertegenwoordigers die met PNT middels GNSS in het dagelijkse werk te maken kunnen krijgen zoals een Chief Information Security Officer, Security Officer of een crisisadviseur. Dat het lastig is om de verantwoordelijke binnen een organisatie te vinden bleek niet alleen bij het aanschrijven van vertegenwoordigers voor de questionnaire maar ook bij het organiseren van de deep-dives. Dit betekent niet noodzakelijkerwijs dat de verantwoordelijkheid niet is ondergebracht bij een functionaris. Maar het betekent in ieder geval wél dat niet centraal binnen de organisatie bekend is bij wie en hoe deze verantwoordelijkheid belegd is. Hieruit volgt de volgende observatie.

Observatie 1: De verantwoordelijkheid voor GNSS-kwetsbaarheden is niet duidelijk belegd in de organisaties (OBS1).

De resultaten van de questionnaire zijn in verband met de vertrouwelijkheid van de respondenten alleen anoniem te analyseren. Het is daarmee dus niet herleidbaar of elke respons ook een aparte organisatie betreft. Sommige vertegenwoordigers hebben de questionnaire vanuit hun specifieke verantwoordelijkheid binnen de organisatie ingevuld; anderen hebben mogelijk de respons afgestemd met de gehele organisatie of zelfs breder binnen de sector. Gezien dit niet bekend is zal het zodoende niet overal mogelijk zijn om sectorbrede conclusies te trekken.

Zoals hierboven aangegeven zijn er 159 vertegenwoordigers aangeschreven. Dit heeft geleid tot 64 responses op de questionnaire. In de IKUS-I studie waren er 91 mensen aangeschreven en reageerden er in totaal 28 respondenten. Sommige organisaties gaven aan dat zij actief zijn in meer dan één sector. Zodoende komen de responses per sector gezamenlijk uit op 136 (zie Tabel 5). In vergelijking met IKUS-I zijn er aanzienlijk meer verschillende sectoren afgedekt. Toch is een aantal sectoren ondervertegenwoordigd. De sectoren gerelateerd aan de voedselketen en de financiële sector bijvoorbeeld. Ongeveer twee-derde van de deelnemers aan de questionnaire (N=43 respondenten) geeft aan niet aan IKUS-I te hebben deelgenomen. Dit laat zien dat er met deze studie ook weer een nieuwe groep organisaties is bereikt.

Tabel 5 Aantal respondenten van de questionnaire per sector[35]

Openbare orde, veiligheid en defensie*	16	Watermanagement*	6
Ruimtevaart	12	ICT/Telecom*	5
Digitale overheidsprocessen*	10	Klimaatdiensten	4
Geografische diensten	10	Spoorvervoer*	3
Luchtvaart*	10	Landbouw en bosbouw	2
Scheepvaart*	9	Gezondheidszorg	2
Overig	8	Chemie*	1
Wegvervoer*	8	Voedselketen	1
Bouw	7	Nucleair*	1
Energieproductie*	6	Drinkwater*	1
Energiedistributie*	6	Visserij	1
Onderwijs en wetenschap	6	Verzekeringen en financiën*	1

* Vitale sectoren

In totaal zijn er vijf masterclasses aangeboden, waaronder één sectorspecifieke gericht op de energiedistributiesector in combinatie met een deep-dive. Voor de financiële sector is er ook een sectorspecifieke masterclass aangeboden in combinatie met een deep-dive. Maar hier is geen gebruik van gemaakt. Aan deze masterclasses hebben in totaal 39 personen deelgenomen (zie Tabel 6).

Ondanks de verbeterde deelname sinds IKUS-I bleef in dit onderzoek een aantal sectoren ondervertegenwoordigd. Vanuit de financiële sector heeft maar één respondent aan de questionnaire meegedaan. Ondanks herhaaldelijke verzoeken aan organisaties binnen deze sector en ook via het Business Continuity platform van DNB, om deel te nemen aan masterclasses of deep-dive sessies is hier niet op ingegaan. En dat terwijl vanuit de literatuur[36] bekend is dat deze sector potentieel kwetsbaar is voor GNSS-verstoringen. De financiële sector heeft wel deelgenomen aan IKUS-I. Het zou mogelijk kunnen zijn dat naar aanleiding daarvan deze sector zich al voldoende heeft beschermd tegen kwetsbaarheden en zodoende nu geen urgentie ziet voor deelname. Dit was in deze studie echter niet te verifiëren. Het was ook niet mogelijk om in IKUS-II te leren van de maatregelen die deze sector heeft genomen.

Ook deelname vanuit de chemie, de nucleaire sector, de drinkwatersector en de visserij is beperkt gebleven tot een enkele respondent aan de questionnaire. Mogelijk kan die ene reactie wel breder afgestemd zijn binnen de sector, maar dat is niet te herleiden. Ook zou het kunnen zijn dat de GNSS positie- of tijdsinformatie van minder belang is voor deze sectoren. Of dat de sector zich al voldoende beschermd heeft tegen deze kwetsbaarheden en zodoende geen urgentie voelt. In het onderzoek hebben we dit echter niet kunnen verifiëren. Ook hier is het dus niet mogelijk om genomen maatregelen inzichtelijk te maken en kennis en kunde hierover te delen met andere sectoren.

[35] Er zijn 14 vitale en 10 niet-vitale sectoren aangeschreven, vanuit de vitale sectoren hebben 72 respondenten deelgenomen en 64 vanuit de niet-vitale sectoren.

[36] Ondermeer "The economic impact on the UK of a disruption to GNSS"

Tabel 6 Aantal deelnemers aan de masterclasses per sector

Watermanagement	7	Onderwijs en wetenschap	2
Openbare orde, veiligheid en defensie	5	ICT/Telecom	2
Luchtvaart	5	Klimaatdiensten	2
Scheepvaart	3	Digitale overheidsprocessen	1
Energiedistributie	10*	Energieproductie	1

* waaronder ook de deelnemers aan de sectorspecifieke masterclass gericht op de energiedistributiesector

Uiteindelijk waren er vier organisaties bereid om deel te nemen aan de deep-dive vanuit de volgende sectoren:

- Openbare orde, veiligheid en defensie;
- Watermanagement;
- Energiedistributie;
- Luchtvaart.

Het is een uitdaging gebleken om organisaties bereid te vinden deel te nemen aan de deep-dive sessies. De precieze oorzaak hiervan is onbekend. Mogelijk hebben organisaties die niet geïnteresseerd waren in deelname de kwetsbaarheden al inzichtelijk en is deelname daarom niet urgent. Maar het zou ook kunnen dat deze organisaties de kwetsbaarheid juist nog onderschatten, waardoor het onderwerp geen urgentie krijgt.

Observatie 2: Een aantal sectoren; voedselketen en visserij maar ook de vitale sectoren verzekeringen en financiën, drinkwater, nucleair en chemie, welke gebruik maken van PNT middels GNSS hebben beperkt deelgenomen aan deze studie waardoor de inzichten voor deze sectoren achterblijven (OBS2).

4.2 Kennis en bewustzijn

Het kennisniveau over het gebruik van PNT middels GNSS verschilt zowel binnen een sector als tussen sectoren aanzienlijk. Dit is zowel terug te zien in de reacties op de questionnaire als in de discussies tijdens de masterclass. Tijdens de masterclass werd ook duidelijk dat het verschil in kennis binnen een organisatie groot kan zijn. Waar de ene persoon haarfijn kan uitleggen waar en waarvoor GNSS gebruikt wordt, heeft de andere persoon geen idee of GNSS gebruikt wordt. Van de 64 responses zijn er 34 die de vragenlijst volledig beantwoord hebben. Een verval van het aantal deelnemers is te zien na de vragen die bedoeld waren om het kennisniveau van de respondent te toetsen. Tijdens de masterclass hebben verschillende organisaties aangegeven dat de kennisvragen hen heeft doen besluiten om eerst de masterclass te volgen. Ze konden dan meer kennis opdoen om vervolgens de vragenlijst beter in te kunnen vullen. Het aanbieden van informatie om kennis mee op te doen leidde hier dus al tot bewustwording over GNSS-kwetsbaarheden.

Er lijkt dus behoefte te zijn aan (aanvullende) kennis over dit onderwerp om een goede inschatting te kunnen maken over kwetsbaarheden ten aanzien van GNSS-verstoringen. De masterclass voorziet hierin: de deelnemers die nog geen basiskennis over GNSS hadden, gaven in hun feedback op de masterclass aan dit na de masterclass wél te hebben. Daarnaast gaven deelnemers aan na afloop de vragenlijst in te kunnen vullen. Verder zijn er deelnemers aan de slag gegaan met het in kaart brengen van kwetsbaarheden binnen de eigen organisatie. Dit laat zien dat het onderwerp relevant wordt gevonden. Verder blijkt: zodra er bewustzijn is, is er ook urgentie om ermee aan de slag te gaan.

Tijdens de masterclasses is er veel kennis uitgewisseld, zowel tussen de onderzoekers en de deelnemers als ook onderling tussen de deelnemers. Na afloop van een aantal masterclasses is de vraag van deelnemers gekomen of het mogelijk was om de contactgegevens van de deelnemers onderling uit te wisselen. Na ieders goedkeuring zijn deze gegevens gedeeld. Dit laat zien dat er ook behoefte is om kennis en kunde onderling uit te kunnen wisselen. De organisaties die

deelnamen aan de deep-dive konden kwetsbaarheden en bijbehorende risico's binnen de eigen organisatie benoemen, maar waren zeker ook geïnteresseerd in het identificeren van nog onbekende kwetsbaarheden. Er was bij de deelnemende organisaties o.a. behoefte aan inzicht en advies voor het maken van keuzes in de verschillende mitigerende maatregelen. Hieruit volgen de volgende observaties.

Observatie 3: Het kennisniveau over het gebruik van PNT middels GNSS en de hieraan gerelateerde kwetsbaarheden verschilt binnen én tussen organisaties (OBS3).

Observatie 4: Er is behoefte aan kennis over GNSS-kwetsbaarheden gerelateerd aan het gebruik van PNT middels GNSS (OBS4).

Observatie 5: De masterclasses zijn een bruikbaar instrument gebleken voor het overdragen van kennis waarmee het bewustzijn over GNSS-kwetsbaarheden is vergroot (OBS5).

4.3 Weerbaarheid

Meer dan 80% van de respondenten op de questionnaire die hebben aangegeven dat zij wel hebben deelgenomen aan IKUS-I (N=17 respondenten), geeft aan dat dit ervoor heeft gezorgd dat er acties zijn genomen om de weerbaarheid tegen GNSS-verstoringen te vergroten. Ook na IKUS-II zijn er direct al acties genomen om de weerbaarheid te vergroten:

- Een organisatie heeft na een masterclass besloten om een GNSS- storingstest op te nemen in haar crisishandboek.
- Twee organisaties hebben besloten om het pakket van eisen voor het inkopen van respectievelijk een navigatietoepassing en een vaartuigbegeleidingssysteem aan te passen: bij toekomstige inkoop houden deze organisaties voortaan rekening met een bepaald niveau van robuustheid tegen GNSS-verstoring.

Hieruit volgt de volgende observatie.

Observatie 6: Zowel IKUS-I als IKUS-II hebben een impuls gegeven aan de verhoging van het bewustzijn aangaande het gebruik van PNT middels GNSS en bij een aantal organisaties ook tot acties om de weerbaarheid te vergroten (OBS6).

Het periodiek uitvoeren van GNSS-storingstesten kan veel inzicht geven in de GNSS-kwetsbaarheden. Bij slechts één organisatie is het testen voor GNSS-verstoringen naar voren gekomen in deze studie. Dit doet vermoeden dat dit soort testen niet perse deel uit maken van beleid en procedures binnen sectoren. Echter is hier in de questionnaire geen expliciete vraag over gesteld. Een dergelijke vraag lijkt een zinvolle uitbreiding van de vragenlijst voor een vervolgstudie (zie ook Bijlage B). Hieruit volgt de volgende observatie.

Observatie 7: Slechts een enkele organisatie voert testen uit om te toetsen of en in welke hoedanigheid zij kwetsbaar zijn voor GNSS-verstoringen (OBS7).

In geval van een GNSS-verstoring, zal een organisatie alternatieve technologie moeten gebruiken voor positie en/of tijdsbepaling. Bijna de helft van de respondenten op de questionnaire geeft aan dat er geen alternatieve technologie beschikbaar is in hun organisatie. In de resultaten wordt er met betrekking tot de beschikbaarheid van alternatieven geen groot verschil gezien tussen vitale en niet-vitale processen. Tijdens de masterclasses is ook gebleken dat organisaties soms verwijzen naar alternatieven voor GNSS die op zichzelf ook gebruikmaken van GNSS. Dit roept het beeld op dat kennis over alternatieve technologie nog geen gemeengoed is. Hieruit volgt de volgende observatie.

Observatie 8: Het gebruik van back-up systemen en kennis over deze systemen is nog geen gemeengoed. Aan het advies van IKUS-I om de toepassing van alternatieven voor GNSS te onderzoeken is onvoldoende invulling gegeven (OBS8).

Om te bepalen in welke hoedanigheid een organisatie kwetsbaar is voor GNSS-verstoringen is het allereerst relevant om te weten van welke GNSS-constellatie(s) er gebruik gemaakt wordt. Zoals toegelicht in paragraaf 2.2 komt het de robuustheid van een applicatie die PNT-informatie van het signaal gebruikt ten goede als er meerdere constellaties worden gebruikt. Echter sommige organisaties kiezen er in hun beleid bewust voor om maar één constellatie te vertrouwen. Van alle deelnemers gaf 59% van de respondenten aan meer dan één GNSS-constellatie te gebruiken, gaf 19% aan niet te weten wat er gebruikt wordt, gaf 22% aan maar één constellatie te gebruiken waarvan 3% vanwege politieke redenen en 19% vanwege technische redenen. Hieruit volgt de volgende observatie.

Observatie 9: Een meerderheid lijkt kennis te hebben over welke GNSS-constellaties gebruikt worden binnen de organisatie (OBS9).

Een van de vragen in de questionnaire is of de kwetsbaarheid voor GNSS-verstoringen meegenomen wordt in de risicobeoordeling c.q. continuïteitsplannen van de organisatie. Op deze vraag antwoordt het merendeel van de respondenten met 'nee' (43%). 18% geeft aan het niet te weten; 39% geeft aan dat dit wordt meegenomen in de organisatie. Op de vraag of de organisatie actief bezig is met de weerbaarheid tegen GNSS-verstoringen antwoordt ongeveer de helft van de respondenten op de questionnaire 'neutraal'. Deze vraag moesten respondenten invullen om de vragenlijst af te ronden. 'Neutraal' staat waarschijnlijk voor zowel de deelnemers die neutraal zijn als de deelnemers die niet goed weten of hier actief op geacteerd wordt. Voor de respondenten binnen de vitale processen geeft een meerderheid van 73% aan dat hun organisatie niet actief bezig is met de weerbaarheid tegen GNSS-verstoringen (of is hier neutraal over). Verder viel tijdens de deep-dives wederom op dat het niet altijd eenvoudig is om de verantwoordelijke voor GNSS-kwetsbaarheden binnen een organisatie te vinden. Hieruit volgt de volgende observatie.

Observatie 10: De aanwezigheid van beleid ten aanzien van GNSS-kwetsbaarheden en het bewustzijn hierover lijkt nog niet vanzelfsprekend binnen organisaties (OBS10).

Tenslotte gaven twee organisaties tijdens de deep-dives aan dat actueel inzicht in de betrouwbaarheid van GNSS-signalen en de mogelijke oorzaak van een GNSS-verstoring zeer gewenst is om snel te kunnen handelen en de vervolgschade te beperken. In één van de deep-dives kwam naar voren dat dit voor een organisatie binnen 15 minuten moet gebeuren. Want dan kan nog voorkomen worden dat het werk grotendeels stil moet worden gelegd. Met de huidige monitoringsystemen om de betrouwbaarheid van het GNSS-signaal te meten is het niet altijd mogelijk om de achterliggende oorzaak van een storing te vinden. Hieruit volgt de volgende observatie.

Observatie 11: Actueel inzicht in de betrouwbaarheid van GNSS-signalen en de mogelijke oorzaak van een GNSS-verstoring biedt kwetsbare organisaties handelingsperspectief bij het reageren op GNSS-verstoringen en het beperken van effecten (OBS11).

4.4 Gebruik

De groep respondenten die aangeeft GNSS te gebruiken voor positiebepaling is groter dan de groep die aangeeft GNSS voor tijdsbepaling te gebruiken. Organisaties gebruiken de positiebepaling voor navigatie en positionering. Ze gebruiken tijdsbepaling voor kloktijd en synchronisatie. Hierbij moet wel vermeld worden dat positionering en navigatie bij de meeste gebruikers bekender is dan het gebruik van tijd. Het kan dus zijn dat organisaties positiebepaling daadwerkelijk meer gebruiken dan tijdsbepaling, maar dat kan ook aan de grotere bekendheid van positiebepaling bij gebruikers liggen. Van alle respondenten geeft 55% aan GNSS voor een vitaal

proces te gebruiken[37]. Van deze groep geeft 94% aan GNSS voor het primaire proces[38] in te zetten. In IKUS-I was dit 70%. Dit kan duiden op een toename van het gebruik van GNSS in het primaire proces of op een verbeterde kennis onder de organisaties.

Observatie 12: PNT middels GNSS wordt veelvuldig (bewust) ingezet in diverse (vitale) processen binnen alle onderzochte sectoren. Deze inzet is niet alleen voor positiebepaling, maar ook voor tijdsbepaling (OBS 12).

Tijdens de deep-dives hebben de organisaties ook een aantal systemen benoemd die zij gebruiken, maar als mogelijk kwetsbaar worden ingeschat door de betreffende organisaties:

- Telecommunicatie/draadloos netwerk;
- Digitaal observatiesysteem met hogesnelheidscomponenten, eventueel fysiek gedistribueerd uitgevoerd;
- Digitaal control systeem met hogesnelheids-componenten;
- Event-logging systeem;
- Besturingssysteem autonoom voertuig;
- Specifieke navigatiesystemen.

In Bijlage H staat een uitgebreid overzicht van die systemen met de reden waarom de organisatie dit systeem als potentieel kwetsbaar ziet, het aantal deep-dive sessies waarin dit type systeem is genoemd en het back-up systeem dat door de organisatie werd genoemd. Grotendeels zijn dit systemen die je breed binnen verschillende sectoren kunt toepassen. Dit betekent ook dat alle sectoren waarin deze systemen worden toegepast potentieel kwetsbaar zijn.

Hieruit volgt de volgende observatie.

Observatie 13: Er is een aantal universele en tevens potentieel kwetsbare systemen geïdentificeerd die gebruik maken van PNT middels GNSS (OBS13).

4.5 Keteneffecten

Een van de doelstellingen van deze studie was het verkrijgen van meer inzicht in keteneffecten die kunnen optreden als gevolg van GNSS-verstoringen. In de questionnaire en tijdens de masterclass en de deep-dives is hier aandacht aan besteed.

Zoals in hoofdstuk 1 al aangegeven heeft de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) plaats- en tijdsbepaling middels GNSS aangemerkt als een categorie B vitaal proces. Dit betekent dat bij verstoring van dit proces er omvangrijke fysieke, sociaal-maatschappelijke en economische gevolgen merkbaar zullen zijn.

Vanuit de questionnaire geeft 12% van de respondenten aan dat er externe gevolgen zijn die een regio-overstijgende impact hebben. Van de respondenten geeft 9% aan dat deze gevolgen een nationale impact heeft; 21% geeft zelfs aan dat dit leidt tot internationale impact. Van de respondenten geeft vervolgens 45% aan dat zij verwachten dat gevolgen direct zullen optreden, 28 % geeft aan dit te verwachten binnen 24 uur, 24% verwacht het tussen 24 en 72 uur en 3% verwacht dat de effecten pas na 72 uur zullen optreden.

De gevolgen die de respondenten benoemden lopen sterk uiteen in geografische omvang, duur en ernst. De gevolgen hangen uiteraard ook weer af van de oorzaak van de verstoring, de duur van de verstoring en de beschikbaarheid van alternatieven. Tabel 7 geeft ter illustratie een overzicht van de mogelijke gevolgen van GNSS-verstoringen binnen de sectoren die hebben deelgenomen aan de deep-dives.

[37] Voor een overzicht van de vitale processen zoals door de Nederlandse overheid gedefinieerd zie https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

[38] Hiermee wordt bedoeld de processen benodigd voor het uitvoeren van de kerntaken en basale activiteiten van een organisatie

Tabel 7 Gevolgen van GNSS-verstoringen per sector vanuit de deep-dives

Sector	***Voorbeeld van toepassingen van GNSS***	***Effecten bij GNSS-verstoringen***
Openbare orde, veiligheid en Defensie	Navigatie voor hulpdiensten (bijvoorbeeld voor ambulances)	Vertraging van transport en overschrijding van de maximale aanrijdtijden.
	Tijdbasis voor het in stand houden van een draadloze telecommunicatie is essentieel voor informatie-uitwisseling tussen hulpdiensten die op afstand van elkaar werken.	Essentiele gegevens zijn niet tijdig bekend waardoor de hulpdiensten niet goed kunnen acteren.
Energiedistributie	Tijdsbasis voor control systems van de energienetwerken (bijvoorbeeld voor het koppelen van twee elektriciteitsnetwerken).	Koppelen van netwerken is niet mogelijk; zonder een goed back-up-systeem voor de tijdsinformatie kan een black-out ontstaan (zie bijvoorbeeld voor black-out Widonski en anderen)[39].
	Tijdsbasis voor event logging systeem. Log-gegevens zijn essentieel voor het snel oplossen van storingen.	Root cause analyse tijdens storingen duurt langer dan nodig en gewenst, waardoor het netwerk te lang uit de lucht kan zijn.
	Positiebepaling bij het inmeten van ondergrondse infrastructuur.	Het lokaliseren van ondergrondse infrastructuur bij het oplossen van storingen loopt vertraging op (extra graafwerkzaamheden).
Luchtvaart	Navigatie voor bemande en onbemande luchtvoertuigen, inclusief drones.	Vliegverkeer moeten worden omgeleid naar andere luchthavens.
	Performance-based navigatie.	Geluidshinder en brandstofverbruik nemen toe.
	Tijdsbasis voor (mobiele) radarsystemen, communicatiesystemen (inclusief 5G en 6G in de toekomst).	De verschillende componenten van de radarsystemen gaan mogelijk uit de pas lopen. De systemen zullen dan gaan falen met vertragingen bij starten en landingen tot gevolg.
	Baanverlichting. Timing van verlichting wordt met de GNSS-tijd gestuurd.	Vliegverkeer moet worden omgeleid naar andere luchthavens.
Maritiem transport	Scheepsnavigatie, inclusief autonoom aanmeren.	Vertraging bij binnenvaren van grote zeehavens.
	Automatic Identification System (AIS) geven positie en tijdsinformatie aan.	Door positie en tijdsbepaling te beïnvloeden van het eigen systeem kan op illegale locaties en/of tijd gevaren/gevist worden.
	Real-time control van maritieme kunstwerken (bruggen, sluizen, et cetera).	Bruggen en sluizen kunnen niet anticiperen op aankomst scheepvaart.

[39] T. Widomski, K. Borgulksi, J. Uzhychi, P.Olbrysz, J. Kowalksi, Faults of Synchronization Based On GNSS Receivers and Ethernet NTP/PTP Network. Robust Synchronization & CyberSecrity In Critical Infrastructures – Energetics & Smart Grids. 2018

De gevolgen zoals getoond in Tabel 7 zijn in lijn met de beschikbare literatuur over keteneffecten als gevolg van GNSS-verstoringen zoals toegelicht in Hoofdstuk 2. De Nederlandse situatie lijkt in deze sectoren dus niet af te wijken van de situatie die breder geschetst wordt. De exacte omvang en ernst kan echter niet vastgesteld worden in deze studie. Dit heeft meerdere redenen:

- Niet alle relevante sectoren hebben deelgenomen aan deze studie
- Veel organisaties hebben nog geen inzicht in welke processen PNT middels GNSS gebruiken. Daarnaast ontbreekt het ook bij veel organisaties aan kennis om dit inzicht op te kunnen halen. Het is zeer aannemelijk dat er momenteel kwetsbaarheden zijn die nog niet geïdentificeerd zijn vanwege de complexiteit van de processen en gezien GNSS-afhankelijkheden vaak diep in apparatuur verborgen zit.

Om de keteneffecten in beeld te krijgen is zodoende een meer diepgaande studie nodig waar alle relevante sectoren aan deelnemen en waarin de tijd genomen moet worden om organisaties te kunnen helpen met het verkrijgen van inzicht in afhankelijkheden en risico's.

Hieruit volgt de volgende en laatste observatie.

Observatie 14: Er zijn meerdere directe gevolgen en keteneffecten geïdentificeerd die in lijn zijn met beschikbare literatuur en studies, maar de exacte omvang en ernst van de Nederlandse situatie kan in deze studie niet bepaald worden (OBS14).

Hoofdstuk 5 Conclusies

Het gebruik van PNT middels GNSS zal blijven toenemen zoals besproken in hoofdstuk 2. Het is dan ook van belang dat er voldoende aandacht is voor kwetsbaarheden van het gebruik van GNSS voor PNT. Dit geldt niet alleen voor de overheid, het is ook zeer relevant voor de betrokken sectoren en de maatschappij in het algemeen. GNSS-verstoringen kunnen namelijk leiden tot omvangrijke gevolgen voor de nationale veiligheid met maatschappelijke en economische schade. Uit dit onderzoek blijkt dat nog niet alle organisaties op de hoogte zijn van de kwetsbaarheden en de bijbehorende risico's. Zodoende zijn er ook nog de nodige verbeteringen denkbaar om de weerbaarheid te vergroten.

Dit is niet uniek, maar past in het beeld wat ook in andere Europese landen wordt gezien. Andere landen doen vergelijkbare studies en er zijn diverse initiatieven om de weerbaarheid tegen GNSS-verstoringen te verbeteren. Zowel op nationaal als op internationaal niveau is er dus nadrukkelijk aandacht voor deze kwetsbaarheden. Dit onderschrijft de urgentie en het belang. Tegelijkertijd moet er ook op de werkvloer kennis en kunde worden uitgewisseld binnen en tussen sectoren. Dit begint bij bewustzijn. De focus van deze studie lag bij kennisoverdracht en het verkrijgen van inzicht over gebruik en de kwetsbaarheid bij uitval van GNSS. Hieronder zijn de hoofdconclusies van het IKUS-II onderzoek beschreven per onderzoeksthema waarbij ook wordt verwezen naar de observaties, zoals beschreven in hoofdstuk 4.

5.1 Kennis en bewustzijn

1. Het kennisniveau ten aanzien van bewust gebruik en weerbaarheid verschilt sterk per organisatie. Over het algemeen kan geconcludeerd worden dat er nog veel ruimte voor verbetering is op het gebied van kennis en bewustzijn (*OBS3, OBS8, OBS9*);
2. Kwetsbaarheidsstudies zoals IKUS-I en IKUS-II zorgen voor een bewustwordingsimpuls aangaande het gebruik van PNT middels GNSS maar leidt niet perse tot het duurzaam vergroten van de weerbaarheid (*OBS6*);
3. De grote belangstelling voor de masterclasses toont aan dat er veel behoefte is aan het uitwisselen van kennis en kunde over PNT middels GNSS (*OBS4, OBS5*).

5.2 Gebruik

1. PNT middels GNSS wordt veelvuldig (al dan niet bewust) ingezet in diverse (vitale) processen van de onderzochte sectoren. Zowel van positie- als van tijdsbepaling wordt gebruik gemaakt. Uitval kan zodoende verstrekkende gevolgen hebben voor de Nederlandse maatschappij (*OBS12*);
2. Zes, waarvan vier vitale sectoren, van de 24 aangeschreven sectoren hebben niet of nauwelijks geparticipeerd in IKUS-II waaronder ook sectoren die in IKUS-I, alsook in internationale kwetsbaarheden studies, als kwetsbaar worden aangemerkt (*OBS2*).

5.3 Weerbaarheid

1. Er is geen actief beleid binnen sectoren en organisaties dat zich richt op vergroten van de weerbaarheid van processen en systemen welke afhankelijk zijn van PNT middels GNSS. De verantwoordelijkheid ten aanzien van het gebruik van PNT middels GNSS is bij de meeste organisaties daarnaast niet duidelijk belegd (*OBS1, OBS7, OBS8, OBS10, OBS11*);
2. Gericht risicomanagement met betrekking tot PNT middels GNSS ontbreekt bij veel organisaties en zodoende worden geen acties ondernomen en/of geïdentificeerd om risico's te reduceren, zoals het onderzoeken van alternatieven voor GNSS. Het inrichten van risicomanagement en het onderzoeken van alternatieven was een aanbeveling vanuit IKUS-I, waar dus onvoldoende invulling aan gegeven is (*OBS7, OBS8, OBS11*);
3. Kennis over (technische) weerbaarheid is zeer beperkt (*OBS7, OBS8, OBS13*).

5.4 Keteneffecten

1. Internationale onderzoeken en het gegeven dat PNT middels GNSS in Nederland een vitaal proces is, tonen aan dat er bij GNSS-verstoringen maatschappij-ontwrichtende keteneffecten kunnen ontstaan. Deze studie schetst een beeld van de te verwachte keteneffecten als gevolg van GNSS-verstoringen in Nederland. Een diepgaande analyse was geen onderdeel van dit onderzoek (*OBS14*).

Hoofdstuk 6 Aanbevelingen

Op basis van de observaties en conclusies die in de vorige hoofdstukken gepresenteerd zijn worden onderstaande aanbevelingen aan de overheid en aan de sectoren gedaan.

6.1 Kennis en bewustzijn

Aanbeveling 1: Zorg als overheid dat het kennisniveau op peil komt en blijft door het laagdrempelig, centraal en continu beschikbaar te stellen van actuele kennis en kunde.

Niet elke sector heeft met volle overgave deelgenomen aan deze studie, hier is veel winst te behalen. De questionnaire, de verdiepende achtergrondinformatie en de informatie over potentieel kwetsbare systemen en mitigerende maatregelen die wordt aangeboden in de bijlagen bij deze studie (Bijlage C, F, G, H en I) kunnen door sectoren gebruikt worden om inzicht te krijgen in kwetsbaarheden. Het is van belang dat dit gemakkelijk en centraal terug te vinden is voor sectoren die hiernaar op zoek zijn. Het ministerie van Infrastructuur en Waterstaat kan hier een faciliterende rol in hebben. De volgende instrumenten om het kennisniveau te vergroten en op peil te houden worden geadviseerd (niet gelimiteerd tot):

Masterclasses

De masterclasses zijn een laagdrempelig instrument gebleken om kennis en bewustzijn te verhogen en om aan te sporen tot verbeteracties.

Awareness campagnes

Het uitvoeren van testen en awareness campagnes helpt om in de praktijk te zien hoe –soms heel eenvoudig- GNSS verstoord kan worden. Tegelijkertijd wordt de potentiële impact zichtbaarder, wat helpt bij de bewustwording en het begrip van de materie.

Kwetsbaarheidsstudies

Het uitvoeren van kwetsbaarheidsstudies zoals IKUS is waardevol gebleken voor het verhogen van het bewustzijn en geeft tegelijkertijd ook handelingsperspectief benodigd voor het verhogen van de weerbaarheid. Daarnaast kunnen resultaten over de jaren heen vergeleken worden om te verifiëren of er sprake is van verhoging van de weerbaarheid.

6.2 Gebruik

Aanbeveling 2: Ga als beleidsverantwoordelijk ministerie in gesprek met sectoren over het verantwoord gebruik van GNSS, vooral met sectoren die niet hebben deelgenomen aan IKUS-II.

Ga op korte termijn als verantwoordelijk ministerie in gesprek met sectoren, in het bijzonder met de sectoren die niet aan IKUS-II hebben deelgenomen, en spoor ze aan om aan de slag te gaan met een kwetsbaarhedenanalyse. Hiervoor kunnen de masterclass en questionnaire, die beschikbaar zijn gesteld in IKUS-II, worden gebruikt.

Aanbeveling 3: Identificeer als PNT-gebruikende organisatie in welke processen er gebruik wordt gemaakt van GNSS en of dit tijd- of plaatsbepaling betreft.

Organisaties zijn zich nog niet altijd bewust van het gebruik van GNSS. Om meer inzicht in risico's en eventuele keteneffecten te krijgen is het van belang dat het duidelijk wordt welke processen gebruik maken van PNT middels GNSS en welke functionaliteit dit precies betreft (tijd- of plaatsbepaling).

6.3 Weerbaarheid

Aanbeveling 4: Beleg als PNT-gebruikende organisatie de verantwoordelijkheid voor het gebruik van GNSS duidelijk en centraal binnen de organisatie.

Aanbevolen wordt om de verantwoordelijkheid voor het gebruik van GNSS binnen een organisatie te beleggen bij een centraal aanspreekpunt. Een (cyber)security- of businesscontinuïteit-verantwoordelijke kan hier een rol in spelen. Hiermee wordt kennis geborgd en wordt structureel overleg, om zowel binnen als buiten de sector ervaringen uit te wisselen, gefaciliteerd.

Aanbeveling 5: Neem het gebruik van PNT middels GNSS op in bestaande crisis- en risicomanagement processen op zowel nationaal (zoals de rijksbrede risicoanalyse) als op organisatieniveau.

De rijksbrede risicoanalyse bevat op dit moment niet het scenario GNSS-verstoring terwijl hierdoor wel keteneffecten kunnen ontstaan die de maatschappij ontwrichten. Diverse buitenlandse kwetsbaarhedenstudies bevestigen dit beeld. De overheid kan dit door aandacht te besteden aan het gebruik van PNT middels GNSS in crisis- en risicomanagement processen ook stimuleren binnen de sectoren. Organisaties dienen dit vervolgens door te vertalen naar eigen crisis- en risicomanagement en/of business continuïteitsprocessen.

Aanbeveling 6: Vergroot als PNT-gebruikende organisatie de (technische) weerbaarheid tegen verstoring van PNT middels GNSS.

De maatregelen om de (technische) weerbaarheid te vergroten verschillen per sector en per organisatie. Hieronder is er een aantal uitgelicht die meerdere sectoren helpen om weerbaarder te worden. Zie hiervoor ook de KIA Veiligheid, waarin een door de overheid en industrie gezamenlijk opgestelde agenda om te komen tot een robuuste PNT-oplossing.

Onderzoeken van de mogelijkheden voor een GNSS-monitoringsysteem

Tijdens deze studie is het onderwerp monitoring aan de orde gekomen. Tijdens de deep-dives is besproken dat er momenteel weinig tot geen inzicht is in GNSS-verstoringen en de oorzaken hiervan. In 2019 heeft het Agentschap Telecom een studie uit laten voeren op Jamming en Spoofing van GNSS[40] hierin wordt verwezen naar een vorm van monitoring van GNSS-verstoringen. Een monitoringssysteem helpt bij het snel detecteren van een GNSS-verstoring en het bieden van inzicht in de achterliggende oorzaak. Dit helpt bij het beperken van de effecten als gevolg van GNSS-verstoringen, en gezien die mogelijk ernstig en omvangrijk van aard kunnen zijn, is er een groot belang om effecten te kunnen beperken. Er zijn verschillende aanpakken voor een monitoringssysteem denkbaar: de verschillende sectoren realiseren ieder een eigen systeem, een centrale nationale aanpak of een internationale aanpak. Tijdens IKUS-II werd aangegeven dat er interesse is om de haalbaarheid van een nationaal monitoringsysteem te onderzoeken met als belangrijke openstaande vragen: wat dient te worden gemeten, in welke omvang (lokaal, regionaal of zelfs landelijk) en hoe kan dit georganiseerd worden.

Preventieve maatregelen alsook voorbereiden op respons en herstel

Het implementeren van preventieve maatregelen zal nooit volledige garantie kunnen bieden dat PNT-verstoringen niet optreden. Zodoende is het van belang om ook aandacht te besteden aan respons en herstel zoals ook toegelicht in Hoofdstuk 2. Voorbeelden hiervan zijn de beschikbaarheid van alternatieve technologie (back-up systemen) maar ook monitoringsystemen die snel detecteren of er GNSS-verstoringen optreden en inzicht kunnen geven in de oorzaak van de verstoring. Tenslotte is het van belang om storingstesten uit te voeren om te kunnen verifiëren of alle kwetsbaarheden in beeld zijn en de effectiviteit van de geïmplementeerde maatregelen te toetsen. Alle aspecten zijn langsgekomen in deze studie en moeten niet los van elkaar beschouwd worden en worden zodoende in deze aanbeveling gezamenlijk geadresseerd.

[40] https://www.agentschaptelecom.nl/documenten/rapporten/2019/07/16/gnss-spoofing

Vergroot de robuustheid van GNSS-signalen

Zoals toegelicht in hoofdstuk 2 is de apparatuur die gebruik maakt van GNSS vrijwel altijd gebaseerd op de open GNSS-signalen. Naast deze open signalen zou ook het gebruik van beveiligde signalen en andere PNT-databronnen moeten worden onderzocht. Het PRS-signaal van Galileo is een voorbeeld van een beveiligd signaal waarvan door de overheid geautoriseerde organisaties gebruik gemaakt kan worden (in tegenstelling tot het M-code signaal van GPS wat alleen voor militair gebruik is). Het gebruikmaken van het PRS-signaal vergroot de robuustheid aanzienlijk en is tijdens deze studie zodoende meermaals aan de orde gekomen. Tijdens masterclasses is de toegevoegde waarde van beveiligde signalen vaker benoemd in analogie aan het reeds jarenlang bestaan van een beveiligd signaal zoals de M-code van GPS. Dat meerdere participanten niet van PRS weten is niet verwonderlijk immers tijdens IKUS-I was PRS als dienst nog volop in ontwikkeling en was het voor veel organisaties nog onbekend. Inmiddels is PRS steeds meer en beter bekend. Voor de eventuele inzet en implementatie van PRS is nader onderzoek nodig.

Aanbeveling 7: Stel als PNT-gebruikende organisatie beleid op voor het gebruik van GNSS.

Het is van belang om beleid op te stellen voor het maken van afwegingen over voordelen versus risico's ten aanzien van GNSS-gebruik. Wanneer dit vastgelegd is in beleid kan dit eenduidig geïmplementeerd worden binnen een organisatie. Implementatie van het beleid raakt diverse processen binnen de organisatie, zoals bijvoorbeeld het inkoopproces waar bij de aanschaf van apparatuur met een bepaalde gewenste robuustheid rekening gehouden kan worden.

Aanbeveling 8: Onderzoek als overheid op welk niveau kaders nodig zijn om te helpen bij weerbaarheids- en continuïteitsmaatregelen voor sectoren.

Vanuit de overheid kunnen hier zowel op nationaal als op Europees niveau kaders voor beschikbaar gesteld worden. Deze kaders zorgen voor uniformiteit en geeft richting aan maatregelen die organisaties zelf kunnen oppakken om een gewenst (minimaal) niveau van weerbaarheid te realiseren. Dergelijke kaders zorgen ook voor de afbakening en begrenzing tussen overheden en organisaties om dit in goed samenspel op te pakken. Hoe deze kaders ingericht kunnen worden dient onderzocht te worden.

Nationale en Europese kaders

Een Europees voorbeeld is de aangepaste regelgeving zoals de verordening 2014/53/EU die compatibiliteit met Galileo verplicht en de verordening (EU) 2014/165 die voorschrijft om meerdere GNSS-systemen te gebruiken. Een Nationaal voorbeeld is het Amerikaanse Resilient PNT Conformance Framework zoals ook toegelicht in Hoofdstuk 2.

6.4 Keteneffecten

Aanbeveling 9: Doe als overheid in samenwerking met PNT-gebruikende organisaties nader onderzoek om de keteneffecten als gevolg van GNSS-verstoringen in Nederland beter in beeld te krijgen.

Om de keteneffecten in Nederland beter in beeld te krijgen is het van belang dat alle sectoren die potentieel kwetsbaar zijn deelnemen. Omdat de kennis over GNSS schaars is en het identificeren van afhankelijkheden veel kennis van de bedrijfsprocessen vereist, wordt geadviseerd om een kwetsbaarhedenanalyse te doen per sector. Zo kan er tussen organisaties in dezelfde sector kennis en kunde worden gebundeld en leidt de analyse tot een sectorbeeld. Wanneer inzicht verkregen kan worden in het 'volwassenheidsniveau' van een sector geeft dit beter inzicht in de keteneffecten op nationaal niveau. In IKUS-II kon er geen sectorbeeld bepaald worden, omdat de onderzoeksopzet bestond uit een vragenlijst en verdiepende risicoanalyses per organisatie. De vragenlijst was anoniem en geeft richting maar een verdiepende risicoanalyse geeft uiteindelijk de benodigde inzichten. Hiervoor moet voldoende tijd uitgetrokken worden om tot de kern te komen gezien de complexiteit van het onderwerp.

Literatuurlijst:

Capgemini Consulting, IKUS, Synthese-rapport Inventarisatie Kwetsbaarheid Uitval Satellietnavigatie, Ministerie van Infrastructuur en Milieu, dd. 11-03-2016, versie: Final.

John A. Volpe National Transportation Systems Center. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. 29 Aug 01.

Government office for Science, Satellite-derived Time and Position, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/676675/satellite-derived-time-and-position-blackett-review.pdf

NLR, GNS Spoofing, NLR-CR-2019-001-PT-1-RevEd-1, June 2019.

Holland HighTech, KIA Veiligheid, 2019, finale versie.

Inside GNSS, Lessons to be Learned from Galileo Signal Outage, October 1, 2019, https://insidegnss.com/lessons-to-be-learned-from-galileo-signal-outage/

Alison Brown, Dale Reynolds, Capt. Darren Roberts, Major Steve Serie, Jammer and Interference Location System – Design And Initial Test Results, Proceedings of the ION GPS '99, Sept 99, Nashville, TN

M. Harris, FAA Files Reveal Surprising Threat to Airline Safety, The US Military's GPS Tests, IEEE Spectrum, Jan 2021 https://spectrum.ieee.org/faa-files-reveal-a-surprising-threat-to-airline-safety-the-us-militarys-gps-tests

Pescaroli, G., Green, L.M., Wicks, R., Bhattarai, S. and Turner, S. Cascading effects of global positioning and navigation satellite service failures. UCL IRDR and Mullard Space Science Laboratory Special Report 2019-02, University College London. DOI: 10.14324/000.rp.10076568.

NOAA, Space Weather Prediction Center, https://www.swpc.noaa.gov.

T. Widomski, K. Borgulksi, J. Uzhychi, P.Olbrysz, J. Kowalksi, Faults of Synchronization Based On GNSS Receivers and Ethernet NTP/PTP Network. Robust Synchronization & CyberSecrity In Critical Infrastructures – Energetics & Smart Grids. 2018

Christophe Marqué, Karl-Ludwig Klein, Christian Monstein, Hermann Opgenoorth, Antti Pulkkinen, Stephan Buchert, Säm Krucker, Rudiger Van Hoof, Peter Thulesen, Solar radio emission as a disturbance of aeronautical radionavigation, J. Space Weather Space Clim., 8 (2018) A42

Carruti A.P. & Kintner Jr. P.M. et al., Effect of intense December 2006 solar radio bursts on GPS receivers, Space Weather, Volume 6, Issue 10, 2008.

ATIS, Alliance of Telecommunications Industry Solutions, GPS Vulnerability Report, December 7th 2016, https://www.gps.gov/governance/advisory/meetings/2016-12/calabro.pdf

Bijlage A Aangeschreven organisaties

Organisatie
ABN AMRO
Agentschap Telecom
Air Cargo Nederland, brancheorganisatie voor de luchtvrachtindustrie
Aircraft Fuel Supply (AFS)
ANWB
Association of Dutch Certified RPAS Operators
Astron
Basetime XYZ
Bureau Telematica Binnenvaart
Centraal Bureau voor de Rijn- en Binnenvaart (CBRB)
Corendon
Coteq netbeheer
Cyber Security Raad
De Autoriteit Nucleaire Veiligheid en Stralingsbescherming
De Nederlandse Aardolie Maatschappij
De Nederlandse Bank
De Vereniging van Leidingeigenaren in Nederland (VELIN)
Deltares
Dienst Justitiële Inrichtingen
EDSN
Eindhoven Airport
Energie Nederland
Flamingo Airport Bonaire
Gasunie
Groningen Airport Eelde
Groningen Seaports
Haven Amsterdam
Havenbedrijf Rotterdam
Immigratie en Naturalisatie Dienst
Inspectie Leefomgeving en Transport
Instituut Fysieke Veiligheid (IFV)
Kadaster
KLM
KLM Cityhopper (KLC)
KNMI
KNVvL, or AOPA Netherlands (Aircraft Owners and Pilots Association)
Koninklijke Marechaussee (KMar)
Koninklijke Vereniging Nederlandse Rederijen (KVNR)
Koninklijke Vereniging van de Nederlandse Chemische Industrie (VNCI)

Koninklijke Vereniging van Gasfabrikanten in Nederland (KVGN)
Koninklijke Vereniging van Nederlandse Reders
Lelystad Airport
Luchtverkeersleiding Nederland (LVNL)
Lyondell Chemie Nederland B.V.
Maastricht Aachen Airport
Maastricht Upper Area Control Centre (MUAC)
Marin
Martinair
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Ministerie van Defensie
Ministerie van Economische Zaken en Klimaat
Ministerie van Financiën
Ministerie van Infrastructuur en Waterstaat
Ministerie van Justitie en Veiligheid
Ministerie van Justitie en Veiligheid- DG Ondermijning
Ministerie van Justitie en Veiligheid- DG Politie en Veiligheidsregio's
Ministerie van Landbouw, Natuur en Voedselkwaliteit
Ministerie van Onderwijs, Cultuur en Wetenschap
Nationale Beheersorganisatie Internet Providers (NBIP)
Nationale Politie
Nederlands Forensisch Instituut
Nederlandse Industrie voor Defensie en Veiligheid (NIDV)
Netherlands Space Office (NSO)
NIDV
NL Digital
NLR
Nogepa
NOVE
NS
NVL/Rotterdam The Hague Airport
Openbaar Ministerie (OM)
ProRail
Regionale Ambulance Voorziening (RAV) Brabant Midden-West-Noord
Rijkswaterstaat
RVO
Schiphol
Schiphol Group
Schuttevaer
SkyDec
Stedin

Stichting Centraal Orgaan Voorraadvorming Aardolieproducten
Tennet TSO B.V.
TNO
Transavia
TU Delft
TUI fly NL
Universiteit Twente
Universiteit Utrecht
Wageningen University & Research
Veiligheidsregio Amsterdam Amstelland
Veiligheidsregio Noord-Holland Noord
Vereniging afvalbedrijven
Vewin
VLNG
VNPI
Volksbank
Votob

Bijlage B Vragenlijst, masterclass en awareness campagne

A. Vragenlijst

De studie naar de kwetsbaarheid van de samenleving bij GNSS is gestart met het uitzenden van een vragenlijst naar de respondenten genoemd in Bijlage A. De vragenlijst is opgebouwd met de volgende doelen:

- inzicht krijgen in het niveau van GNSS kennis bij de verschillende organisaties;
- verandering van kennis en weerbaarheid ten opzichte van IKUS-I;
- het enthousiasmeren van deelnemers voor het onderwerp GNSS en de deelname in de masterclass/deep-dive.

Om deze doelen te behalen is de vragenlijst opgebouwd uit vijf verschillende pagina's met de volgende verdeling:

Pagina 1: Openingspagina

Pagina 2: Algemene vragen om te begrijpen wie de respondenten zijn

Pagina 3: Vragen om te begrijpen of de deelnemers snappen wat GNSS is en kan

Pagina 4: Eerste stap richting risicoanalyse betreffende de kwetsbaarheid

Pagina 5: Vragen of deelnemers verder in het traject willen deelnemen

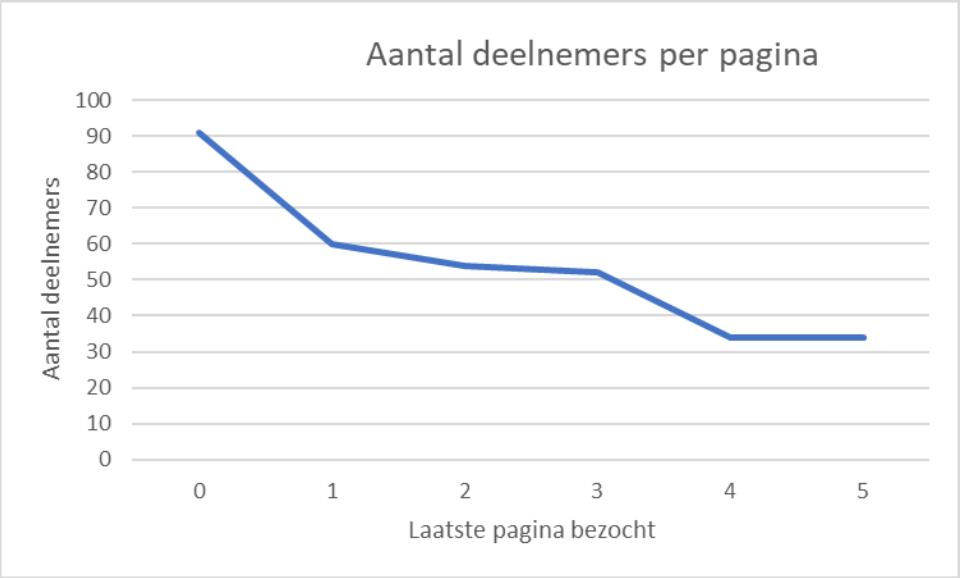
De gehele vragenlijst is te vinden in Bijlage C.

Analyse resultaten

De resultaten van de vragenlijst zijn alleen anoniem te analyseren. Het voordeel van de anonimiteit is dat deelnemers sneller bereid zijn om de vragenlijst in te vullen. Het nadeel is dat het acteren op ingevulde kwetsbaarheden lastig is. Daarnaast is het niet herleidbaar of meerdere personen uit dezelfde organisatie de vragenlijst hebben ingevuld.

Algemene vragen

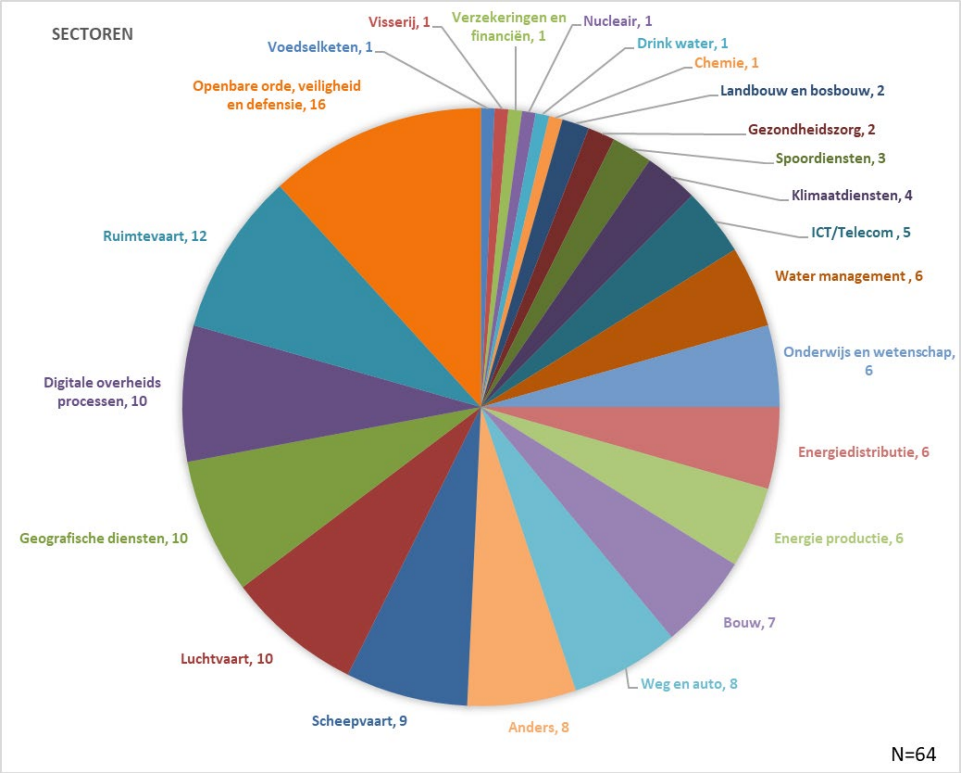
In totaal zijn 91 deelnemers gestart met de vragenlijst. Na het openen van de vragenlijst zijn er een flink aantal personen gestopt met de vragenlijst. Doordat de vragenlijst anoniem is ingevuld is het niet herleidbaar of deze personen later alsnog de vragenlijst hebben afgerond. Vervolgens is er een verval in het aantal deelnemers te zien na pagina 3. Deze pagina was bedoeld om te toetsen wat het kennisniveau van de deelnemer was. Tijdens de masterclass is er vanuit verschillende organisaties gecommuniceerd dat deze pagina hen heeft doen besluiten om eerst de masterclass te volgen om meer kennis op te doen om de vragenlijst daarna goed in te kunnen vullen.



In totaal waren er 159 personen aangeschreven en is de vragenlijst 91 keer geopend en hebben 34 mensen de vragenlijst in totaliteit ingevuld. De vragenlijst is verspreid binnen organisaties dit zal er toe hebben geleid dat meer dan 159 personen de vragenlijst uiteindelijk toegestuurd hebben gekregen.

In de IKUS-I studie waren er 91 mensen aangeschreven en hebben 28 respondenten gereageerd.

De volgende sectoren zijn bereikt met de vragenlijst en hebben minimaal de eerste vraag van de vragenlijst beantwoord. In totaal hebben 64 deelnemers de vragen beantwoord. Een deelnemer kon invullen dat hij/zij in meerdere sectoren werkzaam is.



In vergelijking met IKUS-I zijn er aanzienlijk meer verschillende sectoren afgedekt. Desalniettemin zijn er een aantal sectoren ondervertegenwoordigd. Zo waren de voedingssectoren en de financiële sector ondervertegenwoordigd.

Ongeveer twee-derde van de deelnemers (N=43 respondenten) geeft aan niet aan IKUS-I te hebben deelgenomen, dit laat dan ook zien dat er met deze studie weer een nieuwe groep organisaties is bereikt.

Van de respondenten die wel aan de IKUS-I studie hebben deelgenomen (N=17) geeft meer dan 80% aan dat IKUS-I ervoor heeft gezorgd dat er acties zijn genomen om de weerbaarheid tegen GNSS uitval te vergroten.

Kennisniveau

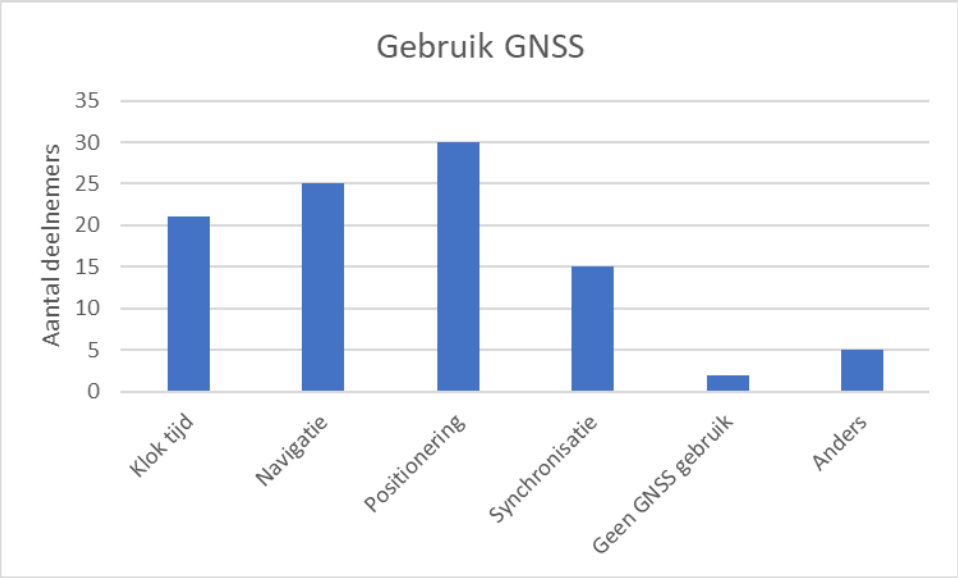
Het kennisniveau zowel binnen een sector als tussen de sectoren verschilt aanzienlijk. Dit is zowel terug te zien in de antwoorden van de vragenlijst als tijdens de discussies tijdens de masterclass. Een deel van de IKUS-II deelnemers maakt gebruik van GNSS en snapt wat het binnen de organisatie brengt en de kwetsbaarheden van het gebruik.

Daarnaast is er een deel dat niet precies weet wat GNSS is en wat je er eigenlijk precies mee kan en de kwetsbaarheden die het gebruik kent. Voornamelijk deze laatste groep is geadresseerd in de masterclass. Tijdens de masterclass werd ook duidelijk dat het verschil in kennis binnen een organisatie groot kan zijn. Waar de ene persoon haarfijn kan uitleggen waar GNSS gebruikt wordt, heeft de andere werknemer geen idee of GNSS gebruikt wordt. Zodoende is het ook van belang dat het dialoog binnen de organisatie gehouden wordt.

Risicoanalyse

GNSS bieden de gebruiker zowel tijd als positie informatie. In het figuur hieronder kan gezien worden dat de organisaties GNSS voor verschillende toepassingen gebruiken. De positiebepaling wordt gebruikt voor navigatie en positionering, dit lijkt een grotere groep te zijn dan voor tijdsbepaling (klok tijd en synchronisatie). Hierbij moet wel vermeld worden dat positionering en navigatie bekender bij de meeste gebruikers is dan het gebruik van tijd. Naast dat plaats bepaling daadwerkelijk meer gebruikt wordt (denk aan Google Maps in de auto), zou er ook door de bekendheid een bias gezien kunnen worden.

In vergelijking met IKUS-I is er een grotere focus betreffende het gebruik van tijd en tijdssynchronisatie.



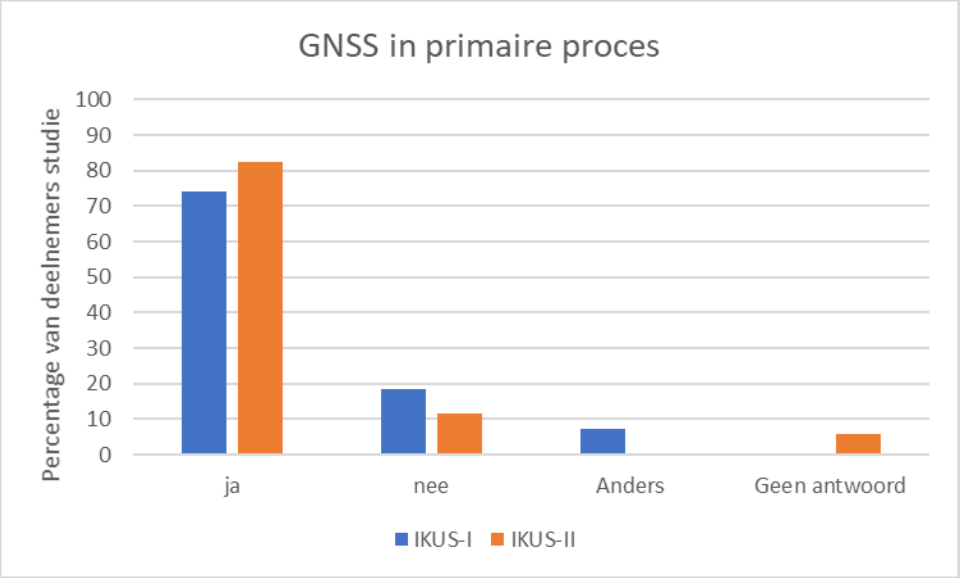
In het IKUS-II onderzoek zijn er vier sectoren waar een deep-dive mee georganiseerd is. Voor deze sectoren worden in deze sectie de resultaten getoond op sectorniveau daar waar geacht relevant te zijn voor de studie. Aangezien het aantal deelnemers binnen een sector klein is, is het van belang om dit in acht te houden bij het interpreteren van deze resultaten.

Deelnemers met een verschillende functie binnen de sector of verschil in GNSS kennisniveau kunnen verschillende en soms tegenstrijdige antwoorden invullen.

	Klok	Navigatie	Positionering	Synchroni-satie	Geen GNSS gebruik
Luchtvaart (n=6)	100%	100%	100%	66%	-
Energie distributie (n=3)	67%	33%	66%	66%	-
Water management (n=6)	67%	83%	100%	50%	-
Openbare orde, veiligheid en defensie (n=8)	75%	75%	87.5%	50%	12.5%

Van alle deelnemers geeft 55% aan GNSS voor een vitaal proces te gebruiken[41], van deze groep geeft 94% aan dat GNSS voor het primaire proces gebruikt wordt.

Van alle deelnemers is het gebruik van GNSS in het primaire proces weergegeven in onderstaande figuur. De resultaten worden hier in percentages weergegeven, waardoor de resultaten van IKUS-I en IKUS-II vergeleken kunnen worden. Bij deze vergelijking kan gezien worden dat er een toename is in het gebruik van GNSS in het primaire proces.



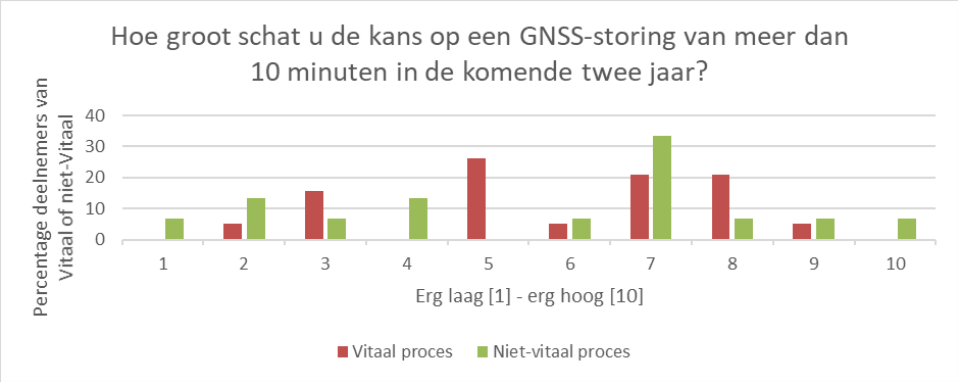
Van de uitgelichte sectoren geeft geen deelnemer aan dat GNSS niet gebruikt wordt voor het primaire proces.

	Ja	Nee
Luchtvaart (n=6)	100%	-
Energie distributie (n=3)	66%	-
Water management (n=6)	100%	-
Openbare orde, veiligheid en defensie (n=8)	87.5%	-

Van alle deelnemers geeft 59% van de respondenten aan meer dan een GNSS constellatie te gebruiken, geeft 19% naan niet te weten wat er gebruikt wordt. Van de 22% die aangeeft maar één constellatie te gebruiken zegt 3% dit te doen vanwege politieke redenen en 19% vanwege technische redenen.

De deelnemers is gevraagd hoe groot zij de kans schatten dat er in de komende twee jaar een GNSS storing van minimaal 10 minuten plaats vindt. Onderstaande figuur heeft de resultaten van de deelnemers uitgezet, waarbij er een onderscheid gemaakt wordt tussen vitaal en niet-vitaal.

[41] Hierbij is vitaal aangegeven zoals aangemerkt door de Nederlandse overheid.

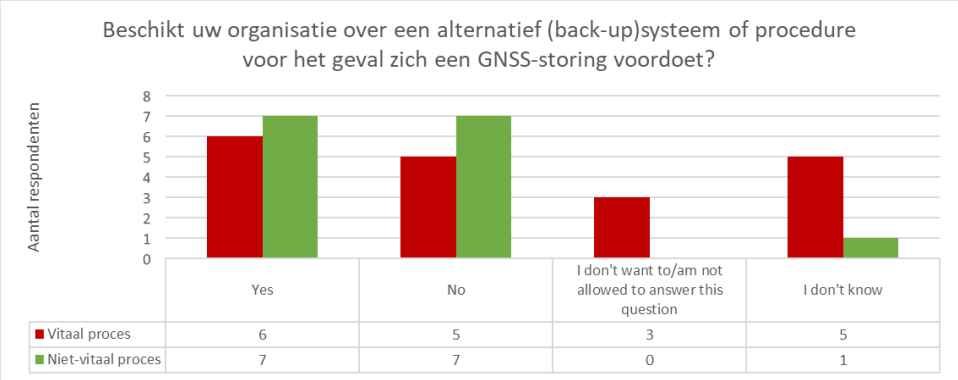


Daarnaast is de deelnemers gevraagd om aan te geven hoe bewust zij zichzelf achten betreffende de gevolgen voor de organisatie in geval van GNSS storing.

Bovenstaande figuren zijn voor de vier uitgelichte sectoren in onderstaande tabel opgesomd. Herin is dus aangegeven welk cijfer de deelnemers zelf hebben gegeven aan de kans die zij schatten dat GNSS verstoord wordt en aan hoe bewust zij zijn van de gevolgen van GNSS uitval. In onderstaande tabel is zowel het gemiddelde cijfer weer gegeven als de standaarddeviatie. Hiermee kan gezien worden hoe 'verdeeld' de antwoorden zijn (hoe hoger de standaarddeviatie hoe groter de antwoorden verschilde).

	Kans op verstoringen	Bewust gevolgen
Luchtvaart (n=6)	6.2 (σ = 2.4)	7.7 (σ = 1.03)
Energie distributie (n=3)	6.3 (σ = 3.8)	6.3 (σ = 3.2)
Water management (n=6)	5.3 (σ = 2.0)	6.5 (σ = 2.1)
Openbare orde, veiligheid en defensie (n=8)	5.25 (σ = 2.4)	7.25 (σ = 1.5)

In geval van GNSS uitval zal er een alternatief gebruikt moeten worden voor positie en/of tijdsbepaling. De deelnemers is gevraagd of alternatief systeem of procedure ingeregeld is in de organisatie. Hierbij geeft bijna de helft van de deelnemers aan dat er geen alternatief beschikbaar is. In de resultaten wordt er geen groot verschil gezien tussen vitale en niet vitale processen.



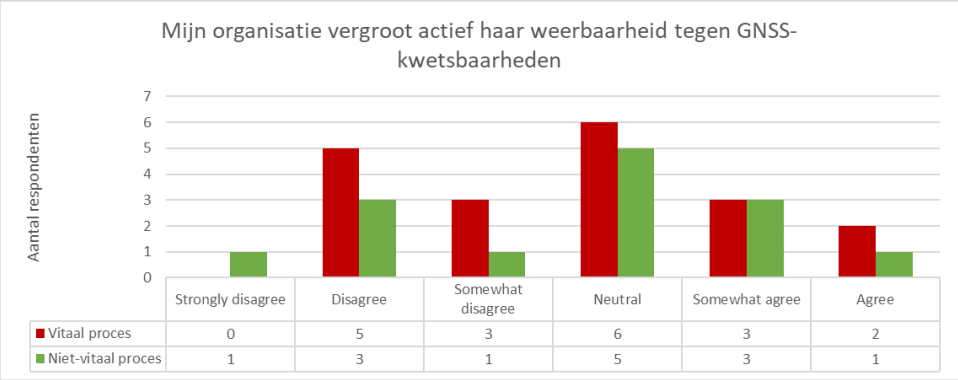
Om een vergelijking te kunnen maken met de resultaten uit de IRAM studie en de vragenlijst zijn de antwoorden van de vier uitgelichte sectoren hieronder geplaatst. Hierin lijkt de luchtvaart en de energie distributie een alternatief te hebben voor GNSS en bij de watermanagement sector lijkt er geen alternatief te zijn.

Bij het interpreteren van deze cijfers moet er rekening gehouden worden met het lage aantal respondenten.

	Ja	Nee	Ik kan/mag hier geen antwoord opgeven	Ik weet het niet
Luchtvaart (n=6)	83%	-	17%	-
Energie distributie (n=3)	66%	-	-	33%
Water management (n=6)	-	50%	17%	33%
Openbare orde, veiligheid en defensie (n=8)	25%	37.5%	25%	12.5%

Om inzicht te krijgen in het vergroten van de weerbaarheid tegen GNSS-kwetsbaarheden van de verschillende organisaties is onderstaande vraag gesteld aan de deelnemers. In de uitwerking is er een verschil gemaakt tussen de organisaties die gebruik maken van GNSS voor vitale processen en zij die dat niet doen.

Een groot deel van de deelnemers geeft hier neutraal aan. Deze vraag moest ingevuld worden om de vragenlijst af te ronden, neutraal zal waarschijnlijk staan voor zowel de deelnemers die neutraal zijn als deelnemers die niet goed weten of hier actief op geacteerd wordt. In de vitale processen is een meerderheid van mening dat hun organisatie niet actief is met het vergroten van haar weerbaarheid tegen GNSS-kwetsbaarheden.



	Zeer oneens	Oneens	Enigszins oneens	Neutraal	Enigszins mee eens	Mee eens
Luchtvaart (n=6)	-	-	1	2	1	2
Energie distributie (n=3)	1	-	-	2	-	-
Water management (n=6)	-	2	1	1	2	-
Openbare orde, veiligheid en defensie (n=8)	-	3	-	2	-	3

Ja zie Bijlage C 'Primary processes include the core tasks and basic activities of your organisation'

De volgende vraag betreft de vraag of de kwetsbaarheid voor GNSS verstoringen meegenomen wordt in de risicobeoordeling c.q. business continuiteitsplannen.

	Ja	Nee	Ik weet het niet
Luchtvaart (n=6)	67%	17%	17%
Energie distributie (n=3)	67%	-	33%
Water management (n=6)	33%	33%	33%
Openbare orde, veiligheid en defensie (n=8)	37.5%	37.5%	25%

De laatste vraag betreft de vraag op welk niveau de gevolgen van een GNSS-verstoring worden ingeschat (met betrekking tot de activiteiten van uw organisatie). Dat kan variëren van uitsluitend voor de eigen organisatie tot externe gevolgen, met internationale impact.

Gevolgen alleen voor mijn organisatie/bedrijf (n=11)	32%
Externe gevolgen, maar beperkt tot een lokaal niveau (n=9)	26%
Externe gevolgen, meerdere regio's ondervinden gevolgen (n=4)	12%
Externe gevolgen, nationale impact (n=3)	9%
Externe gevolgen, internationale impact (n=7)	21%
Ik weet het niet (n=0)	0%

Conclusies vragenlijst toolbox

Het nadeel van de geanonimiseerde vragenlijst is dat het niet herleidbaar is of organisaties of personen de vragenlijst meerdere keren hebben ingevuld. Echter weegt dit niet op tegen het voordeel dat deelnemers meer open durven te zijn in de vragenlijst omdat de resultaten niet herleidbaar zijn.

Aanbevelingen vragenlijst toolbox

Een belangrijke aanbeveling voor de vragenlijst tool is om de mogelijkheid toe te voegen dat de deelnemer de vragenlijst halverwege kan stoppen en later af kan maken. Met de huidige manier van uitzetten was het niet mogelijk dit te implementeren en de privacy te garanderen. Echter, idealiter zou de gebruiker een keuze moeten kunnen krijgen om of zijn resultaten weg te gooien of later aan te vullen (door bijvoorbeeld een persoonlijke link te krijgen, zonder dat de afnemers van de vragenlijst dit kunnen herleiden).

In de questionnaire wordt geen expliciete vraag gesteld of organisaties hun weerbaarheid ten aanzien van GNSS-verstoringen testen, deze vraag lijkt een zinvolle uitbreiding van de vragenlijst (zie observatie 7).

Tijdens de masterclass kwam naar voren dat een aantal deelnemers tijdens het invullen van de vragenlijst erachter kwamen dat hun kennisniveau niet hoog genoeg was om de vragen goed in te kunnen vullen. Het is daarom aan te bevelen om de deelnemers de kans te geven om zich, bijvoorbeeld door middel van een masterclass, meer te verdiepen in het onderwerp GNSS.

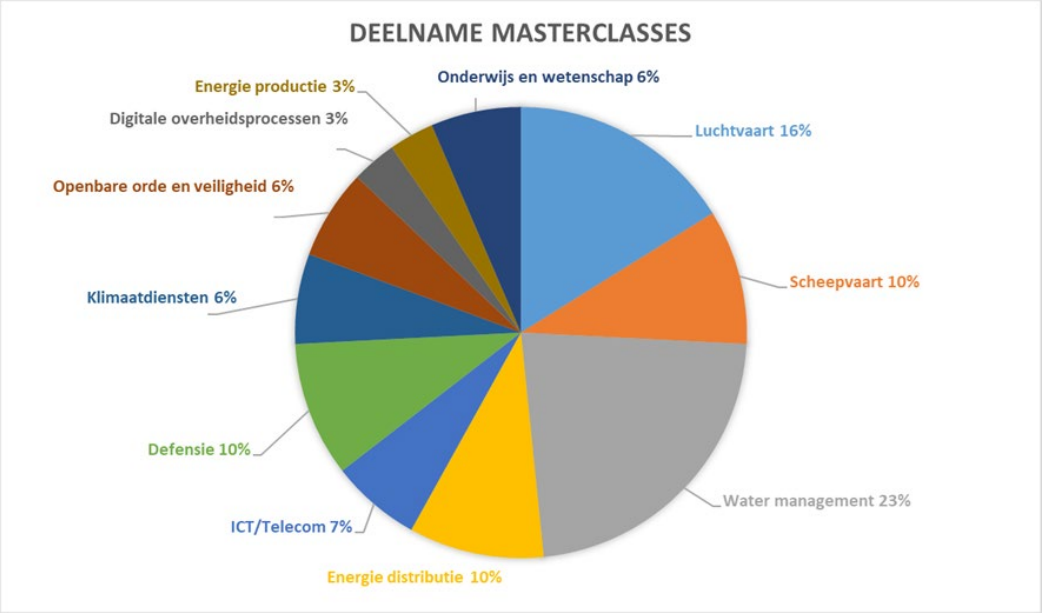
B. Masterclass

Naast de vragenlijst is iedereen ook uitgenodigd om deel te nemen aan de masterclass. De masterclass had meerder doelstellingen:

1. Kennisniveau GNSS naar een basisniveau te brengen
    a. Wat gebruikt kon worden om de vragenlijst in te vullen
    b. Organisaties informatie mee te geven
2. Eerste stap richting kwetsbaarheden analyse
3. Kennis en kunde met elkaar uit kunnen wisselen

In totaal zijn er vier verschillende masterclasses georganiseerd. De masterclass is in twee verschillende varianten aangeboden een algemene en een technische masterclass. De deelnemer kon hierin zelf kiezen welke masterclass het meest geschikt leek. Voor een aantal masterclasses is er om willen van het totaal aantal deelnemers in een klas gekozen om een gecombineerde versie van algemeen en technisch te geven. Zodat de kennis en kunde uitwisseling gewaarborgd kon blijven.

In de vier verschillende klassen zijn er 31 deelnemers geweest die deel hebben genomen.



Daarnaast is er voor energiesector en de financiële sector een sectorspecifieke masterclass aangeboden in combinatie met een verdiepende risicoanalyse. De energiesector heeft hier gebruik van gemaakt en een masterclass met extra focus op tijdsbepaling en synchronisatie is georganiseerd. Deze gecombineerde opzet zorgde voor een levendige kennisuitwisseling tussen de sector en de onderzoekers en in de sector.

Conclusie

De feedback van de deelnemers omtrent de masterclass gaf aan dat de deelnemers die nog geen basiskennis niveau GNSS hadden dit na de masterclass wel hadden. Dit werd ook duidelijk uit de interactie tijdens het interactieve deel van de masterclass. Hierbij werd gevraagd of jamming of spoofing een grotere bedreiging vormde. De redenatie die de deelnemers aanbrachten getuigd van een minimale basiskennis omtrent GNSS. Daarnaast gaf een deel aan na afloop de vragenlijst te kunnen invullen en is er uit organisaties gecommuniceerd dat zij naar aanleiding van de masterclass aan de slag zijn gegaan binnen eigen organisatie.

Tijdens de masterclass werd een groot verschil in kennis van GNSS en de kwetsbaarheden gezien. Daarnaast was er een verschil te zien in de kennis omtrent het eigen systeem. De masterclasses gaven de mogelijkheid om de eerste aanzet richting een risicoanalyse te doen.

Na afloop van een aantal masterclasses is de vraag van deelnemers gekomen of het mogelijk was om de contact gegevens van de deelnemers onderling uit te wisselen. Na ieders goedkeuring zijn deze gegevens gedeeld. Dit laat zien dat er behoefte is om kennis en kunde met elkaar te kunnen wisselen.

Zoals eerder genoemd zorgde de sectorspecifieke gecombineerde (deep-dive + kennisdeling) masterclass ook voor levendige discussie waarbij kennis en kunde binnen een sector plaatsvond.

Aanbevelingen

Een aantal deelnemers hadden specifieke vragen over de ‘state-of-the-art’ betreffende GNSS en over de nieuwe services en PRS. Daar waar mogelijk is hier wel aandacht aangegeven, echter zou dit nog verder uitgediept kunnen worden.

C. Awareness campagne

Als onderdeel van IKUS-II is er ook een awareness campagne gestart om GNSS gebruikers beter bewust te maken van de beperkingen en kwetsbaarheden van het gebruik van GNSS.

Demonstratie Marnehuizen
In samenwerking met Ministerie van Defensie, Netherlands Space Office en CGI is een unieke demonstratie georganiseerd om kwetsbaarheden inzichtelijk te maken. Deze demonstratie is onder professionele begeleiding van Agentschap Telecom uitgevoerd en bijgewoond met grote belangstelling door diverse Ministeries. Op deze dag werd in een open veld de kwetsbaarheid van het open GPS-signaal en de weerbaarheid van het beveiligde Galileo PRS gedemonstreerd. Het is een unieke demonstratie omdat dit soort verstoringen ongewild effect kunnen hebben op de omgeving en de gebruikers. De testen zijn daarom heel secuur en gecontroleerd uitgevoerd.

Tijdens de demonstratie in het militaire oefendorp Marnehuizen is live aangetoond dat open signalen zoals die van GPS kwetsbaar zijn voor misleiding, ook wel bekend als spoofing. Dat gebeurde door met eenvoudig te verkrijgen apparatuur vervalste signalen uit te zenden die lijken op de open GPS-signalen afkomstig van satellieten. Doordat het vervalste signaal sterker is dan het signaal dat vanuit de satelliet afkomstig is, neemt de apparatuur de vervalste signalen voor werkelijkheid aan. Je kunt spoofing vergelijken met deep-fake: wat je ziet lijkt werkelijkheid, maar dat is het niet.

De bevestiging van de demonstratie werd zeer duidelijk toen een toevallige passant, op basis van zijn telefoon, totaal gedesoriënteerd door het oefendorp kwam fietsen. Door inzet van een huis-tuin-en-keuken simulatieapparatuur is deze recreërende fietser op de verkeerde locatie uitgekomen. Een onschuldig voorval, maar toont zeer goed de eenvoud van het probleem en de eventuele gevolgen.

Nieuwsbrief

Tijdens de masterclass kwam naar boven dat deelnemers graag informatie zouden ontvangen waar zij meer bewustwording binnen de eigen organisatie mee zouden kunnen creëren. Zodoende is er in overleg besloten om een aantal nieuwsbrieven uit te sturen. In deze nieuwsbrieven worden vragen die gesteld zijn tijdens de masterclass verder uitgediept, daarnaast worden er meerdere GNSS verstoring ‘evenementen’ beschreven. Door krantenkoppen aan te halen is er getracht om meer bewustwording te creëren.

De nieuwsbrieven zijn in Bijlage L te vinden.

Bijlage C Questionnaire

IKUS-II: inventarisation of vulnerabilities due to GNSS outage

The IKUS-II project is a project comissioned by the Dutch government and executed by the GNSS centre of excellence. The aim of IKUS-II is to assess the current resilience of Dutch organisations against GNSS threats, and to help organisations to become aware of the risks within their organisation. This questionnaire is part of the first stage of the project and will help to assess the current state of recognized threats and the level of resilience. Future activities of the IKUS-II project are announced at the end of this questionnaire.

Completing the questionnaire will take approximately 10 - 15 minutes. Questions indicated with * are mandatory.

The replies to this questionnaire will be handled with care and the processing of the replies is anonymous. The information will be handled as commercially confidential. The outcome of this questionnaire will be reported anonymously and per sector. Answers to open questions will remain confidential. The last section of this questionnaire will in certain cases request an e-mail adress. This section will be processed seperately in order to maintain anonymous processing of the questionnaire.

There are 32 questions in this survey.

General questions

In this section we ask you to answer some general questions regarding your organisation, your function within the organisation and previous participation in GNSS resilience studies.

In what sector does your organisation operate? *

ⓘ Check all that apply
Please choose **all** that apply:

- [ ] Agriculture and forestry
- [ ] Aviation
- [ ] Chemistry
- [ ] Climate services
- [ ] Construction
- [ ] Defence
- [ ] Digital government processes
- [ ] Drinking water
- [ ] Education and science
- [ ] Energy distribution
- [ ] Energy production
- [ ] Fisheries
- [ ] Food chain
- [ ] Geo services
- [ ] Healthcare
- [ ] ICT/Telecom
- [ ] Insurance and finance
- [ ] Nuclear
- [ ] Public order and safety
- [ ] Rail
- [ ] Road and automotive
- [ ] Shipping
- [ ] Space
- [ ] Water management
- [ ] Other:

What is your function within your organisation? *

Choose one of the following answers
Please choose **only one** of the following:

- ◯ I am an expert in / responsible for evaluating my organisations risk of exposure to internal and external threats
- ◯ I am an expert on / responsible for the technical processes within my organisation
- ◯ I make sure daily operations are carried out
- ◯ I manage my organisations affairs (I am a manager)
- ◯ Other [ ]

Have you (or your organisation) participated in the IKUS-I* study (https://www.eerstekamer.nl/overig/20170823/synthese_rapport_inventarisatie/f=/vkh1kaljlc performed in 2015?

*

Choose one of the following answers
Please choose **only one** of the following:

- ◯ Yes
- ◯ No

Has the participation in IKUS-I created awareness of GNSS vulnerabilities and/or has participation resulted in actions to increase resilience against GNSS vulnerabilities? *

Only answer this question if the following conditions are met:
((G02Q04,NAOK (/IKUS-II/index.php/questionAdministration/view/surveyid/147553/gid/2/qid/7) == 'AO01'))

Choose one of the following answers
Please choose **only one** of the following:

- ◯ Yes
- ◯ No

GNSS

This section is meant to introduce the topic of GNSS to you, and provide some insight in the situations where GNSS is used. After completion of this section of the questionnaire, feedback will be provided.

GNSS (Global Navigation Satellite Systems) is used as an umbrella term for all available global navigation satellite systems. Multiple systems, so called constellations, exist and are used. GNSS users can make use of one specific system or a combination of multiple systems: GPS (American), Galileo (European), GLONASS (Russian) and BeiDou (Chinese).

Select the images (/IKUS-II/upload/surveys/147553/files/attributions(1).txt) of the situations where GNSS is used

*If you want to open the link, please do so in a new tab

*

ⓘ Check all that apply

Please choose **all** that apply:

☐ 

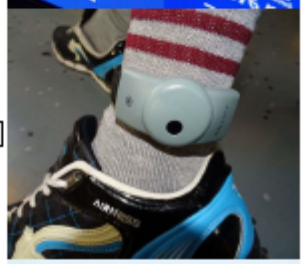
☐ 

☐ 

☐ 

☐

☐ 



What can GNSS do? *

ⓘ Check all that apply
Please choose **all** that apply:

- ☐ Provide information on the current time
- ☐ Provide information on the current location
- ☐ Provide directions
- ☐ Follow your whereabouts and save this information
- ☐ Provide information on your current velocity

GNSS: answers

Curious to what situations do involve GNSS usage?

Situations with GNSS usage

Situations without GNSS usage

And the answers to the question "What can GNSS do?" are:

- Provide information on the current time
- Provide information on the current location
- Provide directions
- Follow your whereabouts and save this information
- Provide information on your current velocity

Please note that questions continue on the next page

Can you think of more unexpected situations where GNSS is used?

Please write your answer here:

Risk assessment

In the previous section of this questionnaire, some situations where GNSS is used were shown as an example. As becomes clear from these examples, GNSS usage is not always easy to identify. Other examples of "hidden" GNSS usage are in wireless communication networks (time synchronization), deformation monitoring of large constructions (position) and dispatch of emergency services (navigation). For more examples see table 1.1 of the UK study to GNSS dependency (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/676675/satellite-derived-time-and-position-blackett-review.pdf)

In this section we ask you to answer some questions regarding the use of GNSS in your organisation and possible consequences in case of GNSS disturbance?

*If you want to open the link, please do so in a new tab

My organisation uses GNSS for *

ℹ Check all that apply
Please choose **all** that apply:

- ☐ Clock time
- ☐ Navigation
- ☐ Position
- ☐ Synchronization
- ☐ No GNSS use
- ☐ I don't know
- ☐ I don't want to/am not allowed to answer this question
- ☐ Other:

My organisation uses *

ℹ Choose one of the following answers
Please choose **only one** of the following:

- ◯ Signals of multiple constellations
- ◯ Signals of only one constellation because of political reasons
- ◯ Signals of only one constellation because of technical reasons
- ◯ I don't know

My organisation uses GNSS for a process labelled as critical* by the Dutch government

*Critical processes are processes which are essential for society. Disturbance or outage of these processes can lead to significant societal disruption and unrest. For a list and more complete description (Dutch) of the critical processes see "Overzicht vitale processen" (https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen)
*

ℹ Choose one of the following answers
Please choose **only one** of the following:

- ◯ Yes
- ◯ No
- ◯ I don't know
- ◯ I don't want to/am not allowed to answer this question

My organisation uses GNSS for a primary process*

*Primary processes include the core tasks and basic activities of your organisation

*

Choose one of the following answers
Please choose **only one** of the following:

- ◯ Yes
- ◯ No
- ◯ I don't know
- ◯ I don't want to/am not allowed to answer this question

What threat causing a possible GNSS disturbance* do you feel is most likely to occur in your organisation?

*Partial or complete failure to receive the GNSS signal due to various reasons (for example (intentional) interference or system outage)

*

Choose one of the following answers
Please choose **only one** of the following:

- ◯ Intentional interference (jamming/spoofing etc.)
- ◯ Space weather (for example solar flares)
- ◯ System outage/damage of GNSS equipment
- ◯ Unintentional interference (for example unintentional jamming due to faulty electronics)
- ◯ Other [ ]

What would effect your organisation more? *

Choose one of the following answers
Please choose **only one** of the following:

- ◯ Compromised data integrity of GNSS position and time information (false data)
- ◯ Unavailability of GNSS signals or systems (no data)

On a scale of 1 to 10 (with 1 being very low and 10 being very high), how large do you estimate the risk of a GNSS disturbance of more than 10 minutes taking place within the upcoming two years to be? *

Please choose the appropriate response for each item:

	1	2	3	4	5	6	7	8	9	10
Risk	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯

On a scale of 1 to 10 (1 being not aware and 10 being very aware), how aware are you of the consequences of a GNSS disturbance for your organisation? *

Please choose the appropriate response for each item:

	1	2	3	4	5	6	7	8	9	10
Awareness	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯

Is vulnerability to GNSS disturbance part of your organisation's risk assessment? *

ℹ Choose one of the following answers
Please choose **only one** of the following:

◯ Yes
◯ No
◯ I don't know

Of what level do you estimate the consequences of a GNSS disturbance to be? (related to the activities of your organisation) *

ℹ Choose one of the following answers
Please choose **only one** of the following:

◯ Consequences for my organisation/business only
◯ External consequences, but limited to a local level (Example financial sector: a few ATMs are not available)
◯ External consequences, multiple regions experience impact (Example energy sector: multiple regions experience small power outages)
◯ External consequences, national impact (Example safety sector: track and tracing of convicts is not possible (electronic tagging))
◯ External consequences, international impact (Example energy sector: large scale power outages also affecting our neighbouring countries)
◯ I don't know

What type of consequences do you expect your organisation or sector to encounter in case of GNSS disturbance? If you can't answer this question please explain why *

Please write your answer here:

After what duration of GNSS disturbance do you expect these consequences to occur? *

ℹ Choose one of the following answers
Please choose **only one** of the following:

- ◯ Direct
- ◯ Between 0-24h
- ◯ Between 24-72h
- ◯ After 72h

Does your organisation have an alternative (backup) system or procedure in place in case a GNSS disturbance occurs? *

ℹ Choose one of the following answers
Please choose **only one** of the following:

- ◯ Yes
- ◯ No
- ◯ I don't know
- ◯ I don't want to/am not allowed to answer this question

Can you elaborate on this alternative/backup system? *

Only answer this question if the following conditions are met:
((G04Q19.NAOK (/IKUS-II/index.php/questionAdministration/view/surveyid/147553/gid/4/qid/46) == 'AO01'))

ℹ Comment only when you choose an answer.
Please choose all that apply and provide a comment:

- ☐ Yes
- ☐ No

My organisation is actively increasing its resilience against GNSS vulnerabilities *

Please choose the appropriate response for each item:

	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
actively increasing resilience	◯	◯	◯	◯	◯	◯	◯

Can you please reflect on the expected future dependency on GNSS within your organisation? (think of increase or decrease of use, implementation of alternatives, additional weaknesses, changes of availability etc.) *

Please write your answer here:

IKUS-II traject

This questionnaire is the first stage of the IKUS-II project. The upcoming questions help us to design the upcoming stages to your wishes and interests.

The next activity of the IKUS-II project will be a GNSS Masterclass. This masterclass will provide the basic level of GNSS knowledge which is necessary to assess the impact of GNSS vulnerabilities on your organisation.

After the masterclass, an awareness event designed to raise awareness to various types of GNSS outages will be organized. The event will consist of a set of activities, including demonstrations of models showing the effects of GNSS and GNSS failures on operations and optional live experiments.

Would you or someone else within your organisation like to learn more about GNSS? *

Choose one of the following answers
Please choose **only one** of the following:

- ◯ Yes
- ◯ No
- ◯ I have already participated in an IKUS-II GNSS masterclass

Please leave your e-mail adress here so we can sent you an invitation to join one of the GNSS masterclasses (multiple e-mail adresses can be entered)

Only answer this question if the following conditions are met:
((G05Q22.NAOK (/IKUS-II/index.php/questionAdministration/view/surveyid/147553/gid/5/qid/56) == 'AO01'))

Could you please provide an explanation on why you are not interested in learning more on the topic of GNSS? *

Only answer this question if the following conditions are met:
((G05Q22.NAOK (/IKUS-II/index.php/questionAdministration/view/surveyid/147553/gid/5/qid/56) == 'AO02'))

Please write your answer here:

Which topic within GNSS specifically interests you *

Only answer this question if the following conditions are met:
((G05Q22.NAOK (/IKUS-II/index.php/questionAdministration/view/surveyid/147553/gid/5/qid/56) == 'AO01'))

ℹ Check all that apply
Please choose **all** that apply:

- ☐ Augmentation systems (for example EGNOS, SBAS, RTK)
- ☐ Position
- ☐ Time
- ☐ Other: _____

Did you find the masterclass helpful? Do you have any comments that can help us improve the masterclass?

Only answer this question if the following conditions are met:
((G05Q22.NAOK (/IKUS-II/index.php/questionAdministration/view/surveyid/147553/gid/5/qid/56) == 'AO03'))

Please write your answer here:

Is your organisation willing to take part in a risk assessment with one of our specialists?

*

ℹ Choose one of the following answers
Please choose **only one** of the following:

- ◯ Yes
- ◯ No

Please leave your e-mail address here so we can send you more information on the IRAM2 risk assessment:

*

Only answer this question if the following conditions are met:
((G05Q26.NAOK (/IKUS-II/index.php/questionAdministration/view/surveyid/147553/gid/5/qid/66) == 'AO01'))

Could you please provide an explanation on why you are not interested in participating in a risk assessment? *

Only answer this question if the following conditions are met:
((G05Q26.NAOK (/IKUS-II/index.php/questionAdministration/view/surveyid/147553/gid/5/qid/66) == 'AO02'))

Please write your answer here:

Do you have any questions or remarks you have regarding (the topic) of this questionnaire? If you want us to come back to you, could you please leave your e-mail adres?

Thank you for your participation. In the near future we will send you an invitation to join the next stage of IKUS-II: a masterclass on GNSS and the risks that come with GNSS usage, We hope to see you there,

Furthermore the main conclusions based on the answers on the questionnaire will be shared with you, taken into account the necessary confidentiality.

Submit your survey.
Thank you for completing this survey.

Bijlage D Methode kwetsbaarheden analyse

Information Risk Assessment Methodology (IRAM2)

Methodologie

De beoordeling van de huidige kwetsbaarheden zal worden uitgevoerd volgens de richtsnoeren van de Information Risk Assessment Methodology 2 (IRAM2) van het Information Security Forum (ISF). De ISF IRAM2-methode is een methode voor risicoanalyse waarbij het bedrijfsperspectief een centrale rol speelt en een alomvattend risicoprofiel kan worden vastgesteld.

Elke gegevensstroom/informatiemiddel ('asset') bestaat uit meerdere componenten. De componenten zijn de risicodragende onderdelen en bepalen de reikwijdte. In samenhang met de Business Impact Reference Table (BIRT) zal er een Business Impact Analyse (BIA) plaatsvinden aan het einde van fase A&B: Scoping & BIA. In fase C richten we ons op de bedreiging van de componenten en in fase D op de kwetsbaarheid. De combinatie hiervan zal leiden tot Fase E waarin een evaluatie zal plaatsvinden. De behandeling in Fase F zal leiden tot aanbevelingen voor risicobeperking.

Figuur 2 IRAM2 model

Wij stellen verschillende primaire variabelen vast die verband houden met GNSS-storingen (zie Bijlage G voor een overzicht van storingsbronnen en daaruit voortvloeiende GNSS-storingen):

- **Nauwkeurigheid**: het verschil tussen de gemeten en de werkelijke positie, snelheid of tijd van een ontvanger;
- **Integriteit**: het vermogen van het systeem om een betrouwbaarheidsdrempel aan te geven en, in geval van een afwijking in de positioneringsgegevens, een alarmsignaal;
- **Continuïteit**: het vermogen van een systeem om zonder onderbreking te functioneren;
- **Availability**: het percentage van de tijd dat een signaal voldoet aan de bovengenoemde criteria inzake nauwkeurigheid, integriteit en continuïteit.

Voor het begin van deze beoordeling is het van belang te weten dat de variabelen van een GNSS-storing in deze methode een binair probleem zijn wanneer zij in een beveiligingscontext worden gebruikt. Het signaal is accuraat of niet, beschikbaar of niet. Er is bijvoorbeeld geen variatie in de integriteit als het gaat om de gevolgen voor het bedrijfsleven. In alle gevallen gaat het om een onbruikbare of ongewenste gegevensstroom en de bedrijfsimpact voor de componenten is - afgezien van de omvang van de storingseffecten - voor elk van de redenen hetzelfde.

Een overzicht van het assessment:

(A) Scoping

Ontwikkelen van een inzicht in de kenmerken van de organisatie als geheel en van de te beoordelen omgeving. De reikwijdte van de beoordeling is de bedrijfsimpact van GNSS-storingen.

Methode en instrumenten

Eerst wordt een selectie gemaakt van de organisaties in verschillende marktdomeinen en wordt de reikwijdte van de beoordeling bepaald. Dit zal gebeuren op basis van de resultaten van de vragenlijst.

(B) Business Impact Assessment en (C) Threat Profiling

De BIA wordt gebruikt om de potentiële bedrijfsimpact voor een organisatie te beoordelen in geval van een (on)opzettelijke uitval van GNSS. In samenwerking met de deelnemende organisatie wordt een lijst opgesteld waarin alle informatiemiddelen en onderliggende componenten worden weergegeven. Deze manier van structureren helpt tijdens het denkproces voor deelnemers die niet noodzakelijk vertrouwd zijn met het in kaart brengen van risico's.

Informatiemiddelen hebben drie kenmerken, te weten:

- **Vertrouwelijkheid** : de informatie alleen toegankelijk is voor bevoegde personen
- **Integriteit** : de informatie juist is (d.w.z. niet gecorrumpeerd en ongewijzigd)
- **Beschikbaarheid** : de informatie toegankelijk en bruikbaar is wanneer dat nodig is.

De Business Impact Reference Table (BIRT) bevat de gecategoriseerde lijst van de meest voorkomende soorten bedrijfsimpact die een organisatie zou kunnen ondervinden als gevolg van het verlies van een (of meer) informatiemiddelen, samen met richtsnoeren om de potentiële impactclassificatie van elk type te bepalen.

Threat Profiling (beschrijving van de bedreigingen) is beperkt tot de primaire variabelen die verband houden met GNSS-storingen. In de basis zijn er drie soorten bedreigingen die het gebruik van GNSS in gevaar brengen:

- Geen signaal beschikbaar
- Slechte beschikbaarheid van het signaal
- Vals signal beschikbaar

Deze bedreigingen kunnen verschillende problemen veroorzaken bij het gebruik van GNSS.

Opmerking:

Om deze beoordeling goed te kunnen uitvoeren is het belangrijk dat de business (afdelingen) begrijpt of en hoe GNSS in hun processen is geïntegreerd. Dit wordt behandeld in de masterclasses en bewustmakings-campagnes en zal verder worden besproken tijdens de deep dive.

(D) Vulnerability Assessment

Er zal een organisatiemodel worden gedefinieerd waarin wordt aangegeven hoe GNSS van invloed is op de dagelijkse gang van zaken en de besluitvorming van deze organisaties.

Identificeren van de controles die van toepassing zijn op de beoordeelde omgeving en inzicht krijgen in hun relevantie voor de GNSS-storingen. Bepalen in welke mate elke controle in de beoordeelde omgeving is uitgevoerd. Inzicht krijgen in de sterkte van de controles die worden uitgevoerd om de omgeving te beschermen tegen GNSS-storingen.

- (E) Risk Evaluation

Verslag uitbrengen over de inzichten uit de voorgaande stappen en de risicostatus evalueren.

Opmerkingen:

Nadat de kwetsbaarheden van elke organisatie zijn geïdentificeerd, zullen de gemeenschappelijke thema's en inzichten in het bijbehorende marktdomein worden geanalyseerd. Op deze manier kunnen organisaties zichzelf benchmarken met anderen en mogelijk van elkaar leren hoe een veilige manier van informatie-uitwisseling kan worden bereikt.

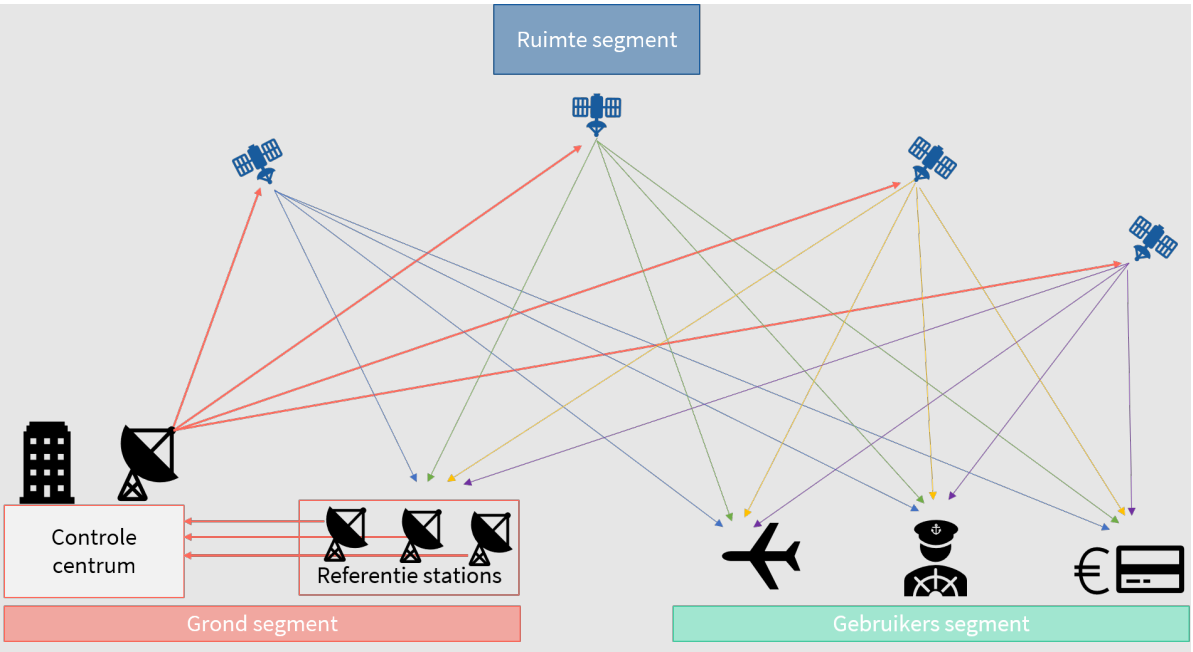
(F) Risk Treatment

Onderzoeken van risicobehandelingsmethoden voor de geïdentificeerde risico's.

Bijlage E Kwetsbaarheden per sector (vertrouwelijk)

Bijlage F Technische diepgang GNSS

Iedere constellatie beschikt over een ruimte segment (de satellieten), een grond segment (het controlestation en de referentie stations) en het gebruikers segment (de gebruikers met ontvangers). In Figuur 3 zijn de verschillende onderdelen van een constellatie schematisch geïllustreerd. Om te begrijpen hoe de verschillende segmenten met elkaar verbonden zijn, is het belangrijk de informatiestromen (weergegeven door de pijltjes) te begrijpen. De satellieten (deel van het ruimte segment) verzenden navigatie berichten richting aarde. Hier kan de gebruiker (gebruikers segment) deze signalen met behulp van een antenne en een ontvanger opvangen, analyseren en gebruiken om een positie en tijd oplossing te bepalen. De gebruiker is niet de enige partij die de signalen op aarde meet. Wereldwijd is er een netwerk van referentie stations. Elk referentie station meet heel precies het GNSS-signaal van een specifieke aanbieder (bijvoorbeeld Galileo), en kan door het gebruik van extra informatie, zoals de bekende eigen positie, correcties berekenen voor het ontvangen signaal. Alle resultaten verkregen door deze losse referentie stations worden doorgegeven naar het controlecentrum. Het controlecentrum gebruikt alle binnengekomen informatie om correcties te berekenen en de constellatie te beheren. De informatie berekend in het controlecentrum wordt vervolgens weer naar de satellieten (ruimte segment) gestuurd. Met deze nieuwe informatie kunnen de navigatie berichten aangepast worden om gebruikers van zo accuraat mogelijke data te kunnen blijven voorzien.

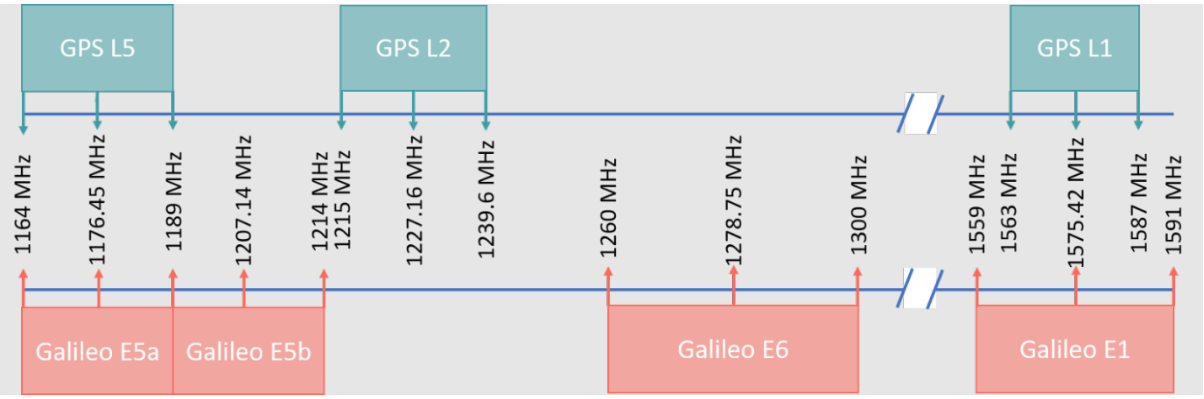


Figuur 3 Schematische weergave verschillende onderdelen van een GNSS constellatie

De constellaties bieden meerdere verschillende signalen. Naast dat iedere GNSS zijn eigen specificaties heeft, zijn er ook andere eigenschappen die voor onderscheid zorgen. Een eerste categorisering die van belang is voor de potentiële gebruiker is of een signaal versleuteld is of open is gesteld voor vrij civiel gebruik. De meeste constellaties zenden open signalen en beveiligdesignalen uit. De open signalen zijn bedoeld voor vrij gebruik, deze signalen zijn niet versleuteld met geheime sleutels en iedereen is vrij deze signalen te gebruiken. Deze open signalen worden bijvoorbeeld door telefoons gebruikt om positiebepaling uit te voeren. De beveiligde signalen zijn gecodeerde signalen die niet te lezen zijn zonder speciale sleutels en codes. Het gebruik van deze signalen wordt sterk gereguleerd, voorbeelden zijn het GPS P(Y) en het toekomstige GPS M-code signaal voor militair gebruik, en het Galileo PRS signaal voor gebruik door partijen in kritische sectoren die voor gebruik speciale toestemming hebben gekregen.

Daarnaast worden er signalen uitgezonden met verschillende draaggolf frequenties. Hoewel alle GNSS-signalen deel zijn van het L-band RF-spectrum, zijn er in deze L-band weer verschillende sub-banden gedefinieerd waarin GNSS-signalen mogen worden uitgezonden. In Figuur 4 de draaggolf frequenties van de GPS en Galileo signalen weergegeven. Zoals te zien worden er ook binnen een constellatie meerdere draaggolffrequenties gebruikt. Gebruik van verschillende draaggolf frequenties voor verschillende signalen vergroot niet alleen de weerbaarheid tegen interferentie (indien de interferentie in een deel van het frequentiespectrum plaatsvindt) maar maakt het ook mogelijk de ionosferische fout te berekenen en te compenseren. Het

frequentiespectrum wordt strak gereguleerd door de ITU (International Telecommunications Union), dit voorkomt interferentie tussen verschillende systemen.

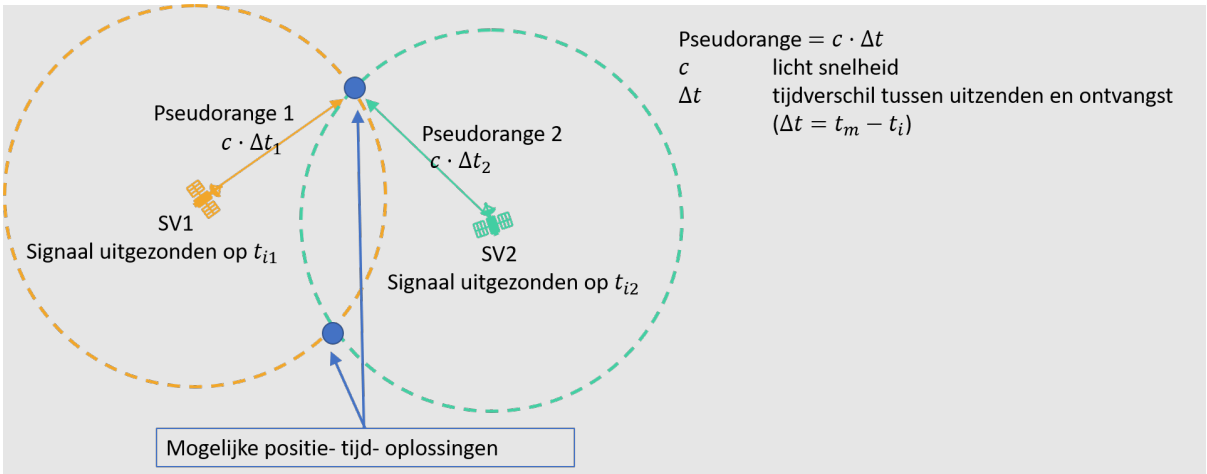


Figuur 4 Draaggolf frequenties van de GPS en Galileo signalen

Niet alle ontvangers kunnen zomaar gebruik maken van alle typen signalen. Daarom is het belangrijk om na te denken over welke signalen de gebruiker wel of juist niet wil gebruiken en een ontvanger uit te zoeken die aan deze gebruikersspecificaties voldoet. De meeste nieuwe commercieel beschikbare ontvangers zijn in staat met signalen van verschillende constellaties te werken. Ook multi-frequentie ontvangers zijn wijd beschikbaar.

Voor de uiteindelijke positie- en tijdbepaling wordt het principe van multilateratie gebruikt. Bij dit principe wordt "de afstand" naar een aantal satellieten gemeten. De afstand van gebruiker tot de satelliet is de zogenoemde pseudorange. Als de pseudorange van gebruiker tot meerdere satellieten bekend is en ook de locatie van de satellieten op het moment van de meting bekend is, kan er een stelsel van vergelijkingen gebruikt worden om de positie en tijd oplossing voor de gebruiker te vinden. Omdat een positie gedefinieerd wordt door een x- y- en z- coördinaat en ook de tijd onbekend is zijn er ten minste vier pseudorange metingen nodig om een oplossing te kunnen vinden. Hier komt dus ook het stukje "satelliet zichtbaarheid" terug. Om een succesvolle positie en tijd oplossing te kunnen vinden moeten er genoeg satellieten in beeld zijn. Voornamelijk in stedelijk gebied kan dit een probleem zijn door (hoge) gebouwen die de satelliet signalen blokkeren, het gebruik van meerdere satelliet constellaties kan hier een oplossing in zijn.

Het gebruik van meerdere constellaties voor het vinden van één positie-tijd-oplossing vereist dat er rekening gehouden wordt met het toevoegen van onbekende systeemtijdfouten aan de vergelijking. Dit betekent dat er boven op de 4 vereiste pseudorange metingen een extra pseudorange meting nodig is voor elke extra constellatie die gebruikt wordt.

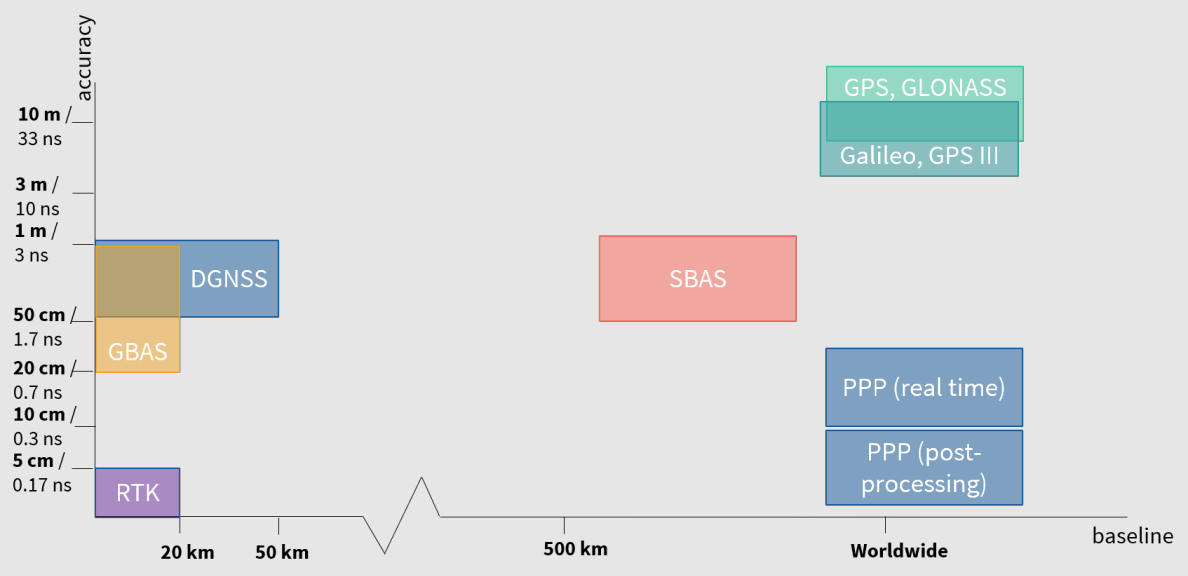


Figuur 5 Overzicht van werkingsprincipe

Het meten van pseudorange gebeurt natuurlijk niet met een meetlint. In plaats van een daadwerkelijke afstandsmeting te doen wordt er eigenlijk een tijdsmeting gedaan. De snelheid van

het licht wordt vervolgens gebruikt om deze tijdsmeting om te rekenen naar een afstand. Er zijn allerlei bronnen van fouten en onzekerheden die de accuraatheid van de tijdsmeting kunnen beïnvloeden, en doordat 1 nanoseconde (ns) verschil in tijdsmeting al overeenkomt met 30 cm verschil in pseudorange zijn kleine fouten in de tijdsmeting meteen van invloed op de uiteindelijke kwaliteit van de positie tijd oplossing. Bekende bronnen van fouten zijn fouten in de klok en ephemeris data, verschillen in propagatie snelheid door ionosfeer en troposfeer, en multi-path effecten veroorzaakt door de omgeving van de ontvanger.

Stand-alone GNSS, zoals hierboven besproken, biedt mogelijkheden om zonder voorkennis of hulp van andere systemen de positie en/of tijd oplossing met een nauwkeurigheid van ongeveer 10 m (of in termen van tijd 33ns) te bepalen. Voor steeds meer toepassingen is dit niet voldoende. Er bestaan verschillende augmentatie systemen die het gebruik van GNSS op gebied van integriteit en precisie kunnen ondersteunen. Een indicatie van de precisie die met gebruik van de verschillende augmentatie systemen behaald kan worden als een functie van het bereik van het augmentatie systeem is weergegeven in Figuur 6. Over het algemeen verbetert het gebruik van augmentatie systemen de precisie en integriteit van een positie tijd oplossing door specifieke correcties en integriteitsparameters aan de gebruiker door te geven. Het precieze werkingsprincipe verschilt per systeem.



Figuur 6 Augmentatie systemen en hun precisie

Bijlage G Toelichting dreigingen betreffende GNSS gebruik

In Figuur 2 in de hoofdtekst is een diagram met de verschillende bedreigingen in het gebruik van GNSS toegevoegd. In onderstaande tekst zijn deze bedreigingen verder toegelicht.

A. Gebruikerssegment

Het gebruikerssegment is het gedeelte waar een gebruiker van GNSS-systemen zelf invloed op uit kan oefenen. Bij onbetrouwbaarheid van de GNSS-positietijd oplossing is het daarom altijd nuttig te kijken of er in dit segment misschien oorzaken te identificeren zijn die de gebruiker zelf kan mitigeren.

A.1. Ontvanger

De ontvanger en de antenne zijn nodig om het GNSS-signaal uit de ruimte op te kunnen vangen, te kunnen lezen en om tot een uiteindelijke positie oplossing te komen. Omdat dit het apparaat is dat een gebruiker uiteindelijk de positie en tijd oplossing levert is het belangrijk ervan overtuigd te zijn dat het een betrouwbaar apparaat is dat de juiste operaties uitvoert. Hoewel GNSS als stand-alone systeem gebruikt kan worden, zijn er tegenwoordig veel ontvangers en systemen die ook in verbinding zijn met het internet of informatie verstrekt krijgen via andere bronnen (bijvoorbeeld de producent). Deze extra connecties kunnen kwetsbaarheden in het systeem introduceren voor bijvoorbeeld cyberaanvallen (direct op de ontvanger of op het overkoepelende netwerk) of foute externe informatie stromen (fouten in de extra informatie die gebruikt wordt om tot een “betere” positie tijd oplossing te komen). In de huidige maatschappij is het niet alleen belangrijk om naar de betrouwbaarheid en robuustheid van een systeem zelf te kijken, maar moet er ook rekening gehouden worden met wetgevingen. Zo kan het zijn dat het land waar een ontvanger geproduceerd is, of waar de database voor data verstrekking of collectie staat macht houdt over bepaalde delen van een systeem. De mogelijke ernst van deze kwetsbaarheid moet voor iedere kritieke toepassing overwogen worden.

A.2. Omgeving

Ook de omgeving van de ontvanger kan metingen beïnvloeden en verstoren. Zoals besproken in sectie 1.2 is het van belang dat er om tot een positie tijd oplossing te komen voldoende satellieten in het rechtstreekse gezichtsveld van de receiver zijn. Ongehinderd zicht naar de hemel is belangrijk voor zowel de precisie van de oplossing als voor de integriteit van de oplossing. Als GNSS gebruikt wordt in bijvoorbeeld bebouwd of bebost gebied worden de signalen van satellieten met een lage elevatie (deels) geblokkeerd. Hierdoor heeft de ontvanger beschikking over minder signalen, en is de geometrische verdeling van datapunten minder gespreid. Naast het blokkeren van signalen kunnen omgevingsobstakels ook zorgen voor reflecties. Deze reflecties kunnen ervoor zorgen dat een signaal indirect, met een extra vertraging, bij de ontvanger beland. De ontvanger meet op deze manier een te lange signaal propagatie tijd, en rekent daardoor met een te lange pseudorange. Dit zorgt voor mogelijke fouten en grote onzekerheden in de uiteindelijke positie tijd oplossing. Dit gereflecteerde signaal wordt een “multi-path” signaal genoemd. Doordat het multi-path signaal eigenlijk een vertraagde kopie is van het echte signaal is het heel moeilijk om onderscheid te maken tussen het echte signaal en de kopie. Als het directe signaal wel ontvangen wordt zullen alle latere kopieën die ontvangen worden een multi-path signaal zijn, maar als het directe signaal geblokkeerd wordt en de receiver niet bereikt kan een receiver het multi-path signaal voor een echt signaal aannemen.

Bij permanente GNSS-installaties, bijvoorbeeld voor monitoringstations of wanneer het GNSS-systeem alleen gebruikt wordt om de tijd op een bekende en vaste locatie te meten, kan er rekening gehouden worden met de ontvangst condities. Gezien deze installaties vaak voor langere tijd in gebruik blijven is het wel belangrijk om in de gaten te houden dat de antenne nog steeds op dezelfde plek staat en dat de omgevingscondities niet veranderd zijn. Voor mobiele GNSS-systemen is het moeilijker om rekening te houden met omgevingscondities. In de positie tijd oplossingen van mobiele systemen spelen fouten door omgeving dus ook een grotere rol.

B. Signal in Space

Zoals al eerder genoemd is het GNSS signaal dat van satelliet naar aarde propageert heel zwak, zo zwak zelfs dat het bij de ontvanger niet boven de gewone ruis uitkomt. Dit maakt het Signal in Space gevoelig voor verschillende soorten verstoringen. Verstoringen van het Signal in Space zijn op te splitsen naar 3 oorzaak groepen: moedwillig, onbedoeld en natuurfenomenen. Omdat de intentie van de verstoring anders is, is het nuttig dit onderscheid te maken. Dit kan helpen bij het oplossen van de verstoring of dreiging.

B.1. Moedwillige verstoringen

Bij moedwillige verstoringen veroorzaakt een derde partij expres een verstoring om ontvangst van het signaal onmogelijk te maken of om een ontvanger te voorzien van foute informatie. Interferentie door uitzenden van andere radiofrequentie signalen wordt ook wel Radio Frequent Interference" genoemd Dit kan ertoe leiden dat een gebruiker geen positie oplossing kan berekenen of tot een valse positie oplossing komt. De aanvallen kunnen uitgevoerd worden voor het eigen gewin van de verstoorder, maar kunnen ook gebruikt worden om algemene chaos te veroorzaken. De hoofdcategorieën moedwillige verstoringen zijn jamming en spoofing.

B.1.a. Jamming

Bij jamming wordt er een signaal geproduceerd van ongeveer dezelfde frequentie als de GNSS draaggolf. Dit jamsignaal is sterker dan het GNSS signaal zelf, en zorgt daardoor voor een verhoogde totale input power. Dit betekent dat het GNSS signaal relatief steeds minder bijdraagt aan de totale ontvangst. Daardoor wordt het voor een receiver steeds moeilijker om het echte GNSS signaal te kunnen detecteren, en op gegeven moment zal de receiver het GNSS signaal niet meer kunnen vinden. Er bestaan minder geavanceerde, brute force, jammers maar ook meer geavanceerde jammers die in de literatuur systematische jammers worden genoemd.

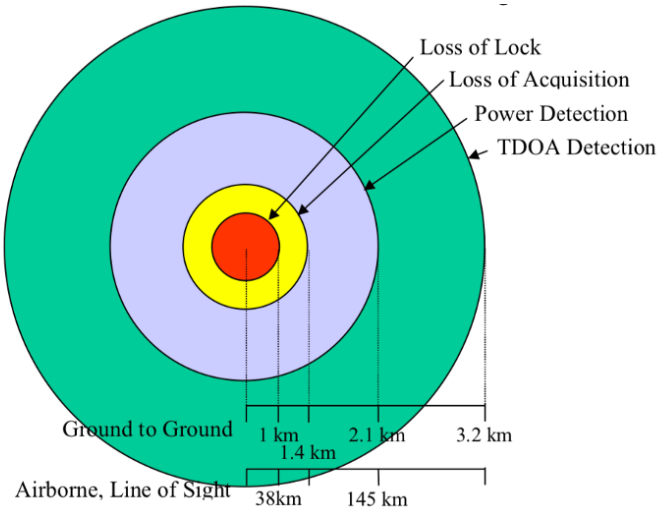
Brute-force jammers zijn veel voorkomend en eenvoudig te verkrijgen. Dit type jammers produceert een krachtig hoog vermogen signaal waardoor het echte GNSS signaal niet meer door de ontvanger gedetecteerd kan worden. Het jammer signaal kan gemoduleerd zijn om effectiever te kunnen storen. Hiervoor bestaan verschillende modulatie patronen. Het effectieve bereik van dit type jammer hangt voornamelijk af van het uitgezonden vermogen. Er bestaan goedkope low-end jammers van usb stick formaat die GNSS ontvangst binnen een straal van ongeveer 10 m verstoren, maar ook hele sterke jammers die GNSS ontvangst binnen een straal van 100 km kunnen verstoren. Het hoge vermogen en het karakteristieke frequentiepatroon, kunnen gebruikt worden om het jamsignaal te kunnen detecteren en tot in zekere mate kunnen mitigeren.

Een meer systematisch type van jamming: Een systematische jammer produceert een verstoring die niet continu aanwezig is; het stoorsignaal wordt onregelmatig uitgezonden met meestal een laag vermogen. Het gevolg hiervan is dat deze systematische jammers moeilijk zijn op te sporen. Het stoorsignaal is dusdanig getimed dat het wordt uitgezonden wanneer het satellietsignaal voor de ontvanger essentiële informatie bevat. Op deze manier wordt de ontvanger gehinderd om de juiste positie- en tijdsinformatie te leveren. Het construeren van een systematische jammer vergt meer inspanning dan eenvoudige jammer, maar dankzij de beschikbaarheid van *Software Defined Radio* (SDR) technologie en informatie op het internet is het ontwerp en de constructie van dit type jammer binnen handbereik van een grote groep geïnteresseerden gekomen. Omdat de effecten van systematische storing op het gedrag van de ontvanger zo subtiel zijn, is het niet altijd duidelijk dat het falen van de ontvanger moet worden toegeschreven aan systematische storing. De reikwijdte van een systematische stoorzender is beperkt omdat, in het algemeen, het vermogen van de zender relatief laag is.

De grootte van het gebied waarbinnen de ontvangers last hebben van de jammer is afhankelijk van het vermogen. Om hierin enig inzicht te verkrijgen is het van belang de functies van het verwerven (*acquisition*) van een (nieuw) satellietsignaal en het volgen (*tracking*) van een satellietsignaal te onderscheiden. De GNSS-satellieten maken een baan om de aarde; dit betekent dat een satelliet zich eerst onder de horizon bevindt – de signalen zijn dan niet te gebruiken voor een ontvanger, dan komt de satelliet op –de signalen kunnen dan gebruikt worden voor positie- en tijdbepaling, en na verloop van tijd gaat de satelliet weer onder –de ontvanger zal dan het contact verliezen. Bij het opkomen van de satelliet zal de ontvanger eerst het signaal moeten verwerven. Daarna zal, zolang de satelliet zichtbaar is het signaal worden gevolgd. Het proces van verwerven is gevoeliger voor stoorsignalen dan het proces van tracking. Om de aanwezigheid en de locatie van een jammer te bepalen kunnen verschillende methoden worden gebruikt. Zo kan gebruik worden gemaakt van een monitoring systeem dat het ontvangen vermogen van het stoorsignaal bepaalt (*power detection*), en van een systeem bestaande uit meerdere antennes. Door de verschillen in de gemeten fasen van het stoorsignaal bij de verschillende antennes is het mogelijk om de richting van het stoorsignaal te bepalen. (*Time Difference of Arrival*, TDOA).

Het volgende Figuur 7 geeft inzicht in het gebied waarbinnen het effect van een jammer op een GNSS-ontvanger merkbaar is. In dit plaatje wordt het effect getoond van een jammer met een vermogen van 4W. Hierbij wordt ook nog onderscheid gemaakt tussen een jammer die op de grond is geplaatst en een die zich in de lucht bevindt. Deze laatst genoemde positie heeft een veel verdere reikwijdte dan die op de grond. Het verschil in "Loss of Lock" (het satelliet signaal kan niet meer gevolgd worden) versus "Loss of Acquisition" (het satellietsignaal kan niet verworven

worden) is ook aangegeven: Voor het verwerven van een satelliet heeft de ontvanger een sterker satellitietsignaal nodig dan voor het volgen van een signaal. Verder is te zien dat voor de lokalisatie van een jammer een multi-antenne-systeem met een zwakker jamming-signaal kan functioneren dan een gebaseerd op het meten van vermogen.



Figuur 7 received J/S as a function of distance from the jammer

B.1.b. Spoofing

Bij spoofing wordt er een vals signaal geproduceerd dat wel de karakteristieken van een echt GNSS-signaal heeft, maar onjuiste PNT-informatie bevat. De spoofersignalen zijn moeilijk te herkennen en kunnen dus wel door ontvangers "gelezen" worden. Het bepalen van de positie-tijd oplossing op basis van de gespoofte signalen resulteert echter in een foute oplossing. Spoofer attacks kunnen op verschillende manieren opgebouwd worden. In het algemeen zijn ze het moeilijkst te herkennen als het vermogen van het signaal net iets hoger of vergelijkbaar is met het vermogen van het echte GNSS-signaal en de valse informatie langzaam wegloopt van de echte informatie. Dit maakt het namelijk moeilijk om het signaalvermogen of discontinuïteiten te gebruiken als eigenschappen om nepsignalen te herkennen en weg te filteren. Vaak gaat een spoofing aanval gepaard met een korte jamming aanval. Door de jamming aanval kan de ontvanger de echte GNSS-signalen niet meer volgen, en nadat de jamming aanval is afgelopen ziet de ontvanger als eerst de net iets sterkere gespoofte signalen. Hoewel spoofing attacks gecompliceerder zijn om uit te voeren dan jamming attacks, maakt de beschikbaarheid van SDR-technologie het voor partijen met enige kennis op het gebied van signalen wel mogelijk om succesvolle aanvallen op te zetten. Geavanceerde spoofing aanvallen worden op dit moment echter nog voornamelijk in het militaire domein gezien.

B.2. Onbedoelde verstoringen

Niet alle kunstmatige verstoringen zijn altijd moedwillig of uitgezonden met kwade intenties. Er kunnen ook per ongeluk interferenties plaatsvinden.

B.2.a. Interferentie andere systemen

Bekende bronnen van onbedoelde interferentie zijn GNSS repeaters. Dit zijn systemen bedoeld om GNSS-signalen ook in GNSS-denied gebied, bijvoorbeeld binnen, beschikbaar te maken. GNSS repeaters zenden met een kleine vertraging een kopie van een ontvangen signaal uit. Als een GNSS repeater signalen verstuurt in een omgeving waar het directe GNSS-signaal ook beschikbaar is, kan er interferentie tussen deze twee signalen plaats vinden.

Door de grote dichtheid van gebruik van frequenties rond de GNSS-draaggolffrequenties kunnen er ook interferenties ontstaan met systemen opererende op aangrenzende frequenties. Kleine fouten of defecten in apparatuur kunnen er voor zorgen dat de zendfrequentie opschuift of dat er een harmonische of intermodulatie component van het signaal in het GNSS-frequentie gebied terecht komt. Dit type interferentie heeft niet de kenmerken van het GNSS-signaal, en zou dus gezien kunnen worden als een vorm van onbedoeld jammen.

B.3. Natuur

Ook natuurlijke fenomenen kunnen voor verstoringen van het Signal in Space zorgen. Hoewel het bekend is dat bijvoorbeeld vulkaanuitbarstingen en grote bosbranden kleine effecten op de ionosfeer en daarmee ook de ontvangen GNSS-signalen kunnen hebben, is het voornamelijk zonneactiviteit dat een grote rol speelt.

B.3.a. Ruimteweer en Ionosfeer

De zon beïnvloed onze aarde en haar atmosfeer op verschillende manieren die het gebruik van GNSS mogelijk kunnen verstoren. De belangrijkste fenomenen zijn a) variaties in het electronengehalte van de ionosfeer en ionosferische scintillaties, b) geomagnetische stormen, c) solar radiation stormen, d) radio blackouts.

De verschillende soorten verstoringen hieronder uitgelegd worden bestudeerd en gemonitord door NOAA. Zij classificeren verstoringen ook aan de hand van een aantal schalen. Elk type verstoring heeft een eigen schaal[42]. In deze schalen worden meetwaardes gekoppeld aan ernst van gevolgen en frequentie per zonnecyclus.

Ionosfeer en scintillaties

Het eerst effect dat genoemd is, de ionosferische variaties en scintillaties. De ionosfeer zorgt voor een vertraging van het electromagnetisch signaal, waardoor er een fout ontstaat in de tijdsmeting tussen uitzenden en ontvangst. Ook zorgt de ionosfeer voor afbuiging van het signaal (denk aan zichtbaar licht dat door een prisma gestuurd wordt), en kan er in extreme gevallen zelfs reflectie plaatsvinden. De ionisferische effecten zijn vooral sterk aanwezig in de poolgebieden en rond de evenaar. Rond de evenaar kan het effect van de ionosfeer zo sterk zijn dat ontvangers het satellietsignaal niet meer kunnen interpreteren en daardoor geen GNSS meting kunnen doen. Ionosferische scintillaties en effecten zijn over het algemeen goed bekend bij operators die in kwetsbare regio's opereren. Lokale variaties, en in het bijzonder scintillaties, blijven echter moeilijk te voorspellen. Voor Nederland spelen ionosferische effecten in het bijzonder een rol in de Caribische regio.

Geomagnetische storm

Een geomagnetische storm is een tijdelijke verstoring van de magnetosfeer van de aarde. Deze verstoringen worden veroorzaakt door efficiënte energie-uitwisselingen tussen de zon en het magneetveld van de aarde. Energie-uitwisseling kan plaats vinden door verstoringen aan het oppervlak van de zon die veranderende magnetische velden veroorzaken. Een voorbeeld van een heftige verstoring is bijvoorbeeld een Coronal Mass Ejection (CME). Hierbij wordt een grote hoeveelheid plasma van de zon de ruimte in geschoten. CMEs zijn de veroorzakers van de grootste geomagnetische stormen. Als een CME plaatsvindt, en het plasma wordt richting de aarde geschoten kan dit behalve een hevige geomagnetische storm ook andere onwenselijke gevolgen hebben. Als de geladen het plasma van de CME de magnetosfeer van de aarde bereikt spreekt men ook van een Solar Radiation Storm. Geomagnetische stormen worden geschaald naar een Kp indexcijfer.

Solar radiation storm

Een solar radiation storm is, hoewel gerelateerd, een ander verschijnsel dan een geomagnetische storm. Waar bij een geomagnetische storm energie wordt overgedragen aan de magnetosfeer van de aarde via veranderende magnetische velden, is er bij een solar radiation storm sprake van geladen deeltjes die de magnetosfeer van de aarde binnenkomen. Deze energetische geladen deeltjes kunnen in elektronica voor schade en kortsluiting zorgen, daarom is een solar radiation storm een gevaar voor bijvoorbeeld satellieten in de ruimte. Zodra de geladen deeltjes de magnetosfeer bereikt hebben worden ze gestuurd door de magnetische velden van de aarde. De gebieden rond de noord- en zuidpool zijn hierdoor het meest kwetsbaar voor de gevolgen. Solar radiation storms worden gemeten als het aantal geladen deeltjes (flux) met een energie groter dan 10 MeV dat de magnetosfeer weet binnen te dringen.

Radio Black-out

Bij een radio black-out produceert de zon tijdelijk een verhoogde hoeveelheid radiogolven. De geproduceerde straling komt daardoor boven de achtergrondstraling uit, en zorgen ook voor een verstoord spectrum van de signalen en straling te ontvangen op aarde. Wanneer de radiogolven

[42] NOAA Space Weather Scales | NOAA / NWS Space Weather Prediction Center

geproduceerd tijdens een radio black-out zich in hetzelfde deel van het spectrum bevinden als de GNSS signalen, zorgt dit voor een natuurlijke bron van jamming. De GNSS signalen kunnen niet meer gedetecteerd worden onder het verhoogde niveau van ruis. Radio Black-outs worden geclassificeerd aan de hand van piek emissie.

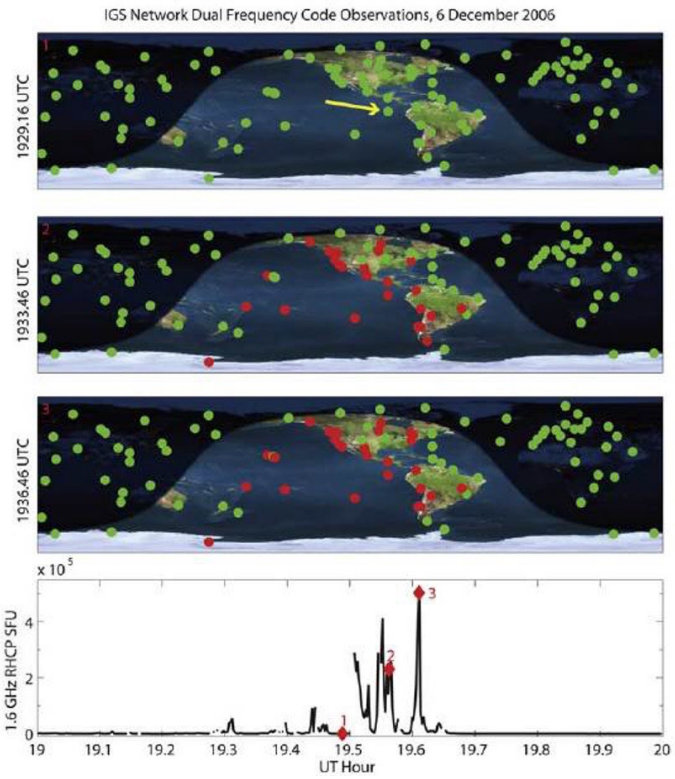
C. Ruimtesegment

Ook het ruimtesegment kan blootgesteld worden aan dreigingen die de betrouwbaarheid en continuïteit van het systeem aan kunnen tasten.

C.1. Natuur/Ruimteweer

Ruimteweer is al besproken als dreiging en verstoring voor het signal in space. In extreme gevallen van coronale massa uitstoot en deeltjesstormen kunnen echter ook de satellieten zelf aangetast worden. Dit kan voor één satelliet gebeuren, maar de kans is groot dat meerdere satellieten tegelijkertijd aangetast worden. De hoogenergetische geladen deeltjes kunnen zich door het schild van de satellieten heen boren en voor grote spanningsverschillen zorgen in de elektronica. Hierdoor kan kortsluiting ontstaan, en deze kortsluiting kan de elektronica aan boord beschadigen en defect maken. Geladen deeltjes en straling kunnen overigens ook tijdelijk de signalen in elektronische systemen beïnvloeden. Hierdoor kunnen verkeerde elektronische signalen uitgezonden worden, en ook dit kan systeemfouten veroorzaken.

In B.3.a. is besproken dat de zon als een interferentiebron (via een SRB) gezien kan worden en de ontvangst van het satellietsignaal door een ontvanger danig kan storen. De effecten van deze SRB's kunnen behoorlijk ernstig kunnen zijn. Hoewel de meest extreme gevallen zeer zeldzaam zijn, kan de omvang groot zijn. Extreme SRB-gebeurtenissen kunnen een signaal uitzenden met een vermogen van maximaal 10^8 zonnestroomeenheden (of *solar flux unit*, of kortweg sfu). De volgende afbeelding toont de spreiding van GNSS-ontvangers die werden getroffen door "slechts" een ernstige burst op 6 december 2006 (tot 10^5 sfu). De informatie die in de figuur is weergegeven is de storing op ontvangers van het IGS-netwerk (International GNSS-Service; een wereldwijd netwerk van referentie-ontvangers) over de tijd gezien. Deze ontvangers zijn allemaal van zeer goede kwaliteit en uitgerust met functionaliteit om storingen op te vangen. Normale gebruikersontvangers zullen vaak meer last hebben van zo'n storing omdat zij met minder storingsmitigatie-functionaliteit zijn uitgerust. Zoals opgemerkt, de storing van 6 December 2006 was alleen een ernstige burst, de gevolgen van een extreme gebeurtenis zullen alleen nog maar ernstiger zijn.



In de Figuur 8 hiernaast wordt de impact van een SRB over de tijd weergegeven. In de grafiek (onderaan) is de sterkte van de SRB (in sfu) over de tijd weergegeven; in elk van de drie wereldkaartjes wordt geografische impact van de burst weergegeven –de rode stippen zijn ontvangers die dusdanig worden gestoord dat ze niet meer functioneren. Het bovenste kaartje geeft de situatie op tijdstip #1 weer: Er is dan nog geen SRB merkbaar en alle ontvangers werken normaal. Het tweede kaartje (tijdstip #2) is de kracht van de SRB zo'n 2 10^5 sfu en overal in het gebied op aarde, dat door de zon wordt beschenen, zijn er ontvangers die niet normaal kunnen functioneren. In het derde kaartje (tijdstip #3) is de kracht van de SRB zo'n 5 10^5 sfu, en het aantal gestoorde ontvangers is alleen maar toegenomen. Merk verder op dat een extreme SBR een kracht heeft in de orde van 10^8 sfu (drie ordes krachtiger dan de situatie zoals hier beschreven).

Figuur 8 Impact van een SRB over de tijd

C.2. Technisch falen

Een onderdeel van een satelliet kan natuurlijk ook gewoon stuk gaan. Hoewel er bij het ontwerp van satellieten al rekening gehouden wordt met technisch falen, en er vaak back-up systemen aanwezig zijn kan het toch gebeuren dat een satelliet tijdelijk of permanent geteisterd wordt door technische problemen. Dit kan variëren van een kapotte atoomklok tot een verkeerde baan om de aarde. Technisch falen beïnvloedt in principe 1 satelliet, en bij een goed gevulde constellatie zijn er voldoende andere satellieten aanwezig om datavoorziening via de kapotte satelliet (tijdelijk) uit te kunnen zetten.

D. Grondsegment

Het grondsegment is als het ware het controlesysteem voor de hele constellatie. Hier wordt de operatie van de gehele constellatie gemonitord en waar nodig gestuurd. Een belangrijk onderdeel van het SiS zijn de correctie-gegevens die worden meegestuurd. Het grondsegment berekent op basis van een wereldwijd netwerk van referentieontvangers wat de exacte waarden van de correcties moeten zijn. Deze waarden worden met regelmatige tussenpozen naar de satellieten opgestuurd zodat een ontvanger altijd kan beschikken over actuele correcties. Fouten, dreigingen en verstoringen in het grondsegment werken daarom door in het hele systeem.

D.1. Systeemfouten

Het grondsegment is een complex systeem waar veel hardware systemen en softwareprogramma's samenwerken om de constellatie zo optimaal mogelijk te laten opereren. Toch kan het voorkomen dat er ergens in dit systeem iets fout gaat, ofwel door menselijk handelen (bijvoorbeeld het laden van verkeerde configuratie data) of door een fout in het systeem zelf (bijvoorbeeld een softwarefout. Hierdoor kan het voorkomen dat een of meerdere satellieten geladen worden met foutieve data en waardoor een verkeerd signaal wordt uitgezonden. Vaak worden deze fouten snel opgespoord door de vele referentiestations op aarde. Meestal is binnen een dagdeel de fout bekend en opgelost.

Een meer drastische fout is als door een systeemfout het gehele grondsegment van een constellatie in een inoperabele status gebracht wordt. Alle satellieten van die constellatie zullen dan niet meer werken.

D.2. Cyberaanvallen

Ook cyberaanvallen kunnen een bedreiging vormen voor het grondsegment. Omdat het grondsegment de controle heeft over de gehele constellatie kan met een cyberaanval in het slechtste geval een gehele constellatie overgenomen worden of onbruikbaar gemaakt worden. Als gebruiker is er weinig te doen tegen eventuele aanvallen op het grondsegment. Wel heeft een gebruiker bij sommige ontvangers misschien de mogelijkheid om ervoor te kiezen bepaalde constellaties tijdelijk niet te gebruiken.

Bijlage H Potentieel kwetsbare systemen zoals genoemd in de deep-dives

De systemen die de GNSS-tijdsinformatie gebruiken hebben hoge eisen aan de stabiliteit van een interne klok; de tijd tussen elke puls van de klok moet namelijk altijd precies even duren. Voor dit soort systemen wordt het GNSS-signaal niet direct gebruikt als tijdssignaal, maar het GNSS-signaal wordt gebruikt om de interne klok extra stabiliteit te geven. De hoge klokstabiliteitseisen worden voornamelijk geëist bij systemen die op een hoge frequentie moeten opereren, of waarbij een meetactie met exact even lange tussenpozen moet worden herhaald.

Potentieel kwetsbaar systeem	**GNSS Functie [Positie | Tijd]**	**Reden kwetsbaarheid**	**Aantal keer genoemd in deep-dives**	**Back-up systeem genoemd**
Telecommunicatie/ draadloos netwerk	Tijd	Synchronisatie van de verschillende onderdelen van de communicatieapparatuur maakt gebruik van het GNSS-tijdssignaal	3x	Alternatieve stabiele tijdsbron in combinatie met computer-netwerk protocol om precisie tijdsinformatie over te kunnen brengen (*) (1x genoemd)
Digitaal observatiesysteem (bijvoorbeeld een radar) met hogesnelheids-componenten, eventueel fysiek gedistribueerd uitgevoerd	Tijd	Synchronisatie van de verschillende componenten van het observatiesysteem maakt gebruik van het GNSS-tijdssignaal De frequentie van de hogesnelheidscomponenten ligt typisch in de orde van enkele GHz-en	1x	Niet genoemd
Digitaal control systeem met hogesnelheids-componenten	Tijd	Het control system heeft een interne klok dat wordt gesynchroniseerd met het GNSS-tijdssignaal Nauwkeurigheid van de klok van het control system moet in de orde van 1 microseconde zijn	1x	Alternatieve stabiele tijdsbron in combinatie met computer-netwerk protocol om precisie tijdsinformatie over te kunnen brengen (*) (1x genoemd)

Potentieel kwetsbaar systeem	GNSS Functie [Positie | Tijd]	Reden kwetsbaarheid	Aantal keer genoemd in deep-dives	Back-up systeem genoemd
Event-logging systeem	Tijd	De tijdsinformatie behorend bij de beschrijving van de events wordt afgeleid van het GNSS-tijdssignaal Nauwkeurigheid moet in de orde van 1 microseconde zijn	1x	Alternatieve stabiele tijdsbron in combinatie met computer-netwerk protocol om precisie tijdsinformatie over te kunnen brengen (*) (1x genoemd)
Besturingssysteem autonoom voertuig	Positie	Robuustheid van de positie informatie tegen jamming en spoofing	1x	Als mogelijkheid werd een ranging systeem gebaseerd op radio-technologie genoemd (**)
Specifieke navigatiesystemen	Positie	Robuustheid van de positie informatie tegen jamming en spoofing	1x	Als mogelijkheid werd "detectie van jamming en spoofing" en een crypto-beveiliging zoals PRS genoemd (**)

(*) = Dit back-up systeem wordt op dit moment geïmplementeerd.

(**) = Dit back-up systeem is nog niet geïmplementeerd of staat nog niet op de planning om geïmplementeerd te worden.

Deze lijst van potentieel kwetsbare systemen komt overeen met in de literatuur beschreven kwetsbaarheden (zie bijvoorbeeld Widomski et al. En ATIS 2016,)[43].

[43] T. Widomski, K. Borgulksi, J. Uzhychi, P.Olbrysz, J. Kowalksi, Faults of Synchronization Based On GNSS Receivers and Ethernet NTP/PTP Network. Robust Synchronization & CyberSecrity In Critical Infrastructures – Energetics & Smart Grids. 2018

Bijlage I Voorbeelden mitigerende maatregelen

Maatregel	Mitigatie	Voordeel
Smart Antenna, of CRPA (Controlled Reception Pattern Antenna)	Detecteert en blokkeert de ongewenste jamming (en spoofing) signalen	Antenne kan zelfs bij zware jamming de correcte satellietsignalen gebruiken
Jamming en spoofing detectie-units (soms Firewall genoemd) welke geplaatst wordt tussen de bestaande GNSS-antenne en -ontvanger	Detecteert jamming en spoofing	Geeft waarschuwingen bij jamming/spoofing. Deze units worden soms ook met een atoomklok uitgevoerd dat als alternatief kan dienen als bron voor tijdsinformatie[44]
GNSS ontvanger met detectie-mogelijkheden in frontend	Detecteert jamming en spoofing	Geeft waarschuwingen bij jamming/spoofing. Heeft een alternatieve PNT-bron nodig
Gebruik maken van een beveiligd signaal (PRS of M-code)	Gebruik maken van een beveiligd signaal wat met de huidige technologische kennis niet gespoofed kan worden	Sterkste bescherming tegen spoofing
Dual frequentie	Gebruik maken van frequenties die niet gejammed worden	Betere bescherming tegen jamming; verstoren van meerdere frequenties is complexer en duurder. Daarnaast accuratere positie en tijdsbepaling door betere ionisferische vertragings-compensatie
Multi-constellatie ontvanger	Gebruik maken van constellaties die niet gespoofed worden	Betere bescherming tegen spoofing; spoofen van meerdere constellaties is complexer en duurder
Positioning using signals of opportunity (bijv. 5G)	Herkennen en mitigeren van GNSS verstoringen	Alternatief/ back-up-systeem voor positiebepaling
Sensor fusion	Herkennen en mitigeren van GNSS verstoringen.	Alternatief/ back-up-systeem voor positiebepaling
Alternatieve tijdsbasis (atoomklok) ter vergelijking met de door de ontvanger geleverde tijdsinformatie	Herkennen van een GNSS verstoring en een alternatieve bron voor tijdsinformatie	Alternatief/ back-up-systeem voor tijdsinformatie
Veerkrachtige GNSS-ontvanger	Herkennen en mitigeren van GNSS verstoringen	Deze ontvangers zijn instaat om autonoom weer in een nominale mode te geraken na een aanval.

[44] Zie bv: https://www.gps-world.biz/products/bluesky-gnss-firewall
https://www.accubeat.com/product-item/time-firewalltm/

Bijlage J Samenstelling interdepartementale begeleidingsgroep

Organisatie	**Directie**
ANWB	
De Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)	
Ministerie van Onderwijs, Cultuur en Wetenschap	
Ministerie van Infrastructuur en Waterstaat	DGWB
Ministerie van Infrastructuur en Waterstaat	DGLM
Ministerie van Infrastructuur en Waterstaat	DGMO
Ministerie van Infrastructuur en Waterstaat	DGMI
Ministerie van Infrastructuur en Waterstaat	FIB
Ministerie van Economische Zaken en Klimaat	
Ministerie van Defensie	
Ministerie van Justitie en Veiligheid	
Ministerie van Landbouw, Natuur en Voedselkwaliteit	
Rijkswaterstaat	CIV
Rijkswaterstaat	BS
Luchtverkeersleiding Nederland (LVNL)	
Het Netherlands Space Office (NSO)	

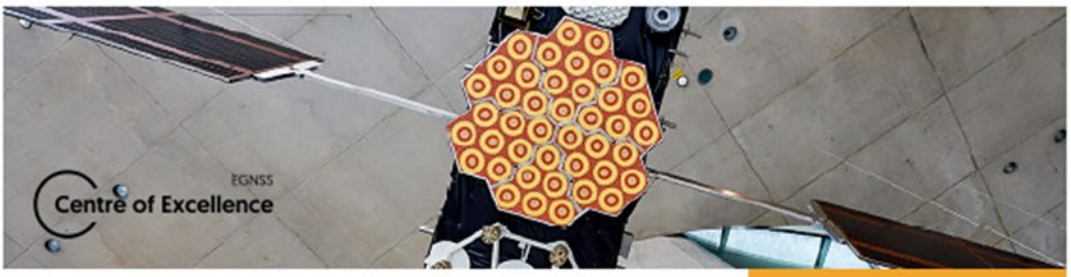
Bijlage K Begrippen en afkortingen

Afkortingen	
AIS	Automatisch Identificatie Systeem
AT	Agentschap Telecom
BCP	Business Continuity Planning
BZK	Ministerie van Binnenlandse zaken en Koninkrijksrelaties
CAET	Capaciteitsanalyse Elektriciteit en Telecom
DMO	Direct Mode Operations
EZK	Ministerie van Economische Zaken en Klimaat
GLONASS	GLObalnaya NAvigatsionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
IenW	Ministerie van Infrastructuur en Waterstaat
ICAO	International Civil Aviation Organization
IKUS	Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie
LVNL	Luchtverkeersleiding Nederland
NRB	Nationale Risicobeoordeling
NTP	Network Time Protocol
PNT	Plaatsbepaling, navigatie en tijdsbepaling
PRN	Pseudo Random Number
PRS	Public Regulated Service
TETRA	Terrestrial Trunked Radio
TLP	Traffic Light Protocol
VenJ	Ministerie van Veiligheid en Justitie
VMS	Vessel Monitoring System
VN	Verenigde Naties
WOB	Wet openbaarheid van Bestuur

Begrippen	
BeiDou/COMPASS	Chinees GNSS
Galileo	Europees GNSS
Global Navigation Satellite Systems	Global Navigation Satellite System (GNSS) verwijst naar het systeem inclusief grondsegment en een constellatie van satellieten die vanuit de ruimte signalen uitzenden die plaats- en tijdsbepalingsgegevens doorgeven aan GNSS-ontvangers..
Global Positioning System (GPS)	Amerikaans GNSS

Begrippen	
GLObal'naya NAvigatsionnaya Sputnikovaya Sistema (GLONASS)	Russisch GNSS
Loss of Acquisition	Het signaal van een satelliet kan niet verworven worden door de GNSS ontvanger. Het signaal bevat de identificatie, een Pseudo Random Number (PRN), van de satelliet en de ontvanger moet het deze identificatie herkennen om gebruik te maken van de data dat onderdeel is van het satellietsignaal. Het verwerven van het signaal komt overeen met het herkennen van de identificatie.
Loss of Lock	Het satellietsignaal kan niet meer gevolgd (Engels: tracking) worden door de GNSS ontvanger. Om het signaal goed te volgen moet de ontvanger het satellietsignaal in de greep houden (Engels: lock). Ook hier (net zoals bij het verwerven van een signaal) wordt de PRN om het signaal te volgen. Als een verstoring op het signaal de ontvanger de greep op het signaal verliest is dit een "Loss of Lock".
Navigatie	Het vermogen om de huidige en gewenste positie (relatief of absoluut) te bepalen en correcties toe te passen op koers, oriëntatie en snelheid om overal ter wereld een gewenste positie te bereiken.
Public Regulated Service	De Galileo Public Regulated Service (PRS) is een versleutelde navigatiedienst voor door de overheid geautoriseerde gebruikers en gevoelige toepassingen die een hoge continuïteit vereisen.
Plaatsbepaling	Bij plaatsbepaling wordt de locatie van een GNSS-ontvanger berekend met behulp van het GNSS-signaal.
PNT	PNT staat voor Positiebepaling, Navigatie en Tijdsbepaling.
Tijdsbepaling	De GNSS-satellieten zenden een zogenaamde navigatieboodschap uit. Eén van de dingen die hierin staan is een hoognauwkeurige tijdsboodschap. Dit tijdsignaal wordt gegenereerd door een groep atoomklokken. Het GNSS-signaal kan dus gebruikt worden als tijdwaarneming of om processen op verschillende locaties te synchroniseren in de tijd.

Bijlage L Nieuwsbrieven



Welkomstwoord Mark

IKUS-II Nieuwsbrief 1

In deze nieuwsbrief kijk ik graag terug op 4 succesvolle masterclasses die we hebben gehouden in de maand april. Aan deze online masterclasses hebben ruim 30 mensen deelgenomen van organisaties uit diverse sectoren zoals luchtvaart, scheepvaart, water management, energie distributie, defensie en klimaatdiensten. Gebleken is dat het kennisniveau van het gebruik en de eventuele kwetsbaarheden met betrekking tot de toepassing van GNSS per organisatie sterk varieert, voor Defensie bijvoorbeeld is dit essentiële technologie terwijl een andere organisatie gebruik maakt van toepassingen waarin GNSS technologie meer 'verborgen onder de motorkap' is. De masterclasses zijn dan ook afhankelijk van het kennisniveau (en de groepsgrootte) in twee varianten qua technische diepgang aangeboden. Naast dat deze masterclasses hebben voorzien in het verhogen van het kennisniveau heeft met name ook de gezamenlijke interactie bijgedragen aan vergroting van het netwerk en bewustzijn van de afhankelijkheden tussen organisaties. Veel praktijkvoorbeelden, inzichten en verschillende invalshoeken vanuit de verschillende organisaties heeft bijgedragen aan een open dialoog (en sfeer) over een vertrouwelijk onderwerp zoals de kwetsbaarheid van GNSS is. Met de masterclasses heeft het onderwerp ook een 'gezicht' gekregen wat heeft gezorgd voor diverse aanmeldingen voor een verdiepende risicoanalyse en toename van de beantwoording van de questionnaire (de questionnaire is tot 25 juni in te vullen via deze link). Twee andere belangrijke onderdelen van het IKUS2 onderzoek!

Mark Hartman, Onderzoeksleider IKUS-II

Deze nieuwsbrief zal de volgende onderwerpen belichten:

- Een beetje meer tijd voor tijd
- GNSS markt rapport
- NAVISP industry days
- Verstoringen in het nieuws

In deze en de aankomende nieuwsbrieven zullen verschillende GNSS onderwerpen belicht worden waar extra vragen of interesse in is getoond tijdens de masterclasses. Mocht er een onderwerp missen of vragen zijn, stuur dan gerust een mailtje naar info@gnss-coe.eu.

Een beetje meer tijd voor tijd

GNSS is niet alleen belangrijk voor toepassingen die afhankelijk zijn van nauwkeurige en constant beschikbare positie-informatie, ook tijdafhankelijke systemen zijn vaak afhankelijk van door GNSS geleverde informatie. Voorbeelden van toepassingen zijn te vinden in de energiesector (synchronisatie elektriciteitsnet, netwerkbewaking, automatische beveiliging), de financiële markt (tijdstempels voor transacties), cellulaire netwerken (tijdsynchronisatie, frequentienauwkeurigheid, faseafstemming van GSM-diensten mobiel internet) en andere telecom- en IT-systemen (NTP-netwerktijdsprotocol, PTP-precisietijdsprotocol).

Het gebruik van GNSS voor tijdwaarnemingen of synchronisatietoepassingen heeft een aantal voordelen ten opzichte van het gebruik van meer conventionele lokale klokken. Aan boord van GNSS-satellieten worden hoogwaardige (atomaire) klokken gebruikt om de tijd te bepalen en een nauwkeurige puls te produceren. Deze hoogwaardige klokken zijn zeer kostbaar en kunnen daarom niet in elke timingafhankelijke toepassing lokaal worden geïmplementeerd. Bovendien hebben alle individuele klokken kleine afwijkingen. De klokken aan boord van de satelliet worden zeer nauwlettend in de gaten gehouden door een hoofdcontrolestation op aarde, en correcties worden naar de satelliet gestuurd. Aangezien alle satellietklokken binnen een constellatie aan één systeemtijd zijn gekalibreerd, verstrekken alle satellieten gesynchroniseerde tijdsinformatie en kan de gebruiker hiermee synchroniseren. Voor dit soort toepassingen zijn speciale tijdontvangers beschikbaar. Deze timingontvangers geven niet alleen de ontvangen navigatieberichten en observaties door, maar leveren ook een 1 puls per seconde signaal en een klokfrequentiesignaal met hoge nauwkeurigheid.

Zoals uitgelegd zijn de satellieten binnen een constellatie alle gekalibreerd aan de hoofdklok van de constellatie. De systeemtijd van de constellatie is niet noodzakelijkerwijs hetzelfde tijdskader als UTC (de universele tijdcoördinaat waarin de tijdzones zijn gedefinieerd), en kan voor de verschillende constellaties verschillend zijn. De verschillen tussen de verschillende tijdskaders zijn echter bekend, en kunnen dus worden gecompenseerd.

Uitdaging GPS Roll-over

Voor GPS begon de systeemtijd (GPST) op 5 en 6 januari 1980 om 0 uur UTC. Hiervandaan wordt er in het navigatiebericht geteld hoeveel weken sindsdien zijn geweest. Door de beperkte aantal bit beschikbaar (10 binaire cijfers) voor de weeknummers schrijft het bericht een maximum weeknummer van 1024 voor. Daarom hebben in 1999 en 2019 zogenoemde roll-overs plaatsgevonden. Effectief werd hierdoor de tijd (weeknummer) weer op 0 gezet. Hoewel de rollover zelf niet noodzakelijk problematisch is voor het GPS-systeem, kunnen niet alle producten en software die gebruik maken van GNSS (in dit geval GPS) correct omgaan met de weeknummer rollover. De rollover die in 2019 plaatsvond, zorgde er bijvoorbeeld voor dat het draadloze netwerk van de New York City Government werd platgelegd (GPS Rollover Hamstrings New York City Wireless Network and a Handful of Other Systems - Inside GNSS - Global Navigation Satellite Systems Engineering, Policy, and Design).

GNSS markt rapport

Tijdens de masterclasses is al een aantal keer gesproken over de omvang van de GNSS sector. Meer informatie over trends binnen het gebruik van GNSS is te vinden in het GNSS-marktapport, te vinden via: https://www.euspa.europa.eu/sites/default/files/uploads/euspa_market_report_2022.pdf. Hierin staan o.a. voorbeelden beschreven van de verschillende marktsegmenten, wat de ontwikkelingen (meest recentste innovaties) zijn binnen deze segmenten en geeft een overzicht van de downstream markt voor ruimtevaart toepassingen.

NAVISP Industry Days

De belangrijkste Europese bedrijven die werken aan positiebepalings-, navigatie- en tijdsbepalingstechnologieën ontmoeten elkaar in het technisch hart van ESA in Nederland voor de NAVISP Industry Days.
De NAVISP Industry Days vinden plaats op 16-17 juni. De tweede dag staat in het teken van "NAVISP Element 3: Ondersteuning van PNT-initiatieven in de lidstaten", het IKUS-II onderzoek is zo'n NAVISP Element 3 initiatief vanuit Nederland. Voor meer informatie, en hoe u zich kunt inschrijven, vindt u hier.

Verstoringen in het nieuws

In de masterclasses van afgelopen april, is er toegelicht hoe gevoelig GNSS is en hoe verstoringen/interferentie, uitval, jamming en spoofing de signalen van GNSS kunnen verzwakken of vervormen.

Verstoring van het GNSS signaal kan door verschillende manieren ontstaan:

- Natuurlijke veranderingen (zoals bijvoorbeeld zonneactiviteit, ionospherishe effecten)
- GNSS constellatie errors
- Interferentie
- Jamming
- Spoofing

Regelmatig komen dergelijke verstoringen in het nieuws, via de nieuwsbrief delen wij graag met jullie een paar van dergelijke gebeurtenissen, zowel recente als iets oudere verstoringen.

Russia jamming aircraft satnav, French official warns
April 1, 2022

Russia jamming aircraft satnav, French official warns - GPS World : GPS World

Radio interference from damaged equipment affects other vessels
Januari 28, 2022

Radio interference from damaged equipment affects other vessels — IMCA (imca-int.com)

Verstoring scheepvaartverkeer Westerschelde mogelijk veroorzaakt door 'dronekiller'
Maart 29, 2021

Verstoring scheepvaartverkeer Westerschelde mogelijk veroorzaakt door 'dronekiller' | Dronewatch

GPS Spoofing Mystery Affirms Need for Protection
April 23, 2019

GPS Spoofing Mystery Affirms Need for Protection (wardsauto.com)

HK$1 million in damage caused by GPS jamming that caused 46 drones to plummet during Hong Kong show
Oktober 29, 2018

HK$1 million in damage caused by GPS jamming that caused 46 drones to plummet during Hong Kong show | South China Morning Post (scmp.com)

IKUS-II Nieuwsbrief 2

Beste lezer, u ontvangt deze nieuwsbrief omdat uw organisatie gebruik maakt van GNSS diensten, of naar verwachting een goed inzicht heeft in het gebruik van deze diensten binnen de eigen sector.

Zoals u waarschijnlijk weet wordt het IKUS-II onderzoek uitgevoerd door het GNSS Centre of Excellence in opdracht van de Nederlandse overheid. Het doel van IKUS-II is om de huidige weerbaarheid van Nederlandse organisaties bij uitval van GNSS signalen te beoordelen en organisaties te helpen zich bewust te worden van de risico's binnen hun organisatie. Als een onderdeel van deze studie is er een vragenlijst opgesteld. Deze zal helpen met de huidige staat van erkende dreigingen en het niveau van weerbaarheid te beoordelen. Wij hebben al van een groot aantal sectoren, waardevolle en bruikbare feedback gekregen.

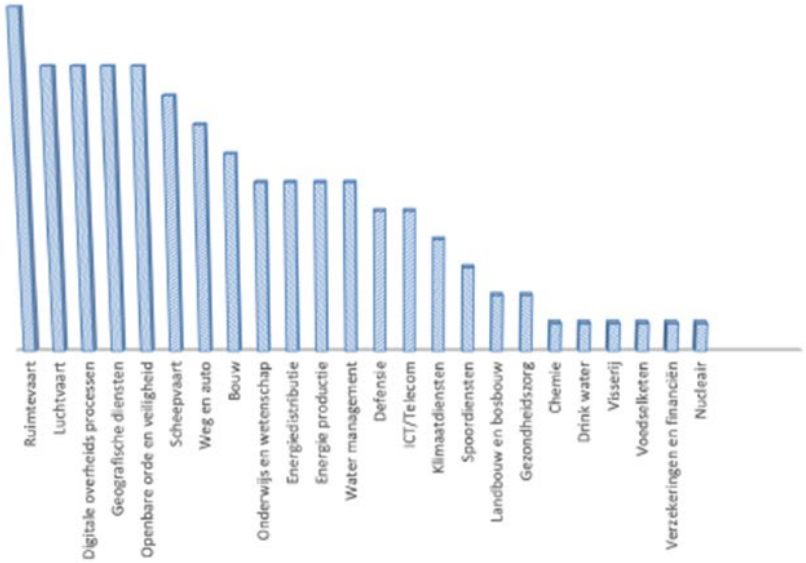
Maar zoals onderstaande grafiek laat zien zijn een aantal sectoren nog onder vertegenwoordigd in het onderzoek. Helpt u mee uw sector op de kaart te zetten?

We hebben de openstelling van de vragenlijst daarvoor verruimd tot 18 juli zodat u nog de tijd heeft om de questionnaire in te vullen!

Deze nieuwsbrief zal de volgende onderwerpen belichten:

- Input gevraagd voor de IKUS-II vragenlijst
- GPS kwetsbaarheid en weerbaarheid Galileo PRS
- Nieuwe services Galileo
- In het nieuws!

In deze en de aankomende nieuwsbrieven zullen verschillende GNSS onderwerpen belicht worden waar extra vragen of interesse in is getoond tijdens de masterclasses. Mocht er een onderwerp missen of vragen zijn, stuur dan gerust een mailtje naar info@gnss-coe.eu.



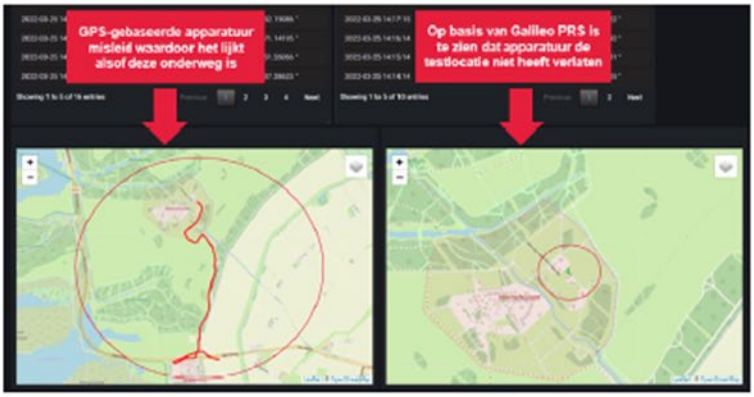
GPS kwetsbaarheid en weerbaarheid Galileo PRS

Dagelijks gebruik
Satellietnavigatie is geïntegreerd in onze samenleving. Voor PNT (Positionering, Navigatie en Tijd) wordt veelal gebruik gemaakt van open signalen van satellieten. Om van A naar B te navigeren, het volgen van transporten, monitoren van bewegingen van verdachten en synchronisatie van financiële transacties zijn een aantal voorbeelden hiervan. Dat deze open signalen kwetsbaar zijn wordt steeds bekender; in de media vind je regelmatig berichten over verstoringen en misleiding van deze signalen.

Unieke demonstratie
In samenwerking met Ministerie van Defensie, Netherlands Space Office en CGI is een unieke demonstratie georganiseerd om kwetsbaarheden inzichtelijk te maken. Deze demonstratie is onder professionele begeleiding van Agentschap Telecom uitgevoerd en bijgewoond met grote belangstelling door diverse Ministeries. Op deze dag werd in een open veld de kwetsbaarheid van het open GPS-signaal en de weerbaarheid van het beveiligde Galileo PRS gedemonstreerd. Het is een unieke demonstratie omdat dit soort verstoringen ongewild effect kunnen hebben op de omgeving en de gebruikers. De testen zijn daarom heel secuur en gecontroleerd uitgevoerd.

Kwetsbaarheid
Tijdens de demonstratie in het militaire oefendorp Marnehuizen is live aangetoond dat open signalen zoals die van GPS kwetsbaar zijn voor misleiding, ook wel bekend als spoofing. Dat gebeurde door met eenvoudig te verkrijgen apparatuur vervalste signalen uit te zenden die lijken op de open GPS-signalen afkomstig van satellieten. Doordat het vervalste signaal sterker is dan het signaal dat vanuit de satelliet afkomstig is, neemt de apparatuur de vervalste signalen voor werkelijkheid aan. Je kunt spoofing vergelijken met deep-fake: wat je ziet lijkt werkelijkheid, maar dat is het niet.

De toevallige passant...
De bevestiging van de demonstratie werd zeer duidelijk toen een toevallige passant, op basis van zijn telefoon, totaal gedesoriënteerd door het oefendorp kwam fietsen. Door inzet van een huis-tuin-en-keuken simulatieapparatuur is deze recreërende fietser op de verkeerde locatie uitgekomen. Een onschuldig voorval, maar toont zeer goed de eenvoud van het probleem en de eventuele gevolgen.



Nieuwe services Galileo

Galileo voorziet Europa niet alleen van een eigen GNSS-constellatie, maar introduceert ook nieuwe functies die de nauwkeurigheid en robuustheid verhogen en hulp kunnen bieden in noodsituaties. Twee van deze functionaliteiten, die zich momenteel beide in de testfase bevinden, worden hier in uitgelicht.

OSNMA
Open Service Navigation Message Authentication (OSNMA) is een authenticatiemethode voor navigatiegegevens die de robuustheid van Galileo tegen "spoofing" zal vergroten (gebeurtenissen waarbij een kwaadwillige zender valse navigatieberichten verzendt in een poging de ontvanger te misleiden). De gebruiker zal dan achteraf kunnen checken of een ontvangen signaal dezelfde speciale code bevat als de satellieten hebben uitgezonden. Deze speciale code is namelijk op voorhand niet te bepalen waardoor de code niet na te maken is.

OSNMA bevindt zich momenteel in de testfase en de start van de eerste operationele fase wordt verwacht in 2023. Aangezien OSNMA beschikbaar zal zijn voor iedereen met een OSNMA compatibele ontvanger en er geen speciale gebruikersver-

gunningen vereist zijn, kan het een grote verscheidenheid van gebruikers in staat stellen de authenticiteit van de Galileo-signalen die in hun positie- en tijdstoepassing worden gebruikt te verifiëren. Voor meer informatie over OSNMA zie Galileo_OSNMA_Info_Note.pdf (gsc-europa.eu).

HAS

Een van de onderwerpen die tijdens de masterclasses is besproken, is de nauwkeurigheid die kan worden bereikt met standalone GNSS-oplossingen en de verbeteringen die kunnen worden aangebracht door nauwkeurige correcties toe te passen. Voor professionele toepassingen zijn verschillende correctiemethoden beschikbaar, elk met hun eigen voordelen en beperkingen. Aangezien er steeds meer hoge nauwkeurigheidseisen worden gesteld, heeft het Galileo-programma besloten een hoge-nauwkeurigheidsdienst aan te gaan bieden, genaamd HAS (High Accuracy Service). Deze zeer nauwkeurige dienst zal extra correcties rechtstreeks via het E6-B-signaal (signaal verstuurt door Galileo) en via het internet verschaffen. De dienst zal dus real time correcties op het ontvangen signaal mogelijk maken. De dienst kan worden beschouwd als een alternatief voor andere augmentatiesystemen en is gericht op toepassingen in de geomatica, landbouw, luchtvaart, weg-, spoor-, zee- en ruimtevaart. Naar verwachting zal HAS in 2023 operationeel worden verklaard. Voor meer informatie over HAS, zie Galileo_HAS_Info_Note.pdf (gsc-europa.eu).

In het nieuws!

'They're Jamming Everything': Putin's Electronic Warfare Turns Tide of War
June 3, 2022 - by Jake Thomas

https://www.newsweek.com/theyre-jamming-everything-putins-electronic-warfare-turns-tide-war-1712784

OSNMA anti-spoofing tech now on PolaRx5 GNSS reference receivers
June 6, 2022 - by Tracy Cozzens

https://www.gpsworld.com/osnma-anti-spoofing-tech-now-on-polarx5-gnss-reference-receivers/

Rising Demand in Global GPS Anti-Jamming Market Size & Share to Hit USD 7.12 Bn Growth by 2028 | CAGR of 7.6% - Exclusive Report
June 27, 2022

https://www.bloomberg.com/press-releases/2022-06-27/rising-demand-in-global-gps-anti-jamming-market-size-share-to-hit-usd-7-12-bn-growth-by-2028-cagr-of-7-6-exclusive-report