Capgemini Consulting

IKUS

Synthese Rapport

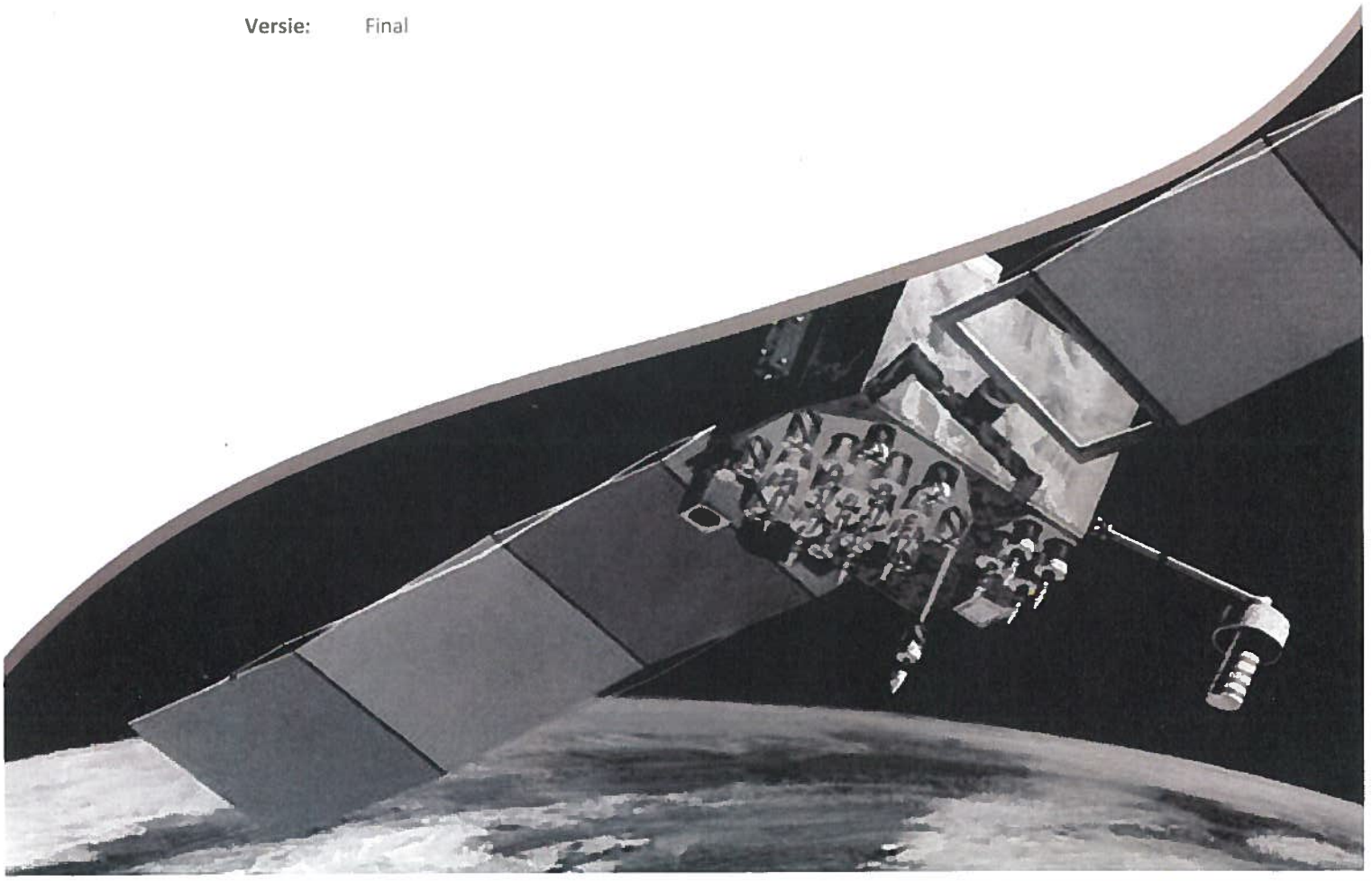
Inventarisatie Kwetsbaarheid Uitval Satellietnavigatie

Ministerie van Infrastructuur en Milieu

Rubricering: TLP Wit

Datum: **11-03-2016**

Versie: Final



Inhoudsopgave

MANAGEMENTSAMENVATTING 4

1. AANLEIDING EN DOELSTELLING ONDERZOEK 6

1.1 Inleiding en achtergrond 6
1.2 Doelstelling 6
1.3 Vraagstelling 6
1.4 Aanpak 7
1.5 Uitgangspunten 8
1.6 Opzet 9
1.7 Vertrouwelijkheid 10
1.8 Leeswijzer 10

2. GNSS IN HET KORT 11

2.1 Inleiding 11
2.2 Gebruik GNSS 11
2.3 Kwetsbaarheden en dreigingen GNSS 12
2.4 Mogelijke oorzaken van verstoring of uitval 13
2.4.1 Natuurlijke oorzaken 13
2.4.2 Jamming 14
2.4.3 Spoofing en Meaconing 14
2.5 Waarschijnlijkheid en duur van GNSS uitval 14
2.6 Maatregelen en alternatieven voor GNSS 15
2.7 Tijdsynchronisatie in computernetwerken 16

3. VITALE INFRASTRUCTUUR EN GNSS 17

3.1 Definitie van vitale processen 17
3.2 Gebruik van GNSS in vitale infrastructuur 19
3.2.1 Trends in gebruik van GNS 20
3.3 Kwetsbaarheden vitale infrastructuur voor uitval of verstoring GNSS 20
3.3.1 Kwetsbaarheid plaatsbepaling 20
3.3.2 Kwetsbaarheid tijdsbepaling 20
3.3.3 Kwetsbaarheid indirecte afhankelijkheden 20
3.4 Bestaande maatregelen tegen uitval of verstoring 22
3.4.1 Technische maatregelen 22
3.4.2 Organisatie van de sectoren en belegging van de verantwoordelijkheid 23
3.4.3 Preventieve maatregelen: detectie, opsporing en interventie bij het optreden van GNSS verstoringen 24

4. CONCLUSIES 26

4.1 Afhankelijkheid en Kwetsbaarheid 26
4.2 Bestaande en nieuwe maatregelen 27
4.2.1 Bestaande maatregelen tegen uitval GNSS 27
4.2.2 Nieuwe maatregelen: Systeemverwevenheid en kwetsbaarheid 27
4.3 Bewustzijn 27

BIJLAGEN **29**

Bijlage 1: GNSS, dreigingen en kwetsbaarheden 30

Bijlage 2 : De nul/één meting 34

Toelichting nul/één meting *35*

Bijlage 3: Feed back deelnemers IKUS symposium 38

Bijlage 4: Betrokkenen in het traject 40

Bijlage 5: Begrippen en afkortingen 42

Bijlage 6: IKUS Factsheet 44

MANAGEMENTSAMENVATTING

Het ministerie van Infrastructuur en Milieu (IenM) heeft opdracht gegeven voor de uitvoering van het project Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie (IKUS) om de weerbaarheid van de vitale infrastructuur tegen uitval van satellietnavigatie inzichtelijk te maken en zo nodig te vergroten. Onder vitale infrastructuur verstaan we producten, diensten en de onderliggende processen die, als zij uitvallen, grootschalige maatschappelijke ontwrichting kunnen veroorzaken.

In plaats van de term satellietnavigatie wordt in dit rapport de internationaal gebruikelijke verzamelterm Global Navigation Satellite System (GNSS) gebruikt. GNSS-systemen, waaronder GPS en Galileo, worden gebruikt voor positiebepaling, navigatie en tijdsbepaling (PNT). De directe aanleiding voor het IKUS-project is het natuurverschijnsel zonnestorm. Een zonnestorm is een periodieke mega eruptie van zonne-energie waardoor onder meer de elektromagnetische eigenschappen van de atmosfeer zodanig verstoord worden, dat de correcte ontvangst van GNSS-signalen tijdelijk niet meer mogelijk is. GNSS-signalen kunnen echter ook opzettelijk worden verstoord (*jamming*) of worden nagebootst en vervalst om de ontvanger te misleiden (*spoofing and meaconing*).

Kortdurende uitval van GNSS-signalen komt regelmatig voor. Langdurige uitval, enkele uren tot enkele dagen is echter vrij zeldzaam. Voor tijdwaarneming zal GNSS-uitval tot enkele dagen door het merendeel van de gebruikers nauwelijks worden opgemerkt, omdat interne kloksystemen in staat zijn om dit interval te overbruggen. Voor positiebepaling zal uitval van enkele minuten al kunnen leiden tot aanzienlijke verstoringen in onder meer de lucht- en de scheepvaart.

Door de digitalisering zijn en worden er steeds meer toepassingen ontwikkeld die gebruik maken van tijd- en positieinformatie. Als bron voor deze tijd- en positie-informatie wordt veelvuldig gebruik gemaakt van GNSS, omdat het nauwkeurig is, ruim voldoende beschikbaar en betrouwbaar geacht wordt en gratis is. Daardoor is het gebruik van GNSS ten opzichte van eerdere inventarisaties in 2005 en 2010 aanzienlijk toegenomen. Ook in de kritische processen van de Nederlandse vitale infrastructuur wordt GNSS gebruikt, onder meer in de telecom -, energie - en financiële sector. De mate van afhankelijkheid van GNSS in de kritische processen verschilt echter per sector, zo blijkt uit dit IKUS onderzoek.

In het IKUS-project is er voor elk van de twaalf vitale sectoren, met betrokken sectorspecialisten een GNSS afhankelijkheid en kwetsbaarheid analyse gemaakt. Door het presenteren van afhankelijkheden, kwetsbaarheden en daarbij mogelijke (preventieve) maatregelen bij uitval en/of verstoring van GNSS, draagt het IKUS traject bij aan bewustzijnsvergroting binnen de vitale sectoren in Nederland. Dit biedt daarmee richting voor verder te nemen maatregelen in lijn met de sector verantwoordelijkheden. Uitkomsten van andere gerelateerde projecten (zoals het project Herijking Vitaal) zijn, voor zover mogelijk, gebruikt ten behoeve van consistentie en efficiëntie. De sectoren zijn nu zelf verantwoordelijk voor het verder vergroten van het bewustzijn, het ontwikkelen van handelingsperspectief en het nemen van maatregelen. Gezien de vertrouwelijkheid van bijdragen van de sectordeelnemers is het ministerie van IenM en de andere betrokken vakdepartementen, alleen op hoofdlijnen geïnformeerd over de aangetroffen kwetsbaarheden en bijbehorende verbetermaatregelen.

Over het algemeen is gedurende het IKUS traject gebleken dat de kennis over gebruik van GNSS in kritische processen niet wijd verspreid was binnen organisaties. Het IKUS traject heeft het bewustzijn bij sleutelfunctionarissen binnen de sectoren wel verhoogd door interviews, workshops en sectorspecifieke rapportages. Het is aan de sectoren om deze bewustzijnsverhoging door te zetten door bijvoorbeeld informatie uit IKUS te delen met collega's. In de lucht- en scheepvaartsector staat GNSS afhankelijkheid overigens op de agenda in internationale overlegfora.

Uit de analyses komt verder naar voren dat het cascade en geaggregeerd risico bij uitval of verstoring van GNSS binnen de sectoren zelf nog weinig aandacht heeft gekregen. Vervolgonderzoek naar de cascade-effecten

verdient daarom aanbeveling. Verder valt op dat veel organisaties in de sectoren voor GNSS-afhankelijke toepassingen vertrouwen op hun telecom-providers en de afgesloten Service Level Agreement (SLA).

De mate waarin maatregelen zijn genomen, is afhankelijk van het risicobewustzijn per sector. Het gebruik van traditionele navigatiemethoden, onafhankelijk van GNSS, is een belangrijke maatregel van de maritieme en luchtvaartsector om hun afhankelijkheid van GNSS te beperken. De internationaal beschikbare budgetten voor de instandhouding van deze traditionele navigatiemethoden zijn alleen aanzienlijk afgenomen. Systemen worden daardoor niet meer onderhouden en worden aan het einde van hun technische levensduur opgeheven. Juist om de GNSS-afhankelijkheid te beperken wordt er door diverse deskundigen in internationaal verband opgeroepen om de nog resterende 'legacy' systemen op enige wijze te handhaven of te moderniseren. Het ontbreken van consensus over de internationale financiering belemmert echter de besluitvorming over de voortzetting van de legacy.

Verschillende sectoren hebben naar aanleiding van het IKUS traject, uitval en/of verstoring van GNSS opgenomen als terugkerend onderwerp binnen de sectorspecifieke (continuïteits-)overleggen. Sectoren zonder een specifiek continuïteitsoverleg wordt aanbevolen om deze alsnog in te richten. Aan alle sectoren is geadviseerd om bij de organisatiespecifieke risicoanalyses en crisismanagementmaatregelen aandacht te geven aan het scenario 'uitval en/of verstoring van GNSS'.

Nationaal en Internationaal is de onwenselijke afhankelijkheid van GNSS aanleiding geweest voor succesvolle onderzoeken naar nauwkeurige alternatieven. Hierdoor zijn nieuwe, GNSS onafhankelijke, plaats- en tijdbepalingtechnologieën ontwikkeld die ook nog tot verdere kostenbesparingen kunnen leiden. Het daadwerkelijk gebruik van dergelijke methoden en technieken is echter nog beperkt. Aan de sectoren wordt geadviseerd om de mogelijkheden van deze nieuwe methoden en technieken te onderzoeken en waar mogelijk te benutten.

1. AANLEIDING EN DOELSTELLING ONDERZOEK

1.1 Inleiding en achtergrond

Het ministerie van Infrastructuur en Milieu (IenM) heeft opdracht gegeven voor de uitvoering van het project Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie (IKUS) om de weerbaarheid van de vitale sectoren tegen uitval van satellietnavigatie inzichtelijk te maken en zo nodig te vergroten.

In opdracht van het ministerie van Veiligheid en Justitie (VenJ) wordt jaarlijks, in het kader van de strategie nationale veiligheid, een Nationale Risicobeoordeling (NRB) opgesteld waarin een aantal veiligheidsthema's wordt geanalyseerd in de vorm van scenario's. In de risicobeoordeling van 2011 is het scenario 'satellietuitval vanwege een zonnestorm' door het Analistennetwerk Nationale Veiligheid (ANV), namens de Stuurgroep Nationale Veiligheid geanalyseerd. Uit die analyse is naar voren gekomen dat extreme zonneactiviteit kan leiden tot verstoringen bij nagenoeg alle sectoren binnen de vitale infrastructuur met zowel directe als indirecte gevolgen.[1]

IKUS richt zich de op afhankelijkheid van de vitale infrastructuur van Global Navigation Satellite Systems (GNSS), zoals GPS, GLONASS en Galileo. Uit voorstudies is gebleken dat de sectoren van de vitale infrastructuur hun afhankelijkheid van GNSS, voor plaatsbepaling, navigatie en/of tijdsbepaling (PNT) niet altijd in beeld hebben.

1.2 Doelstelling[2]

Het project Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie (IKUS) heeft als doel de weerbaarheid van vitale sectoren tegen uitval van satellietnavigatie inzichtelijk maken en zo nodig vergroten. Deze inventarisatie is van belang om maatschappelijke ontwrichting en grote economische impact bij uitval van satellietnavigatie te voorkomen. Na afloop van het IKUS traject zijn:

- continuiteitsmanagers en gebruikers van apparatuur en systemen in vitale sectoren, die afhankelijk zijn van satellietnavigatie, zich bewust van de kwetsbaarheden;
- de kwetsbaarheden met betrekking tot uitval satellietnavigatie in kaart gebracht;
- bestaande en/of nieuw te ontwikkelen preventieve maatregelen en terugvalopties (incl. globale kostenindicaties) t.a.v. uitval satellietnavigatie in kaart gebracht.

1.3 Vraagstelling

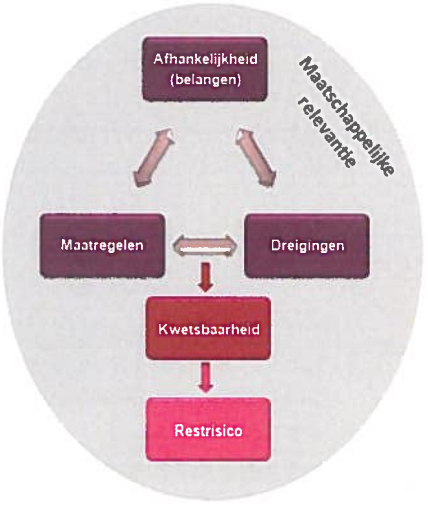
Om deze doelstellingen te vervullen is middels het conceptueel kader (zie figuur 1) gedurende het IKUS traject gericht ingegaan op de volgende vragen:

---

[1] Nationale Risicobeoordeling 2011, Analistennetwerk Nationale Veiligheid (ANV)

[2] Projectopdracht Ministerie van Infrastructuur en Milieu, 4 september 2013, referentienummer 13.0372

1. Wat zijn de vitale processen binnen de sectoren die afhankelijk zijn van GNSS signalen?
   En op welke wijze zijn deze processen afhankelijk van GNSS?
2. Zijn voor de continuïteit van deze processen maatregelen getroffen t.a.v. (een van enkele dagen tot een week durende) uitval of verstoring van GNSS-signalen?
3. Zo ja, hoe lang kunnen met deze maatregelen de kritische processen doorgang hebben zonder beschikbaarheid van (betrouwbare) GNSS-signalen?
4. Wat zijn mogelijke keteneffecten richting andere vitale sectoren?
5. Wat zijn aanvullende maatregelen die getroffen kunnen worden?
6. Wat zijn de globale kostenindicaties van de nieuw te ontwikkelen maatregelen?



Figuur 1. Conceptueel kader

1.4 Aanpak

Het project IKUS is opgebouwd uit een voorbereidende fase, waarin met experts een eerste inventarisatie naar afhankelijkheden, dreigingen, maatregelen en kwetsbaarheden is uitgevoerd. Op basis van inzichten uit de voorbereidende fase en op basis van inzichten uit Herijking Vitaal zijn de sectoren in de aanpak en planning over twee 'clusters' verdeeld:

Cluster 1	Cluster 2
• Digitale Overheid	• Chemie
• Drinkwater	• ICT
• Energie (Gas en Elektriciteit)	• Nucleair
• Financiën	• Olie
• Keren en beheren oppervlaktewater	• Luchtvaart
• Maritiem	
• Openbare Orde en Veiligheid	
• Telecommunicatie	

In de uitvoerende fase zijn sleutelfiguren uit deze sectoren in overleg met vakdepartement benaderd vanuit een standaardaanpak, met oog voor de specifieke kenmerken van de sector. Op basis van literatuuronderzoek en interviews met de betrokken sectorvertegenwoordigers zijn de afhankelijkheden en kwetsbaarheden per sector in kaart gebracht. Tijdens een sectorworkshop is meer inzicht gegeven in het gebruik en de kwetsbaarheden van GNSS, daarbij zijn tevens eerste sector specifieke inzichten gedeeld en aangescherpt. Elk sectoraal traject is afgesloten met een sectorrapportage, welk is afgestemd met de betrokken sectorvertegenwoordigers en de vertegenwoordiger van het vakdepartement. Na afronding van cluster één heeft er een bijeenkomst plaatsgevonden met de sectorvertegenwoordigers waarbij de deelnemers onder andere sector specifieke kennis en ervaringen hebben gedeeld en waarbij wederzijdse afhankelijkheden zijn besproken.

Gedurende de synthesefase zijn zowel sectorvertegenwoordigers als inhoudelijke experts samengekomen bij het IKUS symposium. Het IKUS symposium is specifiek gericht op het delen van de inzichten en aanbevelingen voortkomend uit het IKUS traject, het delen van kennis en het samenbrengen van sectoren, en tot slot het verkennen van sectoroverschrijdende uitdagingen. In de synthesefase is tevens het syntheserapport opgesteld;

de sectorrapportages vormen de basis voor deze syntheserapportage. De uitkomsten van de éénmeting uitgevoerd bij aanvang van de synthesefase zijn tevens opgenomen in het syntheserapport.

1.5 Uitgangspunten

Voor IKUS gelden de volgende uitgangspunten:

1. In plaats van de term satellietnavigatie gebruiken we in het project ook de aanduiding Global Navigation Satellite System (GNSS), waaronder zowel toepassingen voor positiebepaling, navigatie als tijdsbepaling (PNT) worden gevat.
2. Het scenario 'satellietuitval vanwege een zonnestorm' uit de Nationale Risicobeoordeling (NRB) geldt als uitgangspunt. Dit betekent een verstoring of uitval van GNSS signalen voor een periode van enkele dagen tot een week. Het natuurkundige verschijnsel zonnestorm zelf is als zodanig geen onderwerp van onderzoek, enkel de gevolgen. Andere oorzaken van uitval of verstoring van GNSS signalen zijn wel relevant om te benoemen, zeker in het kader van bewustwording, maar vormen ook geen onderwerp van onderzoek.
3. De afhankelijkheden en impact bij verstoring/en of uitval van GNSS wisselt per organisatie. De sectoren zijn en blijven altijd zelf verantwoordelijk voor bewustzijn, handelingsperspectief en het nemen van maatregelen. Het project stimuleert het probleembewustzijn en handelingsperspectief te vergroten, maar neemt de verantwoordelijkheid van de sectoren niet over. Gezien het verschil tussen vitale sectoren, wordt per sector de werkwijze aangepast aan hoe de sector georganiseerd is.
4. Aardobservatie, satellietcommunicatie en militaire communicatie zijn geen onderwerp van onderzoek. Dat geldt ook voor directe effecten van zonnestormen en alertering van ruimteweer, hoewel die wel zijdelings een rol kunnen spelen bij mogelijke keteneffecten, respectievelijk bij mogelijke weerbaarheidmaatregelen. IKUS richt tevens zich niet op de satellieten zelf, maar op toepassingen van hun signalen.
5. Het IKUS traject is gericht op de vitaal aangemerkte kritische processen van de vitale infrastructuur in Nederland. Alle sectoren uit Herijking Vitaal zijn onderwerp van de inventarisatie. Bij geen enkele vitale sector kan vooraf worden uitgesloten dat er kritische processen zijn waarin gebruik wordt gemaakt van apparatuur of systemen die afhankelijk zijn van satellietnavigatie voor tijds- of positiebepaling.
6. Uitkomsten van andere lopende projecten (zoals het project Herijking Vitaal) worden, voor zover mogelijk, gebruikt ten behoeve van consistentie en efficiëntie.
7. Voor het opsporen van kwetsbaarheden wordt het uitgangspunt gehanteerd dat satellietnavigatie enkele dagen tot een week niet beschikbaar is.[3] Daarnaast wordt ook de situatie bekeken dat het signaal gedurende deze periodes onbetrouwbaar is.

[3] Deze duur van de uitval is overgenomen uit het Scenario 'Uitval Satelliet Systemen' van de Nationale Risico Beoordeling 2011.

1.6 Opzet

De gefaseerde opzet van IKUS is als volgt:

0.	**Project start**	Het plan van aanpak voor IKUS is opgesteld in overleg met opdrachtgever. Hierbij is besproken 1) de doelgroepselectie, 2) inrichting team en 3) projectcommunicatie. Het plan van aanpak voor iedere sector is opgesteld met het desbetreffende vakdepartement en sectorvertegenwoordiger(s), hierbij zijn sleutelfiguren uit de sectoren aangewezen om te benaderen.
1.	**Analyse**	De analysefase bestaat uit 1. deskresearch, 2. expertmeeting 3. nulmeting[4] en 4. interviews. Naast het IKUS brede deskresearch is er sector specifiek deskresearch uitgevoerd. Het vakdepartement, de sectorvertegenwoordigers en opdrachtnemer hebben hiervoor informatie geïdentificeerd en aangeleverd. Op basis van eerste inzichten voortkomend uit het deskresearch en de expertmeeting zijn de sleutelfiguren uit de sectoren geïnterviewd.
2.	**Concept sectorrapportage**	Voor iedere sector is op basis van de inzichten uit het deskresearch en de interviews een eerste conceptrapportage opgesteld.
3.	**Sector workshop**	De bevindingen waarop de conceptrapportage is gebaseerd zijn getoetst en aangescherpt in een interactieve workshop van ca. 2 uur met het vakdepartement, sectorvertegenwoordigers en experts (kennisinstituten, koepelorganisaties, leveranciers satellietnavigatie) op het gebied van (uitval) satellietnavigatie. De beoogde uitkomst van iedere workshop: 1. Verhogen van kennis en bewustzijn over GNSS afhankelijkheden en kwetsbaarheden, 2. Delen van bevindingen afhankelijkheden, kwetsbaarheden en maatregelen van specifieke sector, 3. Toetsen van bevindingen en aanvullende inzichten verzamelen; 4. Delen van aanbevelingen voor (aanvullende) maatregelen.
4.	**Definitieve sectorrapportages**	Op basis van de uitkomsten van de workshop zijn de definitieve sectorrapportage opgesteld (*TLP Groen*). Deze rapportages zijn net als de concepten dermate op hoofdlijnen geschreven, dat het risico van vrijkomen van gevoelige informatie zoveel mogelijk is beperkt. Gedurende de workshop en bilaterale contacten is dieper ingegaan op de verschillende aspecten.
5.	**Accorderen eindversies sectorale deelrapportage**	De sectorrapportages zijn geaccordeerd door het betreffende vakdepartement en de sectorvertegenwoordigers. De sectoren en vakdepartementen geven indien nodig zelfstandig invulling aan vervolgstappen naar aanleiding van bevindingen en aanbevelingen.
6.	**Cluster workshop**	Na afronding van de sectorrapportages is door het projectteam en IenM een clusterworkshop georganiseerd voor deelnemers van cluster een. Doel van de workshop was: 1. Resultaten presenteren, 2. Kennis overdracht door experts en/of leveranciers,

[4] Uitgevoerd door Agentschap Telecom

		3. Kruisbestuiving bevorderen tussen sectoren door hen kennis over knelpunten en good practices te laten delen.
7.	**Eénmeting**	In overleg met de opdrachtgever en de uitvoerder van de nulmeting is een enquête, de éénmeting, onder leden van de sector uitgezet. De éénmeting meet de stijging van de kennis, het bewustzijn en de afhankelijkheden en maatregelen na van IKUS. De uitkomsten zijn meegenomen in het syntheserapport en besproken gedurende het symposium.
8.	**Symposium**	In overleg met de opdrachtgever is een IKUS symposium georganiseerd voor de deelnemende sectorvertegenwoordigers en vakdepartementen. Doel van het symposium is het vergroten van het kennis ten aanzien van GNSS-afhankelijkheid en de daarbij horende kwetsbaarheid van de sectoren. Daarnaast is het symposium gericht op het samenbrengen van, en de kennisoverdracht tussen, de verschillende vitale sectoren.

1.7 Vertrouwelijkheid

Vanwege het onderwerp van dit project verdient het thema vertrouwelijkheid van informatie extra aandacht.

Met het oog op de informatiebeveiliging wordt een "black box"-principe gehanteerd. Dit houdt in dat het ministerie van IenM (of andere betrokken vakdepartementen) niet in detail op de hoogte wordt gebracht van eventueel gevonden kwetsbaarheden en bijbehorende verbetermaatregelen. Belangrijk is vooral dat de sectoren zelf informatie uitwisselen met betrekking tot specifieke kwetsbaarheden en onderling aan oplossingen werken. Het ministerie van IenM heeft hierbij een sturende, regisserende rol en richt zich met name op knelpunten die alleen op het niveau van de (rijks-)overheid opgelost kunnen worden. Hierdoor wordt het risico verminderd dat gevoelige informatie in de openbaarheid komt op basis van de Wet Openbaar Bestuur (WOB) en neemt de bereidheid van vitale bedrijven om mee te werken toe.

In verband met vertrouwelijkheid van informatie hebben de rapportages een relatief hoog abstractieniveau. Gegevens die betrekking hebben op het voorkomen van een verstoring, de voorbereiding op een verstoring dan wel het optreden in geval van een verstoring is informatie die (in verkeerde handen) de veiligheid van de Staat kan schaden. Om die reden bevat deze rapportage geen sensitieve detailinformatie.

Deze rapportage is gerubriceerd als TLP Wit. Dit houdt in dat dit rapport openbaar is en onbeperkt verspreid mag worden.

1.8 Leeswijzer

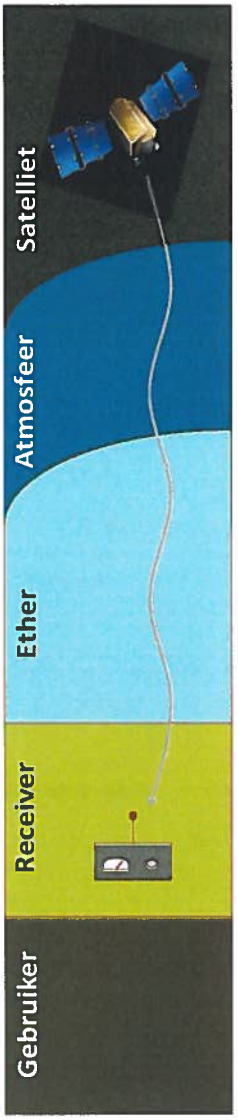
In hoofdstuk 2 staat een algemene beschrijving van GNSS en haar kwetsbaarheden. In hoofdstuk 3 staan de observaties over de afhankelijkheid van GNSS, de getroffen maatregelen, het bewustzijnsniveau en de kwetsbaarheid van de sectoren beschreven. In het afsluitende hoofdstuk 4 staan de conclusies met betrekking tot de sectoren en sectoroverschrijdende conclusies beschreven.

2. GNSS in het kort[5]

2.1 Inleiding

GNSS staat voor Global Navigation Satellite System, een verzamelterm voor de diverse satellietsystemen voor Positiebepaling, Navigatie en Tijdsbepaling (PNT).

Er zijn vier globale systemen. De oudste en bekendste is GPS (Global Positioning System) van de Verenigde Staten. Rusland heeft GLONASS (GLObal'naya NAvigatsionnaya Sputnikovaya Sistema) en China werkt aan de uitbreiding van zijn Beidou/COMPASS systeem. Galileo is het navigatiesatellietsysteem van Europa. Daarnaast zijn er enkele regionale systemen (bijvoorbeeld in Japan, India).



2.2 Gebruik GNSS

GNSS wordt wereldwijd steeds meer gebruikt, omdat het nauwkeurig is, ruim voldoende beschikbaar en betrouwbaar geacht wordt en zonder kosten in rekening te brengen gebruikt kan worden.[6] Naast individueel gebruik, maken organisaties vaak (onbewust) gebruik van GNSS in kritieke processen. Het Europese GNSS Agentschap voorspelt dan ook dat in 2020 wereldwijd meer dan 1 miljard GNSS ontvangers operationeel zullen zijn.[7] Uit cijfers van 'Strategy Analytics'[8] blijkt dat er momenteel wereldwijd 2 miljard smartphone gebruikers zijn. Vrijwel elke smartphone heeft een ingebouwde GPS-ontvanger. Smartphones maken voor locatiebepaling echter niet alleen gebruik van GNSS, maar ook van positie informatie die afkomstig is van de draadloze toegangspunten van het aangesloten netwerk, zoals GSM-masten en WIFI-routers. Daardoor zijn de Location Based Services van een smartphone ook bruikbaar als er geen GNSS ontvangst mogelijk is, zoals is in stedelijke gebieden en in gebouwen.

Een GNSS bestaat uit 3 segmenten:

1. Het space segment: een constellatie van satellieten op 20.000 km hoogte, die radiosignalen uitsturen naar gebruikers.
2. Het 'ground-control' segment, dat bestaat uit een netwerk van voorzieningen op de grond die samen zorgen voor volgen van GNSS satellieten, monitoring en analyse van hun signalen en command & control.

---

[5] Voor een uitgebreide beschrijving van GNSS en haar algemene kwetsbaarheden en dreigingen zie bijlage: *GNSS, dreigingen en kwetsbaarheden*

[6] U.S. Department of Homeland Security, National Risk Estimate: Risks to U.S. Critical Infrastructure from Global Positioning System Disruptions, Public Summary, 2013

[7] GNSS Market Report Issue 2," European GNSS Agency (GSA) Publications, Brussels, 2012

[8] Onderzoek door 'Strategy Analytics' gepubliceerd aan de vooravond van het Mobile World Congress in Barcelona 2014 http://www.emerce.nl/nieuws/2-miljard-mensen-hebben-smartphone

3. Het gebruikerssegment, bestaande uit een receiver (of ontvanger), die GNSS signalen (van meerdere satellieten van één of meerdere systemen) ontvangt. De receiver gebruikt de ontvangen signalen om uit te rekenen wat de driedimensionale positie is van de receiver en/of de tijd.[9]

GNSS signalen kunnen dus gebruikt worden voor zowel positiebepaling, navigatie als tijdsbepaling. GPS is bijvoorbeeld onder normale omstandigheden in staat om een geografische positie aan te geven met een nauwkeurigheid van 5 tot 10m, snelheid te bepalen tot ongeveer 20 cm/s en tijd tot op de microseconde. De nauwkeurigheid hangt wel af van de gebruikte ontvanger, invloeden in de atmosfeer en de constellatie van satellieten die de ontvanger volgt.[10]

GNSS signalen komen als radiosignalen via de ether bij de ontvanger terecht. De verschillende systemen gebruiken hiervoor bandbreedtes (of 'banden') die dicht bij elkaar liggen, of zelfs identiek zijn om redundantie in signalen te bewerkstelligen.

De kwetsbaarheid van GNSS zit voornamelijk in de zwakheid van het signaal. Verstoring of uitval kan op verschillende niveaus plaatsvinden:

1. Het GNSS satellietsysteem;
2. De atmosfeer waardoor GNSS signalen reizen;
3. De radiofrequentieruimte in Nederland, ofwel de ether;
4. GNSS-ontvangers en hun leveranciers;
5. De sectoren zelf als gebruikers van GNSS signalen.

Verstoring of uitval op het niveau van het satellietsysteem valt buiten de scope van dit onderzoek.

2.3 Kwetsbaarheden en dreigingen GNSS

In onderstaand figuur worden de verschillende kwetsbaarheden en dreigingen voor GNSS per niveau benoemd. In bijlage één wordt hier dieper op ingegaan.

[9] United States Government Accountability Office, GPS disruptions. Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced, 2013

[10] University of Texas, UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea, http://www.utexas.edu/news/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/, geraadpleegd op 5-5-2014

Kwetsbaarheden	Dreigingen	
• Laag vermogen (<100 Watt), groot bereik. • Beschikbaarheid van voldoende GNSS signalen • Disfunctioneren van de klok aan boord van de satelliet kan onnauwkeurigheid van het tijdsignaal teweegbrengen	• Technische storing • Verkeerde gegevens vanuit het grondstation, onopzettelijk of opzettelijk (hacking) • Opzettelijke vernietiging • Zonnestorm	Satelliet
• Atmosfeerconditities kunnen snel en aanzienlijk wijzigen	• Elektrische lading van de atmosfeer met reflectie als gevolg (multipath) • Zonnestorm (en geomagnetische storm) • Nucleaire ontploffingen in de atmosfeer • Multipath effect: opvangen van reflectiesignaal door een 'blob'of 'bubbie' in de atmosfeer	Atmosfeer
• onduidelijke afspraken • Niet sync wetgeving internationaal • Niet sync opsporing • Grote commerciele druk op spectrum	• Concurrerend signaal (onopzettelijk wegdrukken van signaal) • Jammen (opzettelijk wegdrukken van signaal) • Spoofing (opzettelijk manipuleren van signaal) (naar gebruiker) • Meaconing (opzettelijk manipuleren van signaal) (naar receiver) • Ongereguleerde groei mobiele communicatie	Ether
• Lage signaalsterkte: 160dBW (1 x 10–16 watts) op de grond • Inferieure apparatuur waardoor overgevoelig voor interferentie • Softwarematige fouten in receiver • Inloggegevens die gemakkelijk te hacken zijn • Onveilige technische protocollen • "achterdeurtjes" voor toegang door leveranciers vormen een kwetsbaarheid	• Multipath effect: opvangen van reflectiesignaal door weerkaatsing van bouwewerken 'Jitter': ruis van het elektronisch circuit van de ontvanger • Timing fouten door roll-overs in het signaal van de satelliet leiden tot sprong in de tijd • Updates van de satelliet (=satelliet ?) • Hacking • (meestal oudere) GPS ontvangers kunnen het signaal heruitzenden en andere antennes verstoren • Ontbreken va effectieve minimum producteisen en productaansprakelijkheid	Receiver
• Ongemerkt grote afhankelijkheid • Gebrek aan terugvalopties • Onbekendheid met de gevolgen van verstoring • Onbekendheid met de ketenafhankelijkheid • Niet authentieke signalen mogelijk door onversleutelde data (GPS)= spoofing=	• Niet toereikende opleiding en training gebruikers • onduidelijke/onvolledige man-machine interface	Gebruiker

2.4 Mogelijke oorzaken van verstoring of uitval

2.4.1 Natuurlijke oorzaken

GNSS-signalen worden verzonden vanaf de satelliet en worden via de verschillende lagen in de atmosfeer (ionosfeer en troposfeer) ontvangen op aarde. Onderweg kunnen de signalen door talrijke oorzaken verstrooien, verzwakken of verdwijnen. De directe aanleiding voor het IKUS-project is het natuurverschijnsel zonnestorm. Een zonnestorm is een periodieke mega eruptie van zonne-energie waardoor onder meer de elektromagnetische eigenschappen van de atmosfeer zodanig verstoord worden, dat de correcte ontvangst van GNSS-signalen tijdelijk niet meer mogelijk is. Maar ook direct op de satelliet zelf kan een zonnestorm een ernstig verstorend effect hebben. Over het zonnestorm verschijnsel is de afgelopen jaren veel gepubliceerd[11] mede omdat in de periode 2012-2015 een piek is opgetreden in de elfjarige eruptiecyclus. Dit piektijdsvenster is bij het opstellen van dit rapport vrijwel gepasseerd zonder, voor zover bekend, ernstige incidenten. Door deze piekperiode is er wel bijzondere aandacht geweest in de media voor de mogelijke effecten van een zonnestorm op de samenleving.

[11] Brochure Ministerie van Infrastuctuur en Milieu, november 2013, 'Weerbaar tegen extreme zonneactiviteit: Gevolgen op aarde van extreme explosies op de zon'

Naast natuurlijke oorzaken van signaalverstoring zijn er ook opzettelijke en onopzettelijke *man-made* technische oorzaken voor verstoring of uitval van GNSS-signalen. Er zijn vele elektromagnetische bronnen die radiosignalen uitzenden in frequentiebanden die door GNSS worden gebruikt en met vermogens waardoor GNSS-ontvangst onopzettelijk verstoord wordt. Voorbeelden hiervan zijn 'ultra wideband radar', televisiezenders, VHF radiozenders, mobiele satellietdiensten en zelfs persoonlijke elektronische devices. Ook slecht afgeschermde apparatuur kan zorgen voor verstoring van de ontvangst.

GNSS-signalen kunnen ook opzettelijk worden verstoord (*jamming*) of worden nagebootst en vervalst om de ontvanger te misleiden (*spoofing and meaconing*).

2.4.2 Jamming

GPS of GNSS jamming is het opzettelijk uitzenden van radiofrequenties of -signalen die de ontvangst van GNSS-signalen uit de ruimte overstemmen. Het is één van de bekendste en meest voorkomende opzettelijke verstoringvormen. Wereldwijd neemt jamming toe. Aanvankelijk waren het vooral overheidsdiensten en krijgsmachten die jamming gebruikten, jamming apparatuur en informatie erover is echter steeds makkelijker verkrijgbaar. Dit soort commerciële (en in Nederland en de EU illegale) jammers worden onder andere terug gevonden in (gestolen) auto's. Het gaat om eenvoudige, maar doeltreffende apparaten die op enkele of meerdere banden de signaalontvangst in de buurt van de zender verstoren. Specialistische GNSS-ontvangers zijn in staat om te signaleren dat er signaaljamming plaatsvindt en dat de weergegeven informatie dus onbetrouwbaar is.

2.4.3 Spoofing en Meaconing

Bij spoofing wordt een echt GNSS-signaal vervangen door een gemanipuleerd en krachtiger signaal dat afwijkt of gaandeweg bewust af gaat wijken van de werkelijke positie of tijd. Activiteiten door de ontvanger worden vervolgens gebaseerd op een foutief signaal. Meerdere wetenschappelijke onderzoeken hebben aangetoond dat het mogelijk is om GNSS-ontvangers met spoofing te misleiden. Tijdens één onderzoek was de afstand tussen ontvanger en spoofing apparatuur zelfs meer dan 1.000 meter. Apparatuur voor spoofing is groter en complexer dan voor jamming en vereist ook meer kennis en vaardigheden van de uitvoerder.

Bij meaconing (masking beacon) wordt er een echt GNSS-signaal opgevangen en opnieuw vertraagd en gemanipuleerd krachtiger uitgezonden (delaying and rebroadcasting). Net als bij spoofing ontvangt het GNSS-apparaat wel een signaal, maar wijkt dit af van de werkelijke tijd en plaats. Meaconing heeft voornamelijk betrekking op het manipuleren van gecodeerde GNSS-uitzendingen voor positiebepaling en navigatie. Spoofing en meaconing komen weliswaar minder vaak voor dan jamming, maar kunnen een grotere impact hebben omdat detectie meer tijd kost.

2.5 Waarschijnlijkheid en duur van GNSS uitval

Kortdurende uitval van GNSS-signalen komt zeer regelmatig voor. Vrijwel dagelijks is er ergens in de wereld een signaalverstoring, waardoor lokaal de GNSS positiebepaling wordt gehinderd. Meestal duurt dit slechts kort, een enkele keer is er een opsporingsdienst nodig om de oorzaak van de storing weg te nemen. Dergelijke incidentele uitval zal door de meeste gebruikers nauwelijks waargenomen worden.

Langdurige uitval, enkele uren tot enkele dagen is echter vrij zeldzaam. Zoals eerder genoemd kan een zonnestorm leiden tot langdurige GNSS-verstoring. Tijdens de piekperiode van enkele jaren in een elfjarige cyclus kunnen plotselinge erupties optreden met een effect op GNSS, dat duurt van enkele seconden tot enkele dagen. Behalve de periodiciteit is er nog geen mechanisme bekend waarmee de intensiteit van de erupties tijdens een piekperiode vooraf kan worden voorspeld. Wel worden er door gespecialiseerde instituten voortdurend metingen gedaan, waardoor het daadwerkelijk optreden van een heftige eruptie kan worden vastgesteld. Afhankelijk van het type eruptie kan, op basis van historische gegevens, voorspeld worden na

hoeveel tijd (minuten-uren-dagen) en met welke hevigheid deze uitbarsting zal leiden tot verstoringen op aarde .

Naast verstoring door zonnestormen kunnen GNSS-signalen ook worden verstoord door grootschalige militaire operaties. Deze stoortactieken worden gebruikt om in een groot gebied de operaties van een tegenstander te hinderen, maar daarbij wordt uiteraard ook het vreedzaam gebruik verstoord. Dergelijke operaties komen de afgelopen tien jaar vrij regelmatig voor, echter veelal specifiek in crisisgebieden met over het algemeen geen of geringe industriële activiteit. Deze verstoring kan wel gedurende een langere periode worden volgehouden.

Voor tijdwaarneming zal GNSS-uitval tot enkele dagen door het merendeel van de gebruikers nauwelijks worden opgemerkt, omdat interne kloksystemen in staat zijn om dit interval te overbruggen. Voor positiebepaling zal een uitval van enkele minuten al kunnen leiden tot aanzienlijke verstoringen in onder meer de lucht en de scheepvaart.

2.6 Maatregelen en alternatieven voor GNSS

In de keten tussen een GNSS-satellietuitzending en de verwerking van die uitzending in een gebruikerssysteem zitten vele schakels die kwetsbaar zijn voor verstoring of uitval. In de loop der tijd zijn verschillende maatregelen getroffen om deze keten te beschermen tegen opzettelijke of onopzettelijke verstoringen.

Satellieten zelf zijn robuuster geworden, verder is wereldwijd meer aandacht voor de bescherming van de GNSS-frequentiebanden tegen ongeoorloofd gebruik, zijn de ontvangers 'smarter' en stabieler geworden en is door uitgebreid onderzoek kennis opgebouwd over de atmosferische effecten die kunnen leiden tot GNSS signaalverstoring.

Ook de introductie van nieuwe GNSS satellietconstellaties die volledig onafhankelijk van elkaar functioneren, dragen bij aan het verbeteren van de robuustheid van GNSS als geheel. Door de EU wordt met het Galileo-project een eigen GNSS-capaciteit ontwikkeld die nu al gedeeltelijk operationeel is. De huidige, meer geavanceerde ontvangers zijn in staat zijn om signalen van meerdere GNSS-operators te verwerken. Alle GNSS-constellaties maken echter wereldwijd gebruik van frequenties in speciale beschermde frequentiebanden, waardoor opzettelijke of natuurlijke storing in de ether nadelige gevolgen heeft voor alle systemen. Dit effect doet zich ook voor bij zonnestormen.

In het Galileo-project is met de PRS dienst (Public Regulated Service) een speciale dienst ontwikkeld voor vitale diensten welke robuust is tegen bepaalde vormen van opzettelijke storing. Ook het Amerikaanse GPS systeem kent een dergelijke bescherming voor een beperkte groep gebruikers. Deze beschermingstechnieken zijn overigens niet toereikend voor ernstige vormen van zonnestormen.

Naast positiebepaling via GNSS wordt er voor specifieke toepassingen ook steeds meer gebruik gemaakt van zogenaamde 'Real Time Location Services' (RTLS). Tegenwoordig is deze technologie bekend voor smartphone apps, waarbij diensten worden aangeboden die gebruik maken van positie-informatie van het toestel; de zogenaamde 'Location Based Services' (LBS). De RTLS technologie komt voort uit de logistieke industrie waarbij de technologie van RFID's (Radio-Frequency Identification) werd doorontwikkeld zodat niet alleen de identiteit maar ook de locatie van een object vastgesteld kon worden. Bijzonder aan de RTLS technologie is dat deze voor de plaatsbepaling geen gebruik maakt van GNSS, maar van de positiegegevens van één of meerdere draadloze toegangspunten, zoals GSM-masten, WIFI-routers maar ook van infrarood of bluetooth stations. In stedelijke gebieden of in gebouwen waar GNSS-signalen nauwelijks doordringen is dit een effectieve methode. Buiten stedelijke gebieden en op zee maken professionele gebruikers, in de lucht- en scheepvaart , weliswaar in steeds mindere mate, nog gebruik van traditionele navigatiesystemen, zoals Loran-C. Loran C is in feite een traditionele vorm va RTLS maar dan over grote afstanden. Door de zeer hoge exploitatiekosten van deze infrastructuur en het afnemende gebruik is een deel van deze internationale infrastructuur inmiddels ontmanteld en staat de instandhouding van het nog restende deel onder grote druk.

2.7 Tijdsynchronisatie in computernetwerken[12]

Tijdswaarneming is wereldwijd van groot belang omdat vele toepassingen, waaronder computernetwerken en applicaties voor hun goede werking, nauwkeurig in tijd gesynchroniseerd moeten zijn. Zonder deze nauwkeurige synchronisatie degradeert de performance van netwerken en applicaties, waardoor het functioneren van systemen onbetrouwbaar kan worden. Tijdsynchronisatie in een netwerk vindt veelal plaats door toepassing van het NTP-protocol.[13]

Het Network Time Protocol (NTP) is de internetstandaard voor tijdssynchronisatie via netwerken. De werking van NTP is gebaseerd op een hiërarchisch model waarbij een server de tijd volgt van het netwerk waar het deel van uitmaakt en een klein netwerk volgt weer de tijd van een groter netwerk. Eventuele tijdsverschillen tussen bron en cliënt worden door het protocol geleidelijk bijgewerkt. De netwerkbeheerder kan zelf de configuratie-instellingen aanpassen en kiezen welke NTP-server als referentie wordt gebruikt. Ook als de netwerktijd dan afwijkt van UTC[14], blijft de onderlinge synchronisatie op peil. NTP is een zogenaamd zuiver protocol, bij een te grote afwijking wordt een deelnemer als gestoord beschouwd en vervolgens genegeerd.

De implementatie van een gemeenschappelijk tijdsynchronisatieprotocol, tussen grote onafhankelijke netwerken, is in de praktijk echter niet altijd realiseerbaar. Door terug te vallen op de internationale atoomklok kan dat alsnog, ook zonder onderlinge afspraken, synchronisatie bereikt worden. Atoomklokken waren in het verleden zeer kostbaar in aanschaf en onderhoud. Gemeenschappelijk gebruik van centrale atoomklokken was en is daarvoor een efficiënte vervanger. Er zijn nu nog maar weinig operators die een eigen atoomklok beheren. De atoomkloktijd wordt momenteel veelal geraadpleegd via internet maar ook wel door de ontvangst van lange golf radio-uitzendingen met tijdmeldingen (DCF77[15]) en nu dus steeds meer door GNSS-ontvangers.

GNSS tijdontvangers zijn nauwkeurig en goedkoop maar door het zwakke signaal niet altijd betrouwbaar en beschikbaar en dus kwetsbaar. Maar ook atoomklokwaarneming via internet of lange golf is kwetsbaar en in enkele scenario's, waaronder het zonnestormscenario, kunnen deze kwetsbaarheden zich gelijktijdig manifesteren.

---

[12] Open Enterprise Server 2 Installatie en Beheer, door Sander van Vugt, 2008

[13] Network Time Protocol; http://www.ntp.org/ntpfaq/NTP-s-def.htm, geraadpleegd op 20-10-2015

[14] UTC (in het Nederlands ook aangeduid als gecoördineerde wereldtijd) is een standaardtijd, gebaseerd op een atoomklok en gecoördineerd met de rotatie van de aarde. Zie voor de relatie tussen de verschillende standaardtijden: http://leapsecond.com/java/gpsclock.htm , geraadpleegd op 7 augustus 2015.

[15] DCF77 is een tijdseinzender die vanuit Frankfurt via de lange golf permanent een signaal uitzendt welke binnen een straal van meer dan 1500 km te ontvangen is. Hierdoor is het mogelijk een radiografische klok te maken met een zeer geringe (enkele milliseconden) en bekende afwijking. Het tijdseinsignaal van DCF77 wordt afgeleid van een aantal atoomklokken. Zie ook: http://www.ptb.de/cms/en/fachabteilungen/abt4/fb-44/ag-442/dissemination-of-legal-time/dcf77.html

3. VITALE INFRASTRUCTUUR EN GNSS

Het IKUS traject is gericht op de vitaal aangemerkte kritische processen binnen de vitale infrastructuur in Nederland. Bij aanvang van het IKUS traject is ervoor gekozen aan te sluiten op het Herijking Vitaal project van het Ministerie van Veiligheid en Justitie, waarin gekozen is voor een sectorale aanpak.[16].

In dit hoofdstuk zijn de observaties over de afhankelijkheid van GNSS, de getroffen maatregelen, het bewustzijnsniveau en de kwetsbaarheid op sectorniveau toegelicht.

3.1 Definitie van vitale processen

Onder vitale infrastructuur verstaan we producten, diensten en de onderliggende processen die, als zij uitvallen, grootschalige maatschappelijke ontwrichting kunnen veroorzaken. In 2014 en 2015 is in de 'Herijking Vitaal' door het Ministerie van Veiligheid en Justitie, op basis van de economische, fysieke en sociaal-maatschappelijke impact en cascade gevolgen beoordeeld wat de vitale infrastructuur is voor onze samenleving. [17] Daarbij is op basis van impact van uitval onderscheid gemaakt tussen twee categorieën vitaal om recht te doen aan de diversiteit binnen de vitale infrastructuur.[18]

Categorie A

In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de vier impactcriteria voor categorie A raakt:

- Economische gevolgen: > ca. 50 miljard euro schade of ca. 5.0 % daling reëel inkomen.
- Fysieke gevolgen: meer dan 10.000 personen dood, ernstig gewond of chronisch ziek.
- Sociaal maatschappelijke gevolgen: meer dan 1 miljoen personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen.
- Cascade gevolgen: Uitval heeft als gevolg dat minimaal twee andere processen uitvallen.

Categorie B

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.

---

[16] De inhoudelijke analyse gedurende het Herijking Vitaal traject heeft ertoe geleid dat er is gekozen voor een procesmatige benadering. De behandeling van de sectoren in het IKUS project was echter eerder afgerond dan het project Herijking Vitaal. Hierdoor is het, ondanks het streven naar samenhang, onvermijdelijk dat er verschillen in terminologie en focus zijn opgetreden

[17] Voortgangsbrief nationale veiligheid, minister van Veiligheid en Justitie, 12 mei 2015

[18] https://www.nctv.nl/onderwerpen/nv/bescherming-vitale-infrastructuur/herijking-vitaal/

In de voortgangsbrief nationale veiligheid heeft de minister van Veiligheid en Justitie aan de tweede kamer de resultaten van de Herijking Vitaal doen toekomen (zie onderstaand figuur).[19]

Processen	Cat.	Product, dienst of locatie	Sector	Min.
Landelijk transport en distributie elektriciteit	A	Elektriciteit	Energie	EZ
Regionale distributie elektriciteit	B			
Gasproductie Landelijk transport en distributie gas	A	Aardgas		
Regionale distributie gas	B			
Olievoorziening	A	Olie		
Internettoegang en dataverkeer	PM		ICT/ Tel	EZ
Spraakdiensten (mobiel en vast)				
Satelliet				
Tijd- en plaatsbepaling (satelliet)				
Drinkwatervoorziening	A	Drinkwater	Drinkwater	IenM
Keren en beheren waterkwantiteit	A	- (deel van de) primaire waterkeringen - (deel van de) regionale waterkeringen	Water	IenM
Vlucht- en vliegtuigafhandeling	B	Mainport Schiphol	Transport	IenM
Scheepvaartafwikkeling	B	Mainport Rotterdam		
Grootschalige productie/verwerking en/of opslag (petro)chemische stoffen	B	(Petro)chemische industrie	Chemie	IenM
Opslag, productie en verwerking nucleair materiaal	A	Nucleaire industrie	Nucleair	IenM
Toonbankbetalingsverkeer	B	Betalingsverkeer	Financieel	FIN
Massaal giraal betalingsverkeer	B			
Hoogwaardig betalingsverkeer tussen banken	B			
Effectenverkeer	B			
Communicatie met en tussen hulpdiensten middels 112 en C2000	B	Handhaving van de openbare orde en veiligheid	Openbare Orde en Veiligheid (OOV)	VenJ
Inzet politie	B			
Beschikbaarheid van betrouwbare basisinformatie over personen en organisaties, informatie uitwisseling van basisinformatie en beschikbaarheid van datasystemen waarvan meerdere overheidsorganisaties voor hun functioneren afhankelijk zijn.	B	Digitale overheid	Openbaar Bestuur	BZK

[19] Voortgangsbrief nationale veiligheid, minister van Veiligheid en Justitie, 12 mei 2015, pagina 5

3.2 Gebruik van GNSS in vitale infrastructuur

In de sectorrapportages is het gebruik, de kwetsbaarheid en de maatregelen voor iedere vitale sector inzichtelijk gemaakt om daarmee het bewustzijn binnen de sectoren te verhogen.

Het gebruik GNSS verschilt per sector en per organisatie binnen de sector. Het gebruik van GNSS kan betrekking hebben op plaats- en tijdsbepaling.

Bijna alle sectoren maken gebruik van GNSS bij tijdssynchronisatie in datanetwerken en applicaties. Hierbij is te denken aan betalings- en effectenverkeer in de sector financiën, communicatie tussen elektriciteitstations in de sector energie, telecommunicatie en voor bijvoorbeeld specifiek 112 en T2000 binnen de sector Openbare Orde en Veiligheid (OOV). De sector maritiem maakt voor de synchronisatie van walradarketens gebruik van GPS.

> ***Casus: Financiën***
>
> *Uit onderzoek bleek dat de sector financiën gebruik maakt van GNSS in het betalingsverkeer. Voor mobiel bankieren wordt GNSS (GPS) namelijk gebruikt om de locatie van de gebruiker te bepalen en op basis daarvan meer of minder rechten toe te kennen. Uit het buitenland zijn er nog meer toepassingen bekend, b.v. automatisch toeleiden van het mobiele apparaat van de klant naar het (wifi)netwerk van de dichtstbijzijnde ATM. Dit worden ook wel 'location based services' genoemd.*

Met betrekking tot positiebepaling is onder andere het volgen van cargo, voertuigen en medewerkers bij verschillende sectoren naar voren gekomen. Het transport van ladingen wordt in de maritieme sector bijvoorbeeld met behulp van GNSS gevolgd. Bijna alle sectoren maken gebruiken van GNSS voor navigatiediensten, er zijn echter een aantal sectoren waarbij deze functie kritiek is voor de continuïteit van het vitale proces, zoals bijvoorbeeld voor de sector luchtvaart. Bij keren en beheren oppervlaktewater wordt GNSS voor positiebepaling als expliciete afhankelijkheid benoemd omdat de registratie van meetgegevens deel vormt van het vitale proces. Dieptebepaling speelt ook een rol bij andere sectoren zoals onder anderen Olie maar deze vormde geen onderdeel van het in de Herijking Vitaal geformuleerde vitale proces voor de desbetreffende sector.

De sector openbare orde en veiligheid (OOV) is afhankelijk van GNSS in de aansturing en navigatie van hulpdiensten. Deze afhankelijkheid is ook door andere sectoren meermaals benoemd als een indirecte afhankelijkheid, . Vertegenwoordigers van de sector Energie benoemden expliciet de afhankelijkheid van GNSS bij het navigeren van storingsploegen bij het verhelpen van storingen in het energienetwerk.

> ***IKUS éénmeting***
>
> *57% van de respondenten geeft aan dat de vitale processen binnen hun sector afhankelijk zijn van GNSS en 70% geeft aan dat de primaire processen binnen de organisatie of branche gebruik maken van GNSS.*
>
> *(zie bijlage 2)*

Er is dus een onderscheid tussen de directe afhankelijkheid van GNSS in vitale processen en de indirecte afhankelijkheid die het resultaat is van door GNSS uitval gedegradeerde dienstverlening in andere sectoren. De oliesector zal bijvoorbeeld last hebben van verstoring en/of uitval van GNSS in de transport sector De meeste sectoren zijn wel op enige wijze indirect afhankelijk van de telecommunicatie, ICT, energie en de drinkwatersector. Vastgesteld kan daarbij echter worden dat de vitale sectoren ook bij de nu incidenteel voorkomende uitval van telecommunicatie, ICT, energie en drinkwater, om andere redenen dan GNSS-uitval, over het algemeen blijven functioneren.

De afhankelijkheid van GNSS kent ook een internationale component, omdat de gevolgen van GNSS-uitval niet tot Nederland alleen beperkt zal blijven. Uit de analyse komt naar voren dat een aantal sectoren, zoals de energiesector grensoverschrijdend is georganiseerd. Een analyse van de internationale effecten van GNSS-uitval valt echter buiten de scope van dit onderzoek.

3.2.1 Trends in gebruik van GNSS

De huidige afhankelijkheid van GNSS zal naar verwachting in de toekomst alleen maar verder uitbreiden. Dit wordt veroorzaakt door het toenemende belang van logistieke efficiëntie, de kwaliteit van de toepassingen en de toegankelijkheid van nieuwe technologie. Bij enkele sectoren is deze trend al expliciet zichtbaar en is er sprake van een substantiële groei in de komende jaren. Dit sluit aan bij de wereldwijde trend van groeiende afhankelijkheid van GNSS.

Bij de sectoren telecom, energie, maritiem en luchtvaart is deze groeiende afhankelijkheid van GNSS zichtbaar. In de luchtvaart sector is bijvoorbeeld duidelijk een trend zichtbaar richting grotere afhankelijkheid van GNSS bij navigatie van vliegtuigen. En voor de sector energie zal bijvoorbeeld met de komst van Smart Grids tevens een grotere afhankelijkheid van GNSS gaan ontstaan.

3.3 Kwetsbaarheden vitale infrastructuur voor uitval of verstoring GNSS

In het IKUS onderzoek is nagegaan op welke manier de sectoren afhankelijk zijn van GNSS en welke maatregelen er al getroffen zijn om deze afhankelijkheid te beperken. De afhankelijkheden die niet of in onvoldoende mate zijn afgedekt door aanwezige maatregelen vormen de kwetsbaarheden van de sectoren voor GNSS-uitval

3.3.1 Kwetsbaarheid plaatsbepaling

Het IKUS-traject is gericht op de vitaal aangemerkte processen binnen de vitale infrastructuur in Nederland. Het gebruik van GNSS in niet-vitale bedrijfsprocessen binnen de verschillende sectoren worden daarmee niet meegenomen in de analyse.

De maritieme en luchtvaartsector zijn het meest afhankelijk van GNSS voor de plaatsbepaling van schepen en vliegtuigen en de services die hier direct bij betrokken zijn. Deze sectoren maken echter ook nog steeds gebruik van traditionele navigatietechnieken en methoden die onafhankelijk zijn van GNSS. Door de beschikbare alternatieven voor GNSS en het hoge afhankelijkheidsbewustzijn, is de kwetsbaarheid van de sectoren lucht- en scheepvaart op dit moment beperkt. Er is echter een breed gedragen zorg over de *beschikbaarheid van de traditionele systemen op de langere termijn*. Door verschillende instellingen wordt er onderzoek gedaan of en hoe deze traditionele systemen gehandhaafd kunnen en moeten blijven. In specialistische internationale overlegfora vindt regelmatig overleg plaats over de inrichting van de GNSS redundantie. Het bereiken van consensus kost echter veel tijd, zeker ook omdat er hoge kosten mee gemoeid zijn en deze kosten op een goede manier verdeeld moeten worden over de belanghebbenden. Naast de kosten voor infrastructuur gaat het daarbij ook om de opleidingskosten van de gebruikers en de wijze waarop deze kennis vastgehouden en getoetst kan worden. Door de grote veiligheidsbelangen die gemoeid zijn met deze functionaliteit, is hiervoor veel aandacht. De ontwikkeling van een kostenefficiënt GNSS-onafhankelijk alternatief plaatsbepalingsysteem wordt door zowel de lucht- als de scheepvaart op termijn noodzakelijk geacht.

3.3.2 Kwetsbaarheid tijdsbepaling

Binnen vrijwel alle sectoren is er afhankelijkheid van de tijdsbepalingfunctie van GNSS, doordat elk computernetwerk met externe netwerkkoppelingen nauwkeurig in tijd gesynchroniseerd moet zijn. Zonder deze synchronisatie kan de uitgewisselde data- tussen de netwerken niet altijd op de juiste wijze worden verwerkt, waardoor systeemdegradatie kan optreden. Sectoren zoals de energie- en telecomsector, waarbij het primaire proces in hoge mate afhankelijk is van de goede werking van deze infrastructuur, hebben veelal passende maatregelen getroffen om deze synchronisatie te borgen, ook als GNSS niet beschikbaar is.

3.3.3 Kwetsbaarheid indirecte afhankelijkheden

Enkele sectoren, zoals luchtvaart, zeevaart, telecom en ICT maken direct gebruik van GNSS diensten, de kwetsbaarheid hiervan is in de vorige paragrafen aangegeven. De overige sectoren zijn in hun kritische

processen niet, of in veel mindere mate, direct afhankelijk van GNSS diensten, maar zijn wel weer afhankelijk van de dienstverlening van de andere sectoren die op hun beurt direct afhankelijk zijn. In deze indirect afhankelijke sectoren, dat zijn dus alle vitale sectoren, is het noodzakelijk dat er inzicht is in deze onderlinge afhankelijkheid en in de mogelijkheden om ook deze indirecte afhankelijkheid zelfstandig te beperken.

Vrijwel alle andere sectoren zijn afhankelijk van de infrastructuur aanbieders uit de energie- en telecomsector en deze afnemers vertrouwen er veelal op dat de infrastructuuraanbieders zelf passende maatregelen hebben getroffen. Geen van deze sectoren heeft echter dit risico benoemd of opgenomen in contracten, Service Level Agreements (SLA) of risicoanalyses.

De openbare orde en veiligheid sector (OOV) maakt, net als andere sectoren, gebruik van de beschikbare infrastructuur van de marktpartijen. Van de OOV sector wordt verwacht dat ze ook optreden als er door GNSS-uitval onrust ontstaat in de samenleving. *Om die rol te kunnen vervullen is een lagere kwetsbaarheid nodig en zullen aanvullende maatregelen door de OOV-sector moeten worden getroffen.* Door het IKUS project is het bewustzijn van deze kwetsbaarheid gegroeid en enkele maatregelen zijn inmiddels in voorbereiding.

Samenwerking en inzicht in elkaars kwetsbaarheid is ook relevant voor het ondervangen van een gesignaleerde systeemkwetsbaarheid rond GNSS. Steeds meer vitale functies in de samenleving zijn digitaal geïntegreerd en dat geldt dus ook voor crisisbeheersingsfunctie. Veel van de ICT-voorzieningen bij crisisbeheersing maken gebruik van GNSS, vooral voor tijdsynchronisatie.

Wat verder opvalt, is dat enkele sectoren wel fall-back maatregelen hebben getroffen voor eventuele uitval van een van GNSS-afhankelijke voorziening, maar dat die fall-back soms indirect ook weer afhankelijk is van GNSS. Een voorbeeld is het synchroniseren van tijd via internet, waarbij de internet referentiebron zelf ook weer gebruik maakt van GNSS.

Een andere uiting van de onderlinge verwevenheid en complexiteit is de afhankelijkheid van overheden en vitale organisaties, direct of indirect, van telecommunicatievoorzieningen van één enkele partij die op zijn beurt weer deels afhankelijk is van GNSS. De kans op -en impact van- cascade-effecten bij incidenten wordt hierdoor groter. Een ernstig zonnestorm incident kan de aanleiding zijn voor dergelijke grootschalige cascade-effecten. Door de sectorale aanpak van het IKUS project is het zicht op dit effect echter beperkt gebleven. De directe effecten die het gevolg zijn van zonnestormen zijn al eerder onderzocht[20] en vallen buiten het bestek van dit rapport.

Ook het geaggregeerd risico is een bijzonder aandachtspunt. Langdurige en/of grootschalige GNSS-uitval of verstoring kan geljjktijdig alle vitale sectoren beïnvloeden. Ook delen van de samenleving die door de onderzoekssystematiek van Herijking Vitaal en IKUS nu buiten beeld vallen, kunnen worden geraakt en zullen mogelijk de impact van een crisis vergroten.

Voor veel vitale organisaties heeft de kwetsbaarheid voor uitval of verstoring van GNSS potentieel een grensoverschrijdende dimensie. Dit is bijvoorbeeld het geval wanneer het gaat om tijdsynchronisatie tussen netwerken in verschillende landen. De te treffen maatregelen in de verschillende landen moeten worden afgestemd, primair binnen de organisaties en sectoren zelf.

---

[20] Rapport Weerbaar tegen extreme zonneactiviteit, Gevolgen op aarde van extreme explosies op de zon Ministerie van Infrastructuur en Milieu, www.rijksoverheid.nl/ienm, November 2013

3.4 Bestaande maatregelen tegen uitval of verstoring

3.4.1 Technische maatregelen

Voordat GNSS toepassingen vanaf midden jaren negentig grootschalig werden ingevoerd bestonden er al vele vormen van tijd- en plaatsbepaling. Vooral de maritieme en de luchtvaartsector is altijd afhankelijk geweest van plaatsbepaling en een aanzienlijk deel van deze systemen wordt tot op heden nog veelvuldig gebruikt. De nauwkeurigheid van deze systemen, bekend onder namen zoals Loran-C, Omega en Decca is echter aanzienlijk minder dan GNSS, bovendien zijn ze vaak bewerkelijk en zijn de ontvangers en zeker ook de zendersystemen zelf, kostbaar. Vooral voor de professionele gebruikers is momenteel alleen het Loran-C systeem nog in beperkte mate in gebruik mede op basis van International Maritime Organization (IMO) [21] en International Civil Aviation Organization (ICAO)[22] afspraken. Maar de kennis van de gebruikers neemt snel af en de enkele landen die deze omvangrijke zenders nog beheren zijn steeds minder bereid om de enorme kosten voor steeds minder gebruikers te blijven dragen. Juist om de GNSS afhankelijkheid te beperken wordt er door diverse deskundigen in internationaal verband opgeroepen om de nog resterende 'legacy' systemen te handhaven en te moderniseren. De urgentie en de noodzaak van deze behoefte wordt echter nog niet breed erkend. Daardoor is er geen bereidheid van verschillende individuele landen, waaronder Nederland[23], om bij te dragen aan de hoge kosten voor instandhouding van de nog resterende Loran-C installaties in onder meer Frankrijk en Engeland.

Naast de systemen die nu langzamerhand uitfaseren, maakt zowel de luchtvaart als de scheepvaart ook gebruik van zichtnavigatie, radiobakens en radiocommunicatie met verkeersleiders. Ook voor deze systemen geldt net als voor de elektronische systemen dat het gebruik arbeidsintensief is, de nauwkeurigheid relatief laag, de instandhouding van de infrastructuur zoals radiobakens en vuurtorens kostbaar is en de vaardigheid van de gebruikers afneemt.

Zowel in de lucht- als scheepvaart wordt ook nog steeds gebruik gemaakt van traditionele radarsystemen waarbij een verkeersleider nauwkeurig inzicht heeft in de positie van schepen en vliegtuigen. Indien de eigen plaatsbepaling van een schip op vliegtuig binnen radarbereik van deze verkeersleider verstoord is, kan de verkeersleider aanwijzingen geven om het schip of vliegtuig op veilige wijze binnen te loodsen. Deze systemen zijn nog steeds operationeel en ook al wordt er wereldwijd onderzoek gedaan naar verdere innovatie, waaronder geautomatiseerd landen en afmeren, zijn de beide sectoren zich ervan bewust dat door de GNSS kwetsbaarheid, de traditionele radar back-up noodzakelijk blijft.

In tegenstelling tot de hierboven genoemde, op radio-uitzendingen gebaseerde navigatiesystemen zoals Loran-C, is een atoomklok uiterst nauwkeurig, eenvoudig in

Chip Scale Atomic Clock

Sinds enkele jaren is er een zeer compacte atoomklok op de markt: de 'Chip Scale Atomic Clock' (CSAC). Deze miniatuur atoomklok ter grootte van een luciferdoosje, ontwikkeld door DARPA, is op de markt voor ca €1500,-. Deze nieuwe technologie zal ook bruikbaar zijn bij civiele gebruikers die nu fysiek niet in staat zijn om GNSS te ontvangen, zoals in de mijnbouw, onder water of in afgesloten ruimtes. Maar ook voor gebruikers die potentieel doelwit zijn of juist last hebben van GNSS jammers kunnen baat hebben van de CSAC. Verder zullen CSACs bruikbaar zijn voor de synchronisatie van uitgestrekte telecommunicatie-infrastructuren die geen gebruik kunnen maken van het NTP-protocol.

[21] International Maritime Organization (IMO), www.imo.org

[22] International Civil Aviation Organization (ICAO), www.icao.int

[23] https://www.eerstekamer.nl/9370000/1/j4nvhf0njnhd6ks_j9vvhwtbnzpbzzc/vgtwhhhov1v0

gebruik en minder kostbaar. Voor een private operator is een traditionele atoomklok echter nog steeds te kostbaar in aanschaf en onderhoud, waardoor het gebruik van centrale atoomklokken binnen een netwerk een efficiënte vervanger is geworden. Het nadeel van dit gemeenschappelijk gebruik is wel dat de beschikbaarheid van het communicatienetwerk voor het verzenden van het atoomkloksignaal, een nieuwe kwetsbaarheid en onnauwkeurigheid introduceert. Nieuwe ontwikkelingen in atoomklok technologie bieden echter goede vooruitzichten voor nieuwe en brede toepassing van dit concept.

Buiten de maritieme en luchtvaartsector rekenen operators in andere sectoren, al dan niet op basis van een 'Service Level Agreement' (SLA) veelal op de dienstverlening door hun leveranciers en service partners. Zeker daar waar de sectoren geen directe afhankelijkheid kennen en een uitval van enkele uren of enkele dagen niet leidt tot zeer ernstige gevolgen is daarbij de veronderstelling dat door improvisatie en procedurele maatregelen de belangrijkste nadelige gevolgen van GNSS uitval gemitigeerd kunnen worden. GNSS uitval als calamiteit wordt in standaard SLA's echter niet benoemd.

Voor specifiek tijdssynchronisatie wordt er binnen computernetwerken gebruik gemaakt van het NTP protocol waarmee computersystemen zich automatisch oplijnen aan de centrale timeserver in het netwerk. Zoals eerder aangegeven kunnen verschillende netwerken met dit NTP-protocol ook met elkaar synchroniseren. Door het gemak van het gebruik van tijdsignalen afkomstig van GNSS-providers, wordt deze mogelijkheid echter slechts beperkt benut.

3.4.2 Organisatie van de sectoren en belegging van de verantwoordelijkheid

Een belangrijke maatregel om de afhankelijkheid van GNSS te beperken en de weerbaarheid van een vitale sector te vergroten is overleg en coördinatie. Door structureel overleg zowel binnen als buiten de sector kan de kennis over afhankelijkheden en kwetsbaarheden worden gedeeld en kunnen mogelijke maatregelen worden besproken. Voor dit overleg is een effectieve sector governance nodig. Een succesvol voorbeeld van een dergelijke samenwerking is de luchtvaartsector die nationaal en internationaal de afhankelijkheden en kwetsbaarheden van GNSS bespreekt en gezamenlijk afspraken maakt over technische en procedurele maatregelen. Ook wordt de ontmanteling van traditionele navigatiesystemen waar mogelijk afgestemd op de realisatie van nieuwe fall-backs voor GNSS.

Ook in de maritieme sector is men over het algemeen bekend met de grote afhankelijkheid van GNSS en wordt dit in diverse overlegfora ook besproken. Door de omvang en diversiteit van de maritieme sector wordt er in deze sector aan meerdere alternatieven voor GNSS gewerkt. Dit leidt tot onderlinge competitie en dus onduidelijkheid.

Enkele vitale sectoren kennen specifieke samenwerkingsvormen die gericht zijn op 'business continuity' (Telecom, Energie en Financiën). Het onderwerp GNSS-uitval was echter in geen van deze fora voorafgaand aan het IKUS programma, een agendapunt. Door de IKUS workshops en rapportages is het onderwerp alsnog op de agenda gekomen.

Andere sectoren, zoals OOV en digitale overheid, kennen ook verschillende vormen van overleg, maar daarin was voorafgaand aan IKUS het thema GNSS afhankelijkheid nog niet of nauwelijks in beeld. De GNSS afhankelijkheid van deze sectoren is ook veelal indirect. Dat wil zeggen dat deze sectoren afhankelijk zijn van de dienstverlening van andere sectoren die op hun beurt wel direct afhankelijk zijn van GNSS. In deze indirect afhankelijke sectoren is het noodzakelijk dat er inzicht is in deze onderlinge afhankelijkheid en in de mogelijkheden om ook deze indirecte afhankelijkheid zelfstandig te beperken.

In de verschillende overleggen die in het IKUS onderzoek betrokken zijn geweest is veelal ook een departementale vertegenwoordiger (telecom, luchtvaart) of een toezichthouder (financiën, nucleair) opgenomen. De verantwoordelijkheid voor de implementatie van continuïteitsmaatregelen ligt echter in alle sectoren bij de sectordeelnemers zelf. Collectieve knelpunten met mogelijk aanzienlijke maatschappelijke impact kunnen onder de aandacht worden gebracht van het betrokken departement.

Zoals eerder aangegeven is er in Nederland geen centrale coördinator die stimuleert dat de verschillende netwerkbeheerders hun interne tijdssynchronisatie niet alleen binnen eigen hun netwerk organiseren, maar ook goede synchronisatieafspraken malen met andere netwerkbeheerders. Door een netwerk van goede onderlinge afspraken neemt de afhankelijkheid van tijdssynchronisatie via kwetsbare satellietontvangers af en kunnen andere kostbare technische maatregelen voorkomen worden. Door respondenten wordt wel aangegeven dat een expertfunctie wordt gemist die de sectordeelnemers dringend kan adviseren over maatregelen in het algemeen en NTP-configuraties in het bijzonder. In Zweden bijvoorbeeld is een dergelijke functie wel formeel belegd[24].

Door incidenten in het verleden en als gevolg van eerdere kwetsbaarheidanalyses[25] zijn er de afgelopen jaren maatregelen getroffen die onder de beleidsverantwoordelijkheid van het Ministerie van Economische Zaken vallen. Het gaat hierbij vooral om het verkrijgen van meer transparantie bij het gebruik van infrastructuren, het verhogen van 'awareness' bij veilig ICT/Telecommunicatie gebruik en continuïteitsbeleid.[26] Een deel van de te nemen maatregelen is opgepakt via werkprogramma's van het Agentschap Telecom, het NCSC en diverse awareness programma's.

3.4.3 Preventieve maatregelen: detectie, opsporing en interventie bij het optreden van GNSS verstoringen

Het GNSS signaal dat op aarde wordt ontvangen is zeer zwak en dus erg gevoelig voor bedoelde of onbedoelde verstoring. Om die reden zijn er internationaal afspraken gemaakt over het gebruik en de bescherming van de frequentieband waarin deze signalen worden uitgezonden. Dit houdt onder meer in dat het produceren en/of gebruik van zendapparatuur in deze frequentieband verboden is. Deze illegale apparatuur wordt onder meer geproduceerd om opzettelijk GNSS ontvangers te storen, maar ook komt het voor dat legale apparatuur door een bijzonder defect storing veroorzaakt in de GNSS frequentieband. Om de wet te handhaven beschikt het Agentschap Telecom (AT) over een meetnetwerk, voert het bijzondere controles uit en kan indien nodig handhavend optreden.

Wat betreft uitval en/of verstoring van GNSS, het Team High Tech Crime binnen de Landelijke Eenheid van de politie treedt op tegen complexe computergerelateerde criminele activiteiten. Verschillende marktpartijen en bijvoorbeeld de AIVD, de Landelijke Eenheid en het NCSC wisselen informatie uit over nieuwe dreigingen en mogelijke maatregelen om de weerbaarheid te verhogen. Ook internationaal gezien zijn er initiatieven genomen om te komen tot een verbetering van de weerbaarheid tegen ICT-verstoringen. De Europese Commissie zet zich in voor betere samenwerking binnen de Europese Unie en met andere internationale en nationale partijen op het gebied van preventie en respons tegen ICT-dreigingen.

Ook de douane vervult een essentiële rol bij de preventie van GNSS-verstoringen door bijzondere aandacht bij de import van illegale elektronica die bedoeld en onbedoeld het GNSS-domein verstoren. Zowel binnen als buiten de EU wordt er verder beleidsmatig aandacht besteed aan regelgeving en nieuwe afspraken over de productie en export van GNSS verstorende systemen.

Door het KNMI wordt in samenwerking met partners in binnen- en buitenland, onderzoek gedaan naar het ontwikkelen van voorspellingsmodellen voor het optreden van zonnestormen. Met bijzondere

---

[24] http://www.sp.se/en/index/services/time_sync/ntp/sidor/default.aspx, geraadpleegd op 19 oktober 2015

[25] O.m. NICC & NAVI (2010) Rapport weerbaarheid van telecommunicatie sector tegen ernstige uitval van elektriciteit

[26] artikel 11a.2, eerste lid, van de Telecommunicatiewet (wetgeving als gevolg van Europese regelgeving)

waarnemingsinstrumenten kan het optreden van een zonnestorm gedetecteerd worden en kan op basis van analyse en historische gegevens voorspeld worden wanneer en waar dit een impact kan krijgen op aarde. Afhankelijk van het type eruptie kan een dergelijke waarneming een aanwijzing geven op een effect dat variërend tussen enkele minuten tot enkele dagen kan optreden. Op basis van dergelijke voorspellingen kunnen de sectoren contingencyplannen ontwikkelen waardoor de impact van een zonnestorm kan worden beperkt.

4. CONCLUSIES

Uit het IKUS onderzoek komt naar voren dat het gebruik van GNSS-technologie door de digitalisering van de samenleving verder is toegenomen. De kwetsbaarheid van gebruikers voor GNSS-uitval is daardoor ook gegroeid. De sectoren die het meest direct afhankelijk zijn van de goede werking van GNSS hebben maatregelen getroffen om deze kwetsbaarheid te beperken. De overige sectoren zijn veelal indirect afhankelijk en hebben door het IKUS project nu meer kennis opgedaan over hun kwetsbaarheden. Ook zijn ze geïnformeerd over de beschikbare technische en organisatorische mogelijkheden om die kwetsbaarheid te beperken.

Door het presenteren van afhankelijkheden, kwetsbaarheden en daarbij mogelijke (preventieve) maatregelen bij uitval en/of verstoring van GNSS, draagt het IKUS traject bij aan bewustzijnsverhoging binnen de vitale sectoren in Nederland. Daarmee biedt het richting voor verder te nemen maatregelen in lijn met de sector verantwoordelijkheden. In de verschillende sectorrapportages zijn aan de sectoren de specifieke conclusies toegelicht. Deze sectorrapportages zijn per afzonderlijke sector gevalideerd. In dit hoofdstuk zijn de hoofdconclusies van het IKUS traject in algemene zin beschreven.

4.1 Afhankelijkheid en Kwetsbaarheid

- *De afhankelijkheid van GNSS in de kritische processen wisselt per sector, maar duidelijk is dat het **gebruik groeit** ten opzichte van eerdere inventarisaties in 2005 en 2010.*

  Belangrijke overwegingen voor organisaties om GNSS te gebruiken zijn de ruime mate van beschikbaarheid en de lage aanschaf- en exploitatiekosten.. Ook worden de ontvangers steeds compacter. Verder worden er voortdurend nieuwe locatieafhankelijke diensten ontwikkeld voor smartphones en wordt er steeds meer gebruik gemaakt van drones.

  Ook in de kritische processen van de Nederlandse vitale infrastructuur wordt GNSS gebruikt, onder meer in de telecom -, energie - en financiële sector. De mate van afhankelijkheid van GNSS in de kritische processen verschilt echter per sector, zo blijkt uit dit IKUS onderzoek.

- *De kennis over het gebruik en kwetsbaarheid van GNSS is beperkt*

  Over het algemeen is gedurende het IKUS traject gebleken dat de kennis over gebruik van GNSS in kritische processen niet wijd verspreid was binnen organisaties. Het werd meestal **beschouwd als een technisch vraagstuk**, waarvan de exacte consequenties vaak niet bij ieder duidelijk waren. Er werd in de sectorale inventarisaties zelden direct een verband gelegd met het eigen primair proces. De aanwezigheid van een betrouwbaar GNSS signaal werd door de meeste personen die we hebben gesproken voor dit onderzoek (aanvankelijk) dan ook als gegeven beschouwd.

- *Het gebruik van GNSS zal blijven toenemen*

  De verwachting dat het gebruik van GNSS in kritieke processen in vitale sectoren zal toenemen lijkt gerechtvaardigd, zowel voor tijdsynchronisatie als ook voor positie en navigatie. Een goed voorbeeld is de luchtvaart, waar GNSS in de cockpit aan belang toeneemt ten opzichte van andere navigatie- en positiebepalingsmiddelen. De eerste (experimentele) vliegtuiglandingen in stedelijk gebied puur op GPS zijn al uitgevoerd in New York en Zürich. Dit werd voorheen niet toegestaan door de Federal Aviation Authority (FAA).

- *Uitval van GNSS kan keteneffecten creëren.*

  Ook groei in niet-vitale sectoren en/of niet-kritieke processen is vanuit beleidsoogpunt relevant vanwege de impact en het geaggregeerd risico bij grootschalige uitval of verstoring. Het grootschalig gebruik van

GNSS in de gehele maatschappij, kan bij uitval of verstoring een opgeteld effect genereren, net als de cascade-effecten tussen vitale sectoren zelf.

De verantwoordelijkheid voor het opdoen van voldoende bewustzijn en kennis ligt in eerste instantie bij de vitale sectoren zelf. Dat geldt ook voor het stellen van eisen aan ICT en andere apparatuur die afhankelijk is van GNSS, zoals telecommunicatievoorzieningen of meetapparatuur.

4.2 Bestaande en nieuwe maatregelen

4.2.1 Bestaande maatregelen tegen uitval GNSS

Uit de inventarisatie blijkt dat op een aantal niveaus maatregelen zijn ondernomen:

- De mate waarin maatregelen zijn genomen, is afhankelijk van het risicobewustzijn per sector

  Het bewustzijn- en kennisniveau binnen de sectoren en per organisatie verschilt behoorlijk, ook op cruciale aspecten van gebruik van GNSS voor positiebepaling, navigatie en zeker tijdsynchronisatie. Uit de inventarisatie komt naar voren dat het merendeel van de organisaties binnen de sectoren maritiem, luchtvaart en telecommunicatie, zich bewust zijn van hun GNSS kwetsbaarheid en ook passende maatregelen hebben genomen om deze kwetsbaarheid te beperken.

- *Traditionele maatregelen worden in de maritieme en luchtvaartsectornog steeds gebruikt, maar deze maatregelen zullen binnen afzienbare tijd verdwijnen*

  Het gebruik van traditionele navigatiemethoden, onafhankelijk van GNSS, is een belangrijke maatregel van de maritieme en luchtvaartsector om hun afhankelijkheid van GNSS te beperken. Er is echter een breed gedragen zorg over de **beschikbaarheid van deze kostbare en technisch verouderde systemen op de langere termijn,** omdat internationale en intersectorale consensus over zowel de technische inrichting als de kostenverdeling van de noodzakelijke modernisering nog niet is bereikt.

- *Nieuwe alternatieven voor GNSS komen beschikbaar*

  Nationaal en Internationaal is de onwenselijke afhankelijkheid van GNSS aanleiding geweest voor succesvolle onderzoeken naar nauwkeurige, GNSS-onafhankelijke positie en tijdsbepaling, waaronder een 'low-cost minisize' atoomklok en tijdsynchronisatie-protocollen. Dergelijke alternatieven komen nu ook in toenemende mate op de markt. Door deze en andere technologieën zijn nieuwe GNSS-onafhankelijke toepassingen én verdere kostenbesparingen mogelijk.

4.2.2 Nieuwe maatregelen: Systeemverwevenheid en kwetsbaarheid

Maatregelen tegen GNSS kwetsbaarheid worden nu voornamelijk door iedere sector apart ingericht. Intersectorale maatregelen tegen cascade of geaggregeerde risico's krijgen daardoor weinig aandacht. Gedurende het IKUS traject hebben de sectorvertegenwoordigers zich echter zeer geïnteresseerd getoond in de kennis en ontwikkelingen binnen andere sectoren tegen de achtergrond van hun wederzijdse afhankelijkheid.

Deze wil tot samenwerking en inzicht in elkaars kwetsbaarheid is relevant voor het ondervangen van een gesignaleerde **systeemkwetsbaarheid** rond GNSS. Steeds meer vitale functies in de samenleving zijn digitaal geïntegreerd en dat geldt dus ook voor de crisisbeheersingsfunctie. Veel van de ICT-voorzieningen bij crisisbeheersing maken gebruik van GNSS, in het bijzonder voor tijdsynchronisatie.

4.3 Bewustzijn

Bewustzijn is de basis voor handelen. IKUS is daarmee in zichzelf een maatregel. IKUS heeft bijgedragen aan de bewustzijnsverhoging door direct contact met meer dan honderd vertegenwoordigers van organisaties die elk een sleutelrol vervullen in de nationale vitale infrastructuur. Door middel van vele gesprekken, workshops,

publicaties en een symposium is deze bewustzijnsverhoging gerealiseerd. Via deze kanalen zijn de vertegenwoordigers en hun achterban geïnformeerd over GNSS als systeem en de kwetsbaarheden van de organisatieprocessen. Gezamenlijk met de vertegenwoordigers van de sector zijn de sectorale afhankelijkheden vervolgens geïnventariseerd. Hierdoor is er in de sectoren meer inzicht ontstaan in de afhankelijkheden en de nu al beschikbare en nog te realiseren maatregelen. Binnen de verschillende sectoroverlegfora is het onderwerp GNSS-afhankelijkheid hoger op de agenda gekomen. Ook is de kennis over alternatieven voor GNSS binnen de verschillende sectoren vergroot. Door het presenteren van de mogelijke maatregelen is bijgedragen aan het versterken van het handelingsperspectief van de deelnemers.

Bijlagen

1. GNSS, dreigingen en kwetsbaarheden
2. De nul/één meting
3. Feed back deelnemers IKUS symposium
4. Betrokkenen in het IKUS traject
5. Begrippen en afkortingen
6. Factsheet IKUS

Bijlage 1: GNSS, dreigingen en kwetsbaarheden

Kwetsbaarheden satellietsysteem

De Achilleshiel van alle GNSS systemen is het erg zwakke signaal dat uiteindelijk bij de receivers terecht komt. Een navigatiesatelliet zendt met niet meer vermogen uit dan een koplamp van een auto (<100 Watt), maar moet wel een groot deel van het aardoppervlak bereiken vanaf 20.000 km hoogte.[27]

Aan het aardoppervlak is de signaalsterkte gedaald tot -160dBW (1 x 10–16 watts)[28]. Dit zwakke signaal is gevoelig voor opzettelijke of onopzettelijke verstoringen van dit signaal in de atmosfeer of de ether. Een concurrerend signaal kan eenvoudig het oorspronkelijke signaal wegdrukken en/of het circuit van de ontvanger verstoren ('overload')[29].

Een andere kwetsbaarheid van GNSS betreft de beschikbaarheid van voldoende GNSS signalen. Als er onvoldoende satellieten vanuit het oogpunt van de receiver zichtbaar zijn, is er geen positiebepaling mogelijk op basis van GNSS. De Amerikaanse overheid investeert daarom in een vervangings- en uitbreidingsprogramma voor GPS. De EU en landen als Rusland, China, Japan en India investeren mede om deze reden in eigen GNSS systemen, die al dan niet in samenhang met GPS kunnen worden gebruikt.

Satellieten zelf kennen ook kwetsbaarheden, zoals technische storingen waardoor incorrecte data wordt verstuurd[30]. Ook komt het voor dat vanuit het grondstation verkeerde gegevens worden verzonden, waardoor de satelliet niet goed functioneert.

Civiele GPS signalen zijn verder niet beveiligd, maar gaan onversleuteld door de atmosfeer en ether. Alleen militaire GPS signalen zijn versleuteld en geauthenticeerd. Deze zijn echter alleen beschikbaar voor de Amerikaanse strijdkrachten.[31] Het Europese Galileo bevat daarom om een eigen versleuteld, geauthenticeerd kanaal, Public Regulated Service (PRS).

Kwetsbaarheden transmissie signalen in atmosfeer

De GNSS signalen reizen door de atmosfeer en zijn in die fase kwetsbaar voor verstoring in de atmosfeer, waardoor signalen geheel wegvallen of reflecteren. De atmosfeer is namelijk dynamisch, waarbij voortdurend verschillen in temperatuur en dichtheid optreden. B.v. door bubbles/blobs,

De bovenste laag van de atmosfeer (de ionosfeer) is elektrisch geladen en kan daardoor ook voor verstoringen van GNSS signalen leiden. Ongecorrigeerd is dit één van de grootste oorzaken van fouten. [14]

Bij reflectie haakt een ontvanger niet aan op het originele satellietsignaal, maar op een reflectie ervan, waardoor er onverwachte en grote afwijkingen in de waarneming van positie en tijd kunnen plaats vinden. Dit wordt ook wel het multipath effect genoemd. Dit effect kan leiden tot gevaarlijke misleidende informatie in kritische applicaties [14]

---

[27] Last, David, GNSS: The Present Imperfect, Inside GNSS, May 2010

[28] Jon S. Warner, Ph.D. and Roger G. Johnston, Ph.D., CPP , GPS Spoofing Countermeasures, in Homeland Security Journal, December 12, 2003

[29] Royal Academy of Engineering, Global Navigation Space Systems: reliance and vulnerabilities, 2011

[30] Royal Academy of Engineering, Global Navigation Space Systems: reliance and vulnerabilities, 2011

[31] Jon S. Warner, Ph.D. and Roger G. Johnston, Ph.D., CPP , GPS Spoofing Countermeasures, in Homeland Security Journal, December 12, 2003

Kwetsbaarheden transmissie signalen in ether

De lage sterkte van het GNSS signaal is ook in de ether de belangrijkste kwetsbaarheid. Hierdoor wordt het relatief eenvoudig weg gedrukt door signalen in zelfde of nabije bandbreedte, al dan niet opzettelijk. Een voorbeeld van opzettelijke verstoring is het 'jammen' van signalen, d.w.z. het GNSS signaal als het ware wegdrukken met een ander, sterker signaal. Zie hierover verder het volgende hoofdstuk.

Kwetsbaarheden op ontvangers en leveranciers

De kwetsbaarheid van ontvangers en hun leveranciers ligt deels in technologie en deels in de wijze waarop de *markt van ontvangstapparatuur functioneert.*

Technische kwetsbaarheden

De ontvangers kennen verschillende technische kwetsbaarheden die kunnen leiden tot verstoring of onjuiste interpretatie van de ontvangen signalen, of uitval van de apparatuur. We laten hierna algemene oorzaken van verstoring achterwege, zoals stroomstoring of molest, maar richten ons op de zaken die samenhangen met de werking van GNSS ontvangers.

- De ruis van het elektronisch circuit in de receiver kan ontvangst van het GNSS signaal verstoren ('jitter')[14]
- Timing fouten door zogenaamde numerieke 'roll-overs' in het signaal van de satelliet, leidend tot een sprongetje in tijd ('leap second'). Hoewel er technische voorschriften zijn om om te gaan met dit soort sprongetjes, bleken bij een incident in 1999 niet alle ontvangers er mee om te kunnen gaan. [14]
- Updates in de software of constellatie van satellietsystemen (bijvoorbeeld GPS) kunnen bij ontvangers leiden tot problemen, indien deze niet om kunnen gaan met de veranderingen. B.v. in april 2007 werd een 32e satelliet toegevoegd aan het GPS systeem, maar sommige ontvangers bleken alleen berekend op 31 satellieten. In 2010 vond een software upgrade plaats in het grondsegment van GPS, wat leidde tot problemen met civiele en militaire ontvangers die het signaal minder goed vast konden houden.
- Net als elke computer kunnen ook GNSS ontvangers softwarematige bugs bevatten. Er gelden echter geen externe vereisten of standaarden voor GNSS ontvangers om aan te voldoen. Testen en eventueel certificering zijn optioneel. De kans dat geïnstalleerde software geheel vrij is van fouten is, net als bij overige software, erg klein. [32]
- En net als bij elke computer is het ook niet uitgesloten dat GNSS ontvangers gehackt kunnen worden. Er is bij schrijven geen onderzoek bekend dat zich specifiek richt op hackbare kwetsbaarheden van GNSS ontvangers. Dergelijk onderzoek is er wel voor ontvangers van satellietcommunicatie. De uitkomst is dat verschillende modellen ernstige kwetsbaarheden bevatten, zoals hard coded inloggegevens (altijd zelfde wachtwoord), onveilige technische protocollen en 'achterdeurtjes' voor toegang door de leverancier.[33]

AGPS: Het gebruik van Efemeriden data om de ontvangst van een GPS receiver (Assisted GPS) te versnellen brengt nieuwe kwetsbaarheden met zich mee voor de beschikbaarheid en kwaliteit van de informatie. [14]

---

[32] Royal Academy of Engineering, Global Navigation Space Systems: reliance and vulnerabilities, 2011

[33] IOActive, *A Wake-up Call for SATCOM Security*, 2014. Samen met: The Register, *Sat comms kit riddled with backdoors for hackers – researcher. Right, shipmate, identify yourself. What's your meaning?*, 23 Apr 2014

Overlay vulnerabilities: Gebruikers gaan in de toekomst afhankelijker worden van verschillende 'overlay systems' die noodzakelijk zijn voor het vergroten van de presetatie van GNSS. Dit levert mogelijk meer kwetsbaarheden in het systeem op.

Kwetsbaarheden bij leveranciers of in de markt

In tegenstelling tot het ruimtesegment van GNSS, is er een grote variëteit aan ontvangstapparatuur en hun leveranciers. De markt varieert van leveranciers van militaire ontvangers, gecertificeerde ontvangers en wetenschappelijke apparatuur tot huis-tuin-en-keuken ontvangers in mobiele telefoons. Fabrikanten ontwerpen GNSS receivers op diverse kwaliteitsniveaus, maar zelfs de meest eenvoudige ontvanger is al een redelijk complexe combinatie van hardware en software.

Op zichzelf zorgt deze diversiteit voor beschermingen tegen dreigingen die alleen een bepaalde soort ontvangers raken. Ontwerpfouten kunnen zich echter altijd voordoen en oorzaak zijn van falen van de ontvanger. Bij wijd gebruik in kritische systemen in vitale sectoren kan dit ernstige gevolgen hebben, zeker als de betreffende ontvanger niet ontworpen was voor kritisch gebruik.[14]

Kwetsbaarheden op gebruikersniveau

Te grote en ongemerkte afhankelijkheid, gebrek aan back-up opties, onbekendheid met kans op en gevolgen van verstoring en keteneffecten zijn belangrijke kwetsbaarheden op het niveau van gebruikers in vitale sectoren.

Ongemerkt is de afhankelijkheid van GNSS erg groot geworden

Langzaam maar zeker is de beschikbaarheid van GNSS voor positie, navigatie en tijdsbepaling voor vanzelfsprekend aangenomen en gebruikt voor een grote variëteit aan (kritische) systemen en processen. Het is echter niet altijd helder voor gebruikers (uitzonderingen daargelaten) dat ze bijvoorbeeld GPS gebruiken om hun kritische systemen te laten functioneren. Uit onderzoeken in de Verenigde Staten en het Verenigd Koninkrijk blijkt dat gebruikers een te lage bewustwording hebben als het gaat om de mate waarin GNSS in hun systemen is opgenomen. GNSS is een nutsvoorziening geworden, maar wel één die onzichtbaar is. [34]

For example, DHS officials and the GPS experts from academic and other research institutions we contacted cited a GPS incident in San Diego that impaired normal operations in the communications, maritime, and aviation sectors, even though it was a short-term disruption, which according to communications sector industry representatives, should not have impaired operations because of the sector's backup and mitigation measures. [35]

Kans op en gevolgen van uitval en/of verstoring onbekend bij gebruikers

Eerdere rapporten over de risico's van satellietuitval wezen op een onderschatting door gebruikers van de kans op en gevolgen van uitval of verstoring van signalen [36]. Deze lage risicoperceptie wordt niet ondersteund door

[34] Last, David, GNSS: The Present Imperfect, Inside GNSS, May 2010 & United States Government Accountability Office, GPS DISRUPTIONS. Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced, 2013

[35] United States Government Accountability Office, GPS disruptions. Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced, 2013

[36] Malcolm J Airst, GPS Network Timing Integrity, Mitre, 2010

de feitelijke groei van bijvoorbeeld de beschikbaarheid van jammers en apparatuur voor spoofing, integendeel zelfs. Zonder voldoende onderkenning van de kans en impact komen maatregelen te weinig van de grond.

Gebrek aan back-up opties bij uitval

GNSS wordt overal gebruikt, voor een veelheid aan toepassingen. Het is als het ware een (gratis) nutsvoorziening, waar bedrijven, overheden en particulieren op vertrouwen voor tijd, positie en/of navigatie. Vanwege het gemak en de lage kosten waarmee GNSS beschikbaar zijn, zijn er lang niet altijd (niet op GNSS gebaseerde) back-up voorzieningen voor het geval signalen uitvallen of verstoord raken, laat staan dat die getest en beoefend zijn. Dit is een trend die zich volgens Brits onderzoek ook in *'safety of life critical systems* 'voordoet.[37] De veerkracht, of *resilience,* van de organisatie tegen de gevolgen van uitval of verstoring is dan beperkt. Zo blijkt bijvoorbeeld bij Britse proeven in de maritieme wereld dat de bemanning niet goed was voorbereid op uitval van het GPS signaal en niet meer in staat was om met traditionele middelen te navigeren.[38]

Keteneffecten bij verstoring

Door het onderlinge verband tussen infrastructuur en netwerken ontstaan al snel keteneffecten. Haperende ontvangst van GPS plaats- en tijdsignalen heeft bijvoorbeeld een grote impact op tijdklokken die aanwezig zijn in technische systemen en processen. Voorbeelden hiervan zijn internetrouters en de synchronisatie van mobiele antenneterminals in communicatienetwerken voor GSM / 3G / 4G en het C2000 systeem van de hulpdiensten.[39] Ook de onderlinge afhankelijkheid van elektriciteitsvoorziening en GNSS is sterk.[40]

De uitval of verstoorde werking van deze systemen leidt al snel tot ongewenste gevolgen in andere vitale sectoren, of die nu zelf direct werden geraakt of niet. Zo rapporteerde de FAA in Amerikaans onderzoek, dat hoewel voor de luchtverkeersleiding zelf back-up voorzieningen zijn voor GPS, uitval van communicatievoorzieningen alsnog tot problemen leidt bij de mitigatie van eventuele incidenten. Althans, indien die communicatievoorzieningen afhankelijk zijn van GNSS en niet voorzien zijn van back-up faciliteiten.

Kortom, de vaardigheid van één sector om de effecten van verstoring of uitval te mitigeren, kunnen zeer goed andere sectoren raken.

---

[37] United States Government Accountability Office, GPS disruptions. Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced, 2013

[38] United States Government Accountability Office, GPS disruptions. Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced, 2013

[39] Ministerie van Infrastructuur en Milieu, Weerbaar tegen extreme zonneactiviteit. Gevolgen op aarde van extreme explosies op de zon, 2014 & U.S. Department of Homeland Security, National Risk Estimate: Risks to U.S. Critical Infrastructure from Global Positioning System Disruptions, Public Summary, 2013

[40] National Research Council (USA), Severe Space Weather Events – Understanding Societal and Economic Impacts, 2008

Bijlage 2 : De nul/één meting

Aan het begin van het IKUS project medio 2013 is er door het Agentschap Telecom (AT, Ministerie van Economische Zaken) een onderzoek uitgevoerd naar de kennis en het bewustzijn van Nederlandse bedrijven, organisaties en overheidsinstanties met betrekking tot het gebruik van GNSS. De resultaten van dit onderzoek vormt de basis voor de nul/één meting van het IKUS project.

De volgende sectoren hebben aan dit onderzoek deelgenomen.:

- Transport en logistiek.
- Financieel.
- Energie.
- Telecom.
- Vitale overheden.

De IKUS-eenmeting

Gedurende het IKUS project is het netwerk met betrokkenen aanzienlijk uitgebreid. Voor de kwantitatieve analyse van het IKUS-project zijn daarom ook functionarissen benaderd die oorspronkelijk niet in de nul-meting betrokken waren. De bevindingen van beide onderzoeken zijn apart en in zonderlinge samenhang geanalyseerd. Voor de IKUS-éénmeting medio 2015 zijn uiteindelijk 91 functionarissen personen aangeschreven. Deze respondenten zijn allen betrokken geweest bij de totstandkoming van de sectorrapportages of hebben deelgenomen aan sectorworkshops. Van de 91 aangeschrevenen hebben 28 respondenten (ruim 30 %) gereageerd.

Vanuit de volgende sectoren is een reactie ontvangen:

- Chemie
- Digitale overhead
- ICT
- Keren en Beheren Oppervlaktewater
- Luchtvaart
- Maritiem
- Nucleair
- Openbare Orde en Veiligheid
- Telecommunicatie
- Anders nl. Space sector

Van de 28 respondenten geeft 57% aan dat de vitale processen binnen hun sector afhankelijk zijn van GNSS en geeft 70% aan dat de primaire processen binnen de organisatie of branche gebruik maken van GNSS. Dit percentage ligt iets hoger dan tijdens de nulmeting. Toen gaf 63% (n=38) aan gebruik te maken van GNSS.

43% van de respondenten geeft aan dat het bewustzijn over de afhankelijkheden van GNSS vergroot is ten opzichte van twee jaar geleden en 35% geeft aan dat de kennis over het gebruik van GNSS binnen de organisatie gegroeid is in de afgelopen twee jaar. De bewustwording en kennis over het gebruik van GNSS is volgens de respondenten vergroot door: Training en opleiding (8%), Crisis en of incidenten (8%), Verhoogde aandacht voor GNSS binnen de organisatie (12%), Media (4%), IKUS traject (19%), anders (27%).

Tijdens de één-meting gaf 43% aan dat bij uitval van GNSS geen alternatieven beschikbaar waren. Dit percentage is gestegen ten opzichte van de nulmeting waarbij 31% van de respondenten aangaf een alternatief te hebben voor GNSS. Deze stijging kan duiden op een verbetering van het bewustzijn en kennis die in de afgelopen twee jaar heeft plaatsgevonden. De alternatieven die genoemd worden door respondenten zijn: EDLoran, een eigen atoomklok en een atoomklok op afstand via internet, DCF77.

De antwoorden op de vragen zoals gesteld in de éénmeting zijn hieronder opgenomen.

Toelichting nul/één meting

Achtergrond respondenten éénmeting

N=28	
Sector	Aantal respondenten
Chemie	1
Digitale overhead	1
ICT	4
Keren en Beheren Oppervlaktewater	4
Luchtvaart	3
Maritiem	9
Nucleair	1
Openbare Orde en Veiligheid	3
Telecommunicatie	1
Anders nl. Space sector	1

1. **Zijn vitale processen binnen uw sector afhankelijk van het gebruik van GNSS?**

(in lijn met de resultaten uit het programma 'Herijking Vitaal' door de Nationaal Coördinator Terrorismebestrijding en Veiligheid)

Antwoord	Aantal
Ja	16
Nee	11
Geen Antwoord	1

2. **Zijn primaire bedrijfsprocessen in uw bedrijf, branche of organisatie afhankelijk van het gebruik van GNSS?**

Antwoord	Aantal
Ja	20
Nee	5
Anders	2
Geen Antwoord	1

3. **Waarvoor gebruikt uw bedrijf, branche of organisatie GNSS?** *(meerdere antwoorden mogelijk)*

Antwoord	Aantal
Tijd	3
Navigatie	3
Positie	3
Navigatie en Positie	6
Navigatie, Positie en Tijd	8
Geen antwoord	4

4. **Hoe maakt uw bedrijf, branche of organisatie gebruik van GNSS?**

Antwoord	Aantal
Synchronisatie	4
Navigatie	10
Synchronisatie en Navigatie	2
Synchronisatie, Navigatie en Back-up	2
Synchronisatie en Back-up	1
Anders	4
Geen antwoord	4

5. **Welk systeem gebruikt uw bedrijf, branche of organisatie?**

Antwoord	Aantal
DGPS	9
EGNOS	3
WAAS	-
DGPS, EGNOS en WAAS	2
Anders*	5
Geen Antwoord	8

*Systemen die genoemd worden zijn: 06GPS, RTK, ELoran, LNR Global Net, VRS NetPos

6. **Is sinds de nulmeting in 2013 uw bewustzijn van mogelijke afhankelijkheden van GNSS verhoogd?**

Antwoord	Aantal
Ja	11
Nee	11
Geen antwoord	5

7. **Mijn kennis over de mate waarin mijn bedrijf, branche of organisatie GNSS gebruikt is de afgelopen twee jaar:** (*meerdere antwoorden mogelijk*)

Antwoord	Aantal
Groter geworden	8
Gelijk gebleven	8
Niet van toepassing	3
Geen antwoord	8

8. **Indien van toepassing, op welke wijze heeft u de afgelopen twee jaar meer kennis gekregen over GNSS gebruik?** *(meerdere antwoorden mogelijk)*

Antwoord	Aantal
Training en/of opleiding	2
Crisis en/of incidenten	2
Verhoogde aandacht voor GNSS binnen de organisatie	3
Media	2
IKUS traject (workshops, interviews, rapportage)	5
Anders	7
Geen antwoord	9

9. **Hoe wordt verstoring en/of manipulatie van het GNSS signaal gesignaleerd binnen uw organisatie?**

Antwoord	Aantal
Detectiesysteem	6
Uitval en/of incidenten	7
Dit kunnen wij niet signaleren	6
Anders	5
Geen antwoord	3

10. **Als het GNSS systeem lange tijd niet te gebruiken is, is er dan een alternatief voor uw bedrijf, branche of organisatie?**

Antwoord	Aantal
Ja	12
Nee	11
Geen antwoord	4

11. **Waaruit bestaat dit alternatief?** *(meerdere antwoorden mogelijk)*

Antwoord	Aantal
eLoran	2
Eigen atoomklok	1
Atoomklok op afstand via internet	3
DCF of andere uitgezonden tijdsignalen, anders dan van GPS	2
Anders*	8

*Antwoorden die genoemd worden zijn: handmatig, Total Station, oudere methoden, NTP

12. **Zijn er onderdelen of organisaties binnen uw bedrijf, branche of organisatie die al bezig zijn met oplossingen voor dit probleem van mogelijke lange uitval van het GNSS systeem?**

Antwoord	Aantal
Ja*	14
Nee	9
Geen antwoord	4

*Antwoorden die gegeven worden zijn: onderzoek, discussie, risico's in kaart brengen, EdLoran ontwikkelen

13. **Wat zijn de gevolgen voor uw bedrijf, branche of organisatie als deze systemen afhankelijk van GNSS niet meer functioneren?** *(Impactcriteria uit de nationale risicobeoordeling)*

Antwoord	Aantal
Catastrofaal	1
Zeer Ernstig	4
Ernstig	6
Aanzienlijk	2
Beperkt	8
Anders	1
Onbekend	1
Geen antwoord	5

14. **Ontstaat er een veiligheidsprobleem als GNSS niet meer werkt in uw bedrijf, branche of organisatie?**

Antwoord	Aantal
Ja	13
Ja,, maar weinig	5
Nee	5
Geen antwoord	3

15. **Kunt u aangeven in welke veiligheidsvlakken dit optreedt?** *(meerdere antwoorden mogelijk)*

Antwoord	Aantal
Fysieke veiligheid	13
Financieel economisch	9
Territoriale integriteit van Nederland	
Sociale stabiliteit/ maatschappelijke onrust	2
Ecologisch (gevolgen voor milieu)	5
Anders	5

Bijlage 3: Feed back deelnemers IKUS symposium

Op 8 oktober 2015 is het afsluitende IKUS symposium gehouden waarin de bevindingen van het project warden gepresenteerd en waarin in workshops dieper op de belangrijkste thema's werd ingegaan. Bij de afsluiting van het symposiums is aan alle deelnemers gevraagd om op een formulier, anoniem, antwoord te geven op onderstaande vragen. Hieronder treft de opsomming van de reacties per vraag.

Tijdens dit symposium is herhaaldelijk aangegeven dat satellietnavigatie, in bijzondere gevallen, dagenlang niet beschikbaar kan zijn.

- Wat is voor u de urgentie voor actie op deze onzekerheid ?

- Welke kwetsbaarheid in de vitale sectoren baart u het meeste zorg ?

- Wat gaat u nu doen om de GNSS-kwetsbaarheid in uw omgeving te verminderen, wat heeft u daarvoor nodig?

Wat is voor u de urgentie op deze onzekerheid?

- Medium tot hoog
- Hoog
- Moet nog meer tastbaar worden, hoe verhoudt zich bijvoordbeeld een piek in van zonneactiviteit voor Nederland (noorden breedte) t.o.v. standaard situatie in Noord Scandinavische landen of Alaska
- Het is belangrijk, niet direct urgent
- Dit onder de aandacht brengen bij mijn leiding (MT), aankaarten bij het verantwoordelijk ministerie
- Zorgen dat het in de risicoanalyses een duidelijke plek krijgt
- Hoog, ondermeer ivm Vessel Traffic Management in havens en shipping lanes. Ook voor waterkeringen, sluizen, bruggen etc. die op afstand elektronisch bediend worden
- Bewustwording heel belangrijk
- Geen specifieke urgentie
- Laag
- Laag
- 'we' zijn niet voorbereid op een grootschalige zonnestorm. Althans we weten niet of we dat zijn.
- Toenemende afhankelijkheid van individuele systemen + verwijderen van oude systemen + afhankelijkheden in de sector

Welke kwetsbaarheden in de vitale sectoren baart u het meeste zorgen?

- Ontstaan van eilanden qua communicatie door uitval van interconnectie vanwege clockingverschillen
- Voice en data
- Navigatie voor luchtvaart en vervoer over water
- De onbewuste afhankelijkheid
- Alternatieve oplossingen voor GPS in de maritieme sector en de snelheid waarmee deze beschikbaar komen
- De cascade effecten, het ontstaan van chaos, gebrekkige communicatie en daaraan verbonden veiligheidsvraagstukken
- VTM en vele schepen en boorplatforms o.a. diepzee olieboren gebruiken dynamic positioning op basis van satellietnavigatie. Als dit uitvalt kunnen grote problemen ontstaan.
- Energie, de ketenafhankelijkheid hiervan is groot
- De mogelijke cascade effecten en beperkte inzichten daarover
- Indirecte kwetsbaarheid van Telecommunicatie
- Energie en Telecom
- Gebrek aan crisisbeheersingsmechanismen / Protocollen in geval van schadelijke zonneactiviteit.

- (locale) jamming / Spoofing

Wat gaat u nu doen om de GNSS-Kwetsbaarheden in uw omgeving te verminderen, wat heeft u daarvoor nodig?

- Om slagkracht te hebben: Nationale en ook internationale opererende referentieklokken waar op kan worden teruggevallen
- Intern kenbaar maken / Overdragen
- Onze GNSS kwetsbaarheid is al laag. Nog wel enige zorg rondom afhankelijkheid voor (overheids-) hulpdiensten
- Vergroten overbruggingstijd bij onbeschikbaarheid GNSS (bijv. NTP) nodig: Praktische voorbeelden
- Goede bewustwording (inter) nationale visie op hoe hiermee om te gaan. Geld / Funding
- Factsheet met communicatie over risico's effecten en maatregelen
- Navragen in hoeverre scheepvaart en havens zijn aangehaakt bij Galileo PRS. Daarnaast graag presentaties bij DGB Maritieme Zaken.
- Rapportage IKUS gebruiken als input document
- Welke sectoren hebben welke mate van kwetsbaarheid voor GNSS verstoringen
- Controle tijdsynchronisatie, controle ketenafhankelijkheid
- Bewustwording
- Kennis opbouwen onderzoek, maatregelen implementeren
- Awareness / aandacht, nader onderzoek. Nodig: netwerk met specialisten

Bijlage 4: Betrokkenen in het traject

Naam	Organisatie
Dhr. Addea	Ministerie van Veiligheid en Justitie
Dhr. Aldenkamp	Amsterdam Airport Schiphol
Dhr. Akkerhuis	NLnetLabs
Dhr. Bareman	Vereniging van de Nederlandse Chemische Industrie
Dhr. Bentvelsen	Unie van Waterschappen
Dhr. Bentvelsen	Uitvoeringsinstituut Werknemers Verzekeringen
Dhr. Bolhuis	Ziggo
Dhr. Boogaard	Ministerie Veiligheid en Justitie
Dhr. Bos	Rijkswaterstaat
Dhr. de Bosch	Luchtverkeersleiding Nederland
Dhr. van de Graaf	Ministerie van Infrastructuur en Milieu
Dhr. de Vries	KPN
Mevr. deKoninck	Ministerie van Financien
Dhr. den Beejen	Tele2
Dhr. Doeland	Betaalvereniging Nederland
Dhr. Donker	Lyondellbasell
Dhr. Doornbosch	Gasunie Transport Services B.V.
Dhr. de Dood	Stedin Netbeheer B.V.
Dhr. Dorst	TenneT TSO B.V.
Dhr. Ehlert	Rijkswaterstaat
Dhr. Folkers	Folkline
Dhr. Fokker	DELTA Netwerkbedrijf B.V.
Dhr. Goslings	AMS-IX
Mevr. Gielens	Vewin
Mevr. Hannema	Equens SE
Dhr. Halman	Shell Nederland
Dhr. Hamelink	NCTV, Ministerie van Veiligheid en Justitie
Dhr. Herpt	TATA steel
Dhr. Hollanders	Hoogheemraadschap van Delfland
Dhr. Holthuis	Luchtverkeersleiding Nederland
Dhr. Hondebrink	Ministerie van Economische Zaken
Dhr. Hoogeland	Waterschap Rijnland
Dhr. Hoogenboom	Rijkswaterstaat
Dhr. Huisman	Kadaster
Dhr. IJpelaar	Waterschap Aa en Maas
Dhr. Inesia	Logius
Dhr. de Dood	Stedin Netbeheer B.V.
Dhr. Jansen	KPN
Dhr. Janssen	Logius
Dhr. Jeen	ExxonMobil
Dhr. Jung	Ministerie van Infrastructuur en Milieu
Dhr. Keizer	Urenco
Dhr. Klinkenberg	Ministerie van Defensie
Dhr. Kloppenburg	Aircraft Fuel Supply
Dhr. Kooij	Kadaster
Dhr. Ligthart	Ministerie van Veiligheid en Justitie
Dhr. Lippens	DOW Chemical
Dhr. Maltha	Ministerie van Infrastructuur en Milieu
Dhr. Miggelbrink	Ministerie van Infrastructuur en Milieu
Dhr. Muller	TenneT TSO B.V.
Dhr. Munnix	Enexis B.V.
Dhr. Mutsaers	Ministerie van Veiligheid en Justitie
Dhr. Nacinovic	Meldkamer Diensten Centrum
Dhr. Nieuwenhuis	Rijkswaterstaat
Dhr. Nieuwenhuizen	Ministerie van Veiligheid en Justitie
Dhr. Nieuwland	Liander N.V

Dhr. Oskam	Agentschap Telecom
Dhr. Paalman	Ministerie van Economische Zaken
Dhr. Paap	Rijkswaterstaat
Dhr. Pas	Kustwachtcentrum
Dhr. Pepping	Ministerie van Economische Zaken
Dhr. Rambi	Liander N.V.
Mevr. Reinders	Ministerie van Infrastructuur en Milieu
Dhr. Roovers	Netbeheer Nederland
Dhr. Rijkschroeff	Rijkswaterstaat
Dhr. Schaper	Wetterskip Fryslân
Dhr. Scheffers	Ministerie Infrastructuur en Milieu
Dhr. Schoenmaker	Vereniging Nederlandse Verkeersvliegers
Dhr. Schraver	Autoriteit Nucleaire Veiligheid en Stralingsbescherming
Dhr. Slegtenhorst	Havenbedrijf Rotterdam/Port of Rotterdam
Dhr. Smit	ABNAMRO bank
Dhr. Steltman	DHPA
Dhr. Strous	De Nederlandsche Bank
Dhr. Terpstra	Amsterdam Airport Schiphol
Dhr. Timmermans	NCTV, Ministerie van Veiligheid en Justitie
Dhr. Tintel	Ministerie van Infrastructuur en Milieu
Dhr. Tynes	Vodafone
Dhr. van Andel	Tata Steel
Dhr. van Brussel	Ministerie van Infrastructuur en Milieu

Dhr. van Buuren	Nederlands Loodswezen
Dhr. ing. van Bruchem	Netbeheer Nederland
Dhr. van den Oord	Koninklijk Nederlands Meteorologisch Instituut
Dhr. van der Helm	Ministerie van Infrastructuur en Milieu
Dhr. van der Hoek	Kadaster
Dhr. van der Linden	Amsterdam Airport Schiphol
Dhr. van der Plas	Koninklijke Luchtvaart Maatschappij NV
Dhr. van der Veen	Binck bank
Dhr. van Hekke	Ministerie van Infrastructuur en Milieu
Dhr. van Osselen	Ministerie van Veiligheid en Justitie
Dhr. van Oudheusden	Ministerie van Infrastructuur en Milieu
Dhr. Verheijen	Luchtverkeersleiding Nederland
Dhr. Vermeulen	Rijkswaterstaat
Dhr. Voesten	Ziggo
Dhr. Vroege	Meldkamer Diensten Centrum
Dhr. Wieleman	Ministerie van Economische Zaken
Dhr. Wisse	Nederlandse Kustwacht
Mevr. Buijtendijk	NCTV, Ministerie van Veiligheid en Justitie
Mevr. Hebbink	NCTV, Ministerie van Veiligheid en Justitie
Mevr. Baron	Ministerie Infrastructuur en Milieu
Mevr. Snoerwang	Amsterdam Airport Schiphol
Mevr. van der Veen	Binck bank
Mevr. van Zuilenkom	Ministerie Infrastructuur en Milieu

Bijlage 5: Begrippen en afkortingen

Afkortingen	
BCP	Business Continuity Planning
BzK	Ministerie van Binnenlandse zaken en Koninkrijksrelaties
CAET	Capaciteitsanalyse Elektriciteit en Telecom
DMO	Direct Mode Operations
GLONASS	GLObal'naya NAvigatsionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
IenM	Ministerie van Infrastructuur en Milieu
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
TETRA	Terrestrial Trunked Radio
TLP	Traffic Light Protocol
VenJ	Ministerie van Veiligheid en Justistie
VN	Verenigde Naties
WOB	Wet openbaarheid van Bestuur

Begrippen	
Beidou/COMPASS	Chinees GNSS-systeem
Galileo	Europees GNSS-systeem
Global Navigation Satellite Systems	Een systeem voor radionavigatie waarbij gebruik wordt gemaakt van satellieten en dat een wereldwijde dekking heeft.
Global Positioning System	Amerikaans GNSS-systeem
GLObal'naya NAvigatsionnaya Sputnikovaya Sistema	Russisch GNSS-systeem
Navigatie	Navigatie betekent dat de positie van de bewegende antenne "continu" (bijv. elke seconde) wordt berekend. Als hiervoor een gewone code-ontvanger wordt

	gebruikt geeft dit posities tot op enkele meters (navigatie). Met een fase-ontvanger (plus DGPS referentiestation) is in principe een kwaliteit van centimeter mogelijk (precieze navigatie).
Plaatsbepaling	Bij plaatsbepaling wordt de locatie van een stilstaande GPS-ontvanger berekend met behulp van het gecodeerde GPS-signaal. De kwaliteit hiervan varieert van één tot enkele meters, afhankelijk van of een referentiesignaal wordt gebruikt.
Tijdsbepaling	De GNSS-satellieten zenden, naast bet gecodeerde stuk voor positiebepaling, ook de zogenaamde navigatieboodschap uit. Eén van de dingen die hierin staan is een boognauwkeurige 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.
Vitale sector	Een sector die bij uitval (van onderdelen van de sector) maatschappelijke ontwrichting veroorzaakt door grote economische schade, vele doden of maatschappelijke onrust.
Zonnestorm	Zonnevlammen worden veroorzaakt door magnetische uitbarstingen op de zon, waarbij vaak een groot aantal elektrisch geladen deeltjes aan het oppervlak ontsnappen. Als een wolk van deze deeltjes de aarde bereikt (meestal ongeveer twee dagen na een zonnevlam) wordt er gesproken van een zonnestorm.

Bijlage 6: IKUS Factsheet

Aanleiding

Jaarlijks laat de overheid via de zogenaamde 'Nationale Risicobeoordeling' crisisgevoelige scenario's analyseren, om de weerbaarheid tegen potentieel verstorende incidenten, rampen en crises te vergroten. In 2012 is het scenario 'satellietuitval vanwege een zonnestorm' door externe deskundigen geanalyseerd. Het blijkt dat extreme zonneactiviteit kan leiden tot verstoringen bij nagenoeg alle vitale sectoren via directe en indirecte gevolgen (bijvoorbeeld als gevolg van uitval satellieten). Daarom heeft het kabinet maatregelen aangekondigd om de weerbaarheid tegen de gevolgen van extreme zonneactiviteit te vergroten.

Doel project

Het project Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie (IKUS) van het ministerie van Infrastructuur & Milieu (IenM) richt zich op Global Navigation Satellite Systems (of GNSS), zoals GPS, GLONASS en Galileo en de afhankelijkheid van vitale sectoren hiervan. Doel van IKUS is de weerbaarheid van vitale sectoren tegen uitval van GNSS inzichtelijk te maken en zo nodig te vergroten.

GNSS wordt in alle publieke en private vitale sectoren gebruikt voor positie- en/of tijdsbepaling. Deze laatste categorie wordt soms vergeten, maar wordt in vitale sectoren zelfs meer gebruikt dan positiebepaling, blijkt uit eerder onderzoek. Ook is er in toenemende mate sprake van GNSS-toepassing waarbij de eigenaar of gebruiker dat niet eens meer onderkent, met name in *embedded* systemen

Na afloop van het IKUS traject zijn:

- continuiteitsmanagers en gebruikers van apparatuur en systemen in vitale sectoren, die afhankelijk zijn van GNSS, zich bewust van de kwetsbaarheden;
- de kwetsbaarheden met betrekking tot uitval GNSS in kaart gebracht;
- bestaande en/of nieuw te ontwikkelen preventieve maatregelen en terugvalopties (incl. globale kostenindicaties) t.a.v. uitval of verstoring van GNSS in kaart gebracht.

De uitvoering van het project is in handen van Capgemini Consulting.

Wat is GNSS?

Satellietnavigatie is een vorm van radionavigatie waarbij gebruik wordt gemaakt van satellieten. Tegenwoordig zijn er meerdere systemen, waaronder GPS (VS), Galileo (EU), GLONASS (Rusland) en Beidou (China).Een systeem dat wereldwijde dekking heeft, wordt ook wel aangeduid als GNSS of Global Navigation Satellite System.

Het werkingsprincipe van satellietnavigatie is dat door kruispeilingen van satellietsignalen een nauwkeurige positie kan worden bepaald. Het signaal bevat hiertoe een nauwkeurige timestamp, waardoor een ontvanger ook gebruikt kan worden om de exacte tijd te bepalen. Het signaal is, door het beperkte zendvermogen van de satelliet en de lange transmissieweg, gevoelig voor verstoringen. Deze verstoring kan veroorzaakt worden door defecten in het systeem, maar ook door natuurverschijnselen (zonnestorm) of opzettelijke signaalstoring. Het zonnestormscenario uit de Nationale Risicobeoordeling is de aanleiding voor het IKUS-project, maar de onderzoeksvraag is verbreed naar de uitval van GNSS-signaal in zijn algemeenheid, ongeacht de oorzaak en richt zich enkel op de gevolgen.

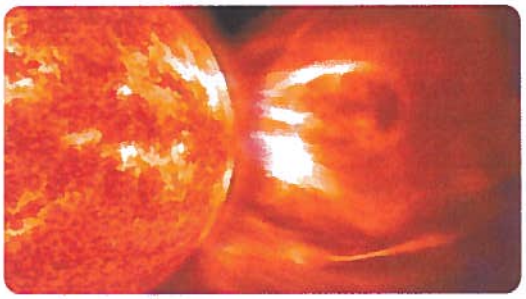
Andere functionaliteiten die gebruik maken van satelliet technologie, zoals aardobservatie, satellietcommunicatie en militaire communicatie zijn out-of-scope. Ook de directe effecten van zonnestormen op elektromagnetische systemen, anders dan GNSS-signalen, vallen buiten de scope van dit onderzoek.

Impact op sectoren

Het project IKUS is opgebouwd uit een voorbereidende fase, waarin op basis van de meningen van experts een eerste inventarisatie wordt uitgevoerd. Vervolgens worden in de uitvoeringsfase alle vitale sectoren benaderd voor een aantal interviews, een sectorale workshop en een workshop voor meerdere sectoren (ter bevordering van de kruisbestuiving). Elk sectoraal traject eindigt met een deelrapport, wat aan het eind van het project uitmondt in een synthese rapport. Sectorvertegenwoordigers van vakdepartementen zullen gedurende dit traject worden gevraagd om aan een interview en/of 1 a 2 workshops deel te nemen en het concept-sectorrapport te toetsen.

Voorts voorziet het project IKUS in een communicatieplan om sectoren, vakdepartementen en andere stakeholders te informeren over afhankelijkheden, kwetsbaarheden en maatregelen bij uitval en/of verstoring van GNSS en over de voortgang van IKUS zelf.

Om onnodige dubbele bevraging van sectoren te voorkomen, werkt het IKUS-project samen met zowel andere op satellietuitval en zonnestorm gerichte trajecten (b.v. KNMI, EZ, V&J) als op de vitale sectoren gerichte projecten (o.a. herijking vitaal).



Geclusterde aanpak

Het project IKUS volgt een geclusterde aanpak waarbij twee clusters van vitale sectoren onderzocht worden Niet alleen maatschappelijke relevantie, afhankelijkheid en kwetsbaarheid zijn hierbij van belang, ook de mate waarin kritieke processen reeds helder zijn gedefinieerd. IKUS richt zich op GNSS-afhankelijkheid van kritieke processen.

Op basis van deskresearch en een expertmeeting vielen de volgende sectoren binnen het eerste cluster (afgerond begin 2015): Elektriciteit, Gas, Drinkwater, Financiën, Keren en Beheren Oppervlaktewater, Openbare Orde en Veiligheid, Telecommunicatie, Digitale Overheid en de Rotterdamse haven. Het tweede cluster (start begin 2015) bestaat uit de volgende sectoren: Chemie, Nucleair, Olie, ICT en Luchtvaart

Elke van deze (sub-)sectoren benaderen we vanuit een standaardaanpak, met oog voor de specifieke kenmerken van de sector en het bijbehorende vakdepartement, in overleg met vakdepartement en sectorvertegenwoordiging.

Vertrouwelijke informatie

Lerend van eerdere ervaringen, werkt het ministerie van IenM voor IKUS met een 'black box', met als doel dat bedrijfsgeheime of anderszins gevoelige informatie te laten waar het hoort. Informatie wordt op basis van '*need to know*' geregistreerd en verspreid. Om dit vorm te geven, hanteren we een breed geaccepteerd protocol, te weten het *Traffic Light Protocol* (TLP). Hierin wordt informatie door de bron (b.v. expert, sector) naar mate van vertrouwelijkheid geclassificeerd in Rood (geheim), Amber (alleen delen in vertrouwde kring), Groen (publiceerbaar) en Wit (publiek).

Bij elk gesprek en elke sessie licht het projectteam van Capgemini dit protocol toe en registreert en rapporteert vervolgens alleen Groene en Witte informatie. De eindrapportages per sector en het syntheserapport zullen ook op het niveau Groen en Wit zijn. Daarnaast rapporteert Capgemini aan IenM tussentijds enkel op procesvoortgang.

Contactpersonen IKUS

Ministerie van Infrastructuur en Milieu:

Erik Kliggelbrink
(gedelegeerd opdrachtgever)

Uitvoerend projectteam:

Peter Kwant
(operationeel projectleider Capgemini)
Email: peter.kwant@capgemini.com