

RGI-149 Geo-info to-go - Geoinformatievoorziening ter plekke

Deelproject WP4

Onderzoek naar Robuustheid Radiofrequentie netwerken tbv. functies Plaatsbepaling, Navigatie & Tijdsynchronisatie(PNT)

Versiebeheer

<i>Datum</i>	<i>Versie</i>	<i>Auteur</i>	<i>Opmerkingen</i>
25-03-2007	0.1	Arnold-Kees van Rongen	Vorbereiding werkzaamheden raamwerk WP4 -PNT
20-05-2007	0.2	idem	Document aangemaakt
24-05-2007	1.0	idem	Def. Correcties / Aanvullingen nav. Pl.v Aanpak WP 4 overleg te Delft dd. 23-05-2007
22-08-2007	2.0	idem	Onderzoek & 1 ^{ste} Concept versie Rapportage WP4-PNT
20-09-2007	2.1	idem	Aanpassingen Rapportage n.a.v. interviews met Yucat & Prov.Gelderland + verzending concept aan RGI-149 Project deelnemers
14-12-2007	2.2	idem	Definitieve versie WP4-PNT + verzending concept aan RGI-149 Project deelnemers

Copyright © 2007 Mobi-Spot B.V. All rights reserved.

INHOUDSTABEL

INLEIDING	3-4
DOELSTELLING.....	
UITGANGSPUNTEN EN ONDERZOEKSVRAGEN	
PROBLEEMSTELLING	4-5
ALGEMENE VERKENNING & BESCHRIJVING PROJECT "BUITEN BETER"	
UITVOERING ONDERZOEK	5-18
PLAATSBEPALING, NAVIGATIE & TIJDSYNCHRONISATIE TECHNIEKEN(PNT).....	
BEANTWOORDING ONDERZOEKSVRAGEN	
ORGANISATIE GEO-ICT; PNT KETENPARTNERSHIPS	19-24
PROJECTVISIE EN SAMENWERKINGSMODEL	
APPENDICES & REFERENTIES:	25-26

1 INLEIDING

Hoofdvraag voor het gehele *project RGI 149: Geo-info To-go* is: "Op welke wijze dient geo-informatie in het Project "Buiten Beter" te worden aangeleverd aan toezichthouders en opsporingsambtenaren in het buitengebied, gegeven hun locatie, beperking draadloze communicatie en minimale gebruikersinterface?" Binnen deze hoofdvraag concentreert Deelproject WP 4 zich op de gewenste beschikbaarheid, nauwkeurigheid en betrouwbaarheid van locatie informatie. *De rapportage zal deels in de nederlandse en/of engelse taal geschieden.*

Als testcase wordt het "Beter Buiten" systeem van de provincie Gelderland gebruikt. Het systeem voorziet in de informatiebehoefte van toezichthouders en opsporingsambtenaren in het veld. Via Smart-phones en PDA wordt de informatie ontsloten en kunnen meldingen direct en ter plekke verwerkt worden. Het gebruik van o.a. GNSS (Global Navigation Satellite Systems) waaronder GPS (Global Positioning System) spelen hierbij een centrale rol in combinatie met topografische en kadastrale gegevens en draadloze informatie & telecommunicatie / internet netwerken. De informatie wordt in centrale database servers opgeslagen en beheerd alsmede weer gedistribueerd en aangeleverd aan toezichthouders en opsporingsambtenaren in het buitengebied, gegeven hun locatie. Alle informatie wordt gebruikt door verschillende organisaties binnen de provincie Gelderland, zoals bijvoorbeeld milieu-opsporingsambtenaren bij gemeenten en politie.

De Hoofdwerkzaamheden voor WP 4 zijn als volgt gedefinieerd:

A) Binnen het kader van Project "Buiten Beter", begeleiding en onderzoek naar aanbod en robuustheid van bestaande (proven technology) mobiele Radio Frequentie(RF) Plaatsbepaling, Navigatie & Tijdsynchronisatie (PNT) netwerk infrastructuur met aanbeveling van de meest optimale keuze mix van RF PNT netwerken en/of autonome systemen ten behoeve van gebruikers in het project "Buiten Beter".

B) Beschrijving van een organisatorisch Geo-ICT gebaseerde "One-Stop Solution" Location Intelligent Business Services Supply-chain Partnership en informatie model met als doelstelling optimale aanbod van producten en diensten aan gebruikers in het project "Buiten Beter"

1.1 Overige betrokken partijen bij de uitvoering van werkpakket (WP 4) van Project RGI-149: Geo-Info To-go zijn :

- Provincie Gelderland - Henk Janssen
- TU Delft -OTB- GIS – Edward Verbree
- Yucat – Barry Peet

2 DOELSTELLING

Mobi-Spot heeft de navolgende doelstellingen gedefinieerd:

1. Kennisoverdracht en meer inzicht verschaffen alsmede bewustwording vergroten bij gebruikers mbt. "Single Point of Failure" risico's bij gebruik van Positiebepaling, Navigatie & Tijdsynchronisatie(PNT) netwerken in GIS en GEO systemen in het algemeen en in kritische applicatie omgevingen op het gebied van handhaving en inspectie in het bijzonder.
2. Bevorderen van Geo-ICT gebaseerde "One-Stop Solution" Location Intelligent Business Services Supply-chain Partnership samenwerkingsverbanden
3. Een conformiteits-check m.b.t het nog te introduceren European Radio Navigation Plan (ERNP) Beleids & strategie document in Europa.
4. Uitwisseling van kennis met andere relevante RGI projecten. Een bijdrage leveren aan de innovaties binnen het geo-werkveld.

3 ONDERZOEKSVRAGEN

De hierboven geformuleerde doelstellingen leiden tot de volgende 5 onderzoeksvragen:

1. Welke verbeteringen zijn gewenst met betrekking tot mobiele PNT functies (In-Car en/of Personal) ter ondersteuning van GEO-ICT applicaties bij inspectie en handhaving?

2. Hoe operationeel kritisch zijn PNT functies bij GEO-ICT applicaties bij inspectie en handhaving?
3. Gelet op het "Single Point of Failure" risico, dienen PNT GEO-ICT systemen enkel- of dubbelvoudig te worden uitgevoerd? En dient hierbij een onderscheid gemaakt te worden tussen In-Car en Personal PNT gebruikers?
4. Wat is qua robuustheid & integriteit, de meest optimale keuze-mix van RF-PNT netwerk en/of autonome systeem ten behoeve van gebruikers in het project "Buiten Beter"? Conformiteitscheck met het European Radio Navigation Plan (ERNP) Beleids & strategie document in Europa.
5. Zijn gebruikers in het project "Buiten Beter" gediend bij het aanbod van een organisatorisch GEO-ICT gebaseerde "One-Stop Solution" Location Intelligent Business Services Supply-chain Partnership samenwerkings- en informatie model?

4 ALGEMENE VERKENNING & BESCHRIJVING: WERKOMGEVING PROJECT "BUITEN BETER"

Relevant voor bovenvermelde WP 4 gestelde onderzoeksvragen bij de opzet van een nieuwe testomgeving *WP 5 (Yucat)* om de werking van handheld devices te onderzoeken op de aangeboden geografische informatie binnen het Project "Buiten Beter" zijn; o.a. de **Technologische** functies van **Plaatsbepaling, Navigatie en Tijdsynchronisatie(PNT)**. Dit in aanvulling op de uitkomsten en ter ondersteuning van in overige deelproject Workpackages beschreven huidige en nog gewenste beschikbaarheid (gebruik en organisatie) van Geo-informatie -in welke vorm dan ook - bij toezichthouders en opsporingsambtenaren vanuit een integrale benadering van de fysieke omgeving van het brede milieugebied.

Eea. heeft ook direct te maken met het onderzoek van *WP 3 (TU Delft-OTB)* naar het aanbod, de functionaliteit en robuustheid van de huidige en toekomstige generatie persoonsgebonden PDA's en Smartphones mbt. de functies Plaatsbepaling, Navigatie en Tijdsynchronisatie(PNT).

In *WP2* (Provincie Gelderland) wordt onderzoek verricht naar de gewenste geo-informatievoorziening vanuit de problematiek van 'Buiten Beter'. Daarvoor is het noodzakelijk de informatiebehoefte van de integrale toezichthouder/handhaver van milieuwetgeving in kaart te brengen. In dit project wordt deze kennis aangeleverd in de persoon van Henk Janssen vanuit zijn ervaringen van het milieubeleidsterrein.

In de slutfase van de *WP 4* rapportage is ook gekeken naar een beschrijving van een **Organisatorisch** Geo-ICT gebaseerde "One-Stop Solution" Location Intelligent Business Services Supply-chain Partnership en informatie Model, met als doelstelling optimale aanbod van producten en diensten aan gebruikers in het project "Buiten Beter" te bundelen.

Binnen het beleidsterrein van het brede milieu worden onderdelen met zg. "*Kleuren sporen*" aangeduid:

- Grijs milieu:* uitvoering wet milieubeheer (gericht op bedrijven) en besluiten
- Groen milieu:* uitvoering natuurwetten, flora- en faunawet, natuurbeschermingswet etc.
- Blauw milieu:* wet verontreiniging oppervlaktewateren en besluiten
- Rood milieu:* wet op de ruimtelijke ordening, wet bodembescherming, externe veiligheid, bouwstoffenbesluit etc.

Op dit ogenblik zijn de meeste toezichthouders en handhavers opgeleid Toezicht te houden, Opsporings- en Handhavingsactiviteiten te verrichten in 1 kleurspoor. Onder druk van veranderende wetgeving: de *Wet Algemene Regelen Omgevings-recht (WABO)* ontstaan er opleidingen voor een meer integraler toezicht en handhaving. Men leert vanuit verschillende gezichtshoeken –*integraal* – naar de omgeving kijken en komt men van daaruit tot acties. In toemende mate zal men specialisten of senior-medewerkers gaan inschakelen die iets meer afweten van een bepaald stukje toezichts-/opsporings wetgeving.

Ook wordt als een indeling gehanteerd: inrichtinggebonden overtredingen en vrije-veld delicten.

Bij inrichtinggebonden controles door toezichthouders en handhavers wordt onderscheid gemaakt tussen een AMvB (*Algemene Maatregel van Bestuur*)bedrijf of een *Vergunningplichtig* bedrijf.

Een AMvB-bedrijf doet een melding aan de gemeente en de gemeente beoordeelt of zij deze melding al dan niet accepteert.

Vergunningplichtige bedrijven krijgen op basis van hun aanvraag hun vergunning waarin maatwerk wordt geleverd op hun specifieke situatie.

Toezicht is informatie verzamelen, om te beoordelen of de bestaande of aangetroffen situatie al dan niet overeenkomt met het door de overheid toegestane planologische ruimte, milieuruimte, fysieke ruimte. Bij de beoordeling van de afwijking van de vergunde situatie wordt bepaald of de afwijking achteraf gelegaliseerd kan worden of dat teruggevallen moet worden op de vergunde situatie. Is dat laatste het geval dan zal via handhaving getracht worden de inrichtingshouder te bewegen het bestaande terug te buigen naar het vergunde.

5 **TECHNIEK: PLAATSBEPALING, NAVIGATIE EN TIJDSYNCHRONISATIE(PNT)**

In WP 4 zijn de werkzaamheden binnen het project "Buiten Beter" gericht op Technologische beantwoording van in sub-paragraaf 3 gestelde onderzoeksvragen nl:

- a. Overzicht van de robuustheid & integriteit van PNT radionetwerken: om vast te stellen of er verbeteringen gewenst zijn?
- b. Hoe operationeel kritisch zijn PNT functies in het gebruik m.a.w. het "Single Point of Failure" risico?
- c. Wat is qua robuustheid & integriteit, de meest optimale keuze-mix van RF-PNT netwerk en/of autonome systeem?
- d. Conformiteitscheck met het European Radio Navigation Plan (ERNP) Beleids & strategie document in Europa.

Uitgangspunt bij het onderzoek in WP 4 is het gegeven; dat het "Buiten Beter" project systeem voorziet in de informatiebehoeften van toezichhouders en opsporingsambtenaren in het veld. Via Smart-phones en PDA wordt de informatie ontsloten en kunnen meldingen direct en ter plekke verwerkt worden.

Voor het doorgeven van lokatie en tijd gegevens wordt op dit ogenblik gebruik gemaakt van het GNSS (Global Navigation Satellite Systems) netwerk, waarbij nu meer specifiek het GPS (Global Positioning System) een centrale rol speelt; dit laatste in combinatie met topografische en kadastrale gegevens met draadloze informatie & telecommunicatie / internet netwerken.

In het veld wordt met behulp van draagbare Pocket PC's (PDA's) een draadloze verbinding voor communicatie van spraak, data en waar nodig stilstaand beeld(foto's) tot stand gebracht met het centrale Provinciale Coördinatie kantoor Gelderland in Arnhem; die op haar beurt weer -via Internet- met de diverse aangesloten Gemeentekantoren communiceert en informeert (in logistieke termen uitgedrukt: een zg. Hub & Spoke model). Er wordt gebruik gemaakt van het landelijke dekkend cellulaire GRPS netwerk. Bij de informatie uitwisseling van genoemde gegevens wordt zoveel mogelijk gebruik gemaakt van specifiek per "kleur spoor" door de firma Yucat ontworpen digitale standaard formulieren, om de applicaties zo gebruikersvriendelijk en voor verdere interne informatie afwikkeling, productief mogelijk te maken. In totaal zijn bij het Project "Buiten Beter" 40 organisaties met ca. 150 mensen betrokken.

Teneinde, een goed inzicht te verkrijgen in lokatie relevante **Plaatsbepaling, Navigatie en Tijdsynchronisatie (PNT)** functies, zal in sub-paragraaf 5.1 een engelstalige uiteenzetting worden gegeven van belangrijke zaken mbt. PNT diensten, zoals tijd- en plaats gevoeligheid voor diverse applicaties alsook inzicht worden verkregen van de 4 belangrijkste functies van PNT ten behoeve werkzaamheden in het veld m.a.w. buitengebieden. Ook wordt ingegaan op kwetsbaarheid & betrouwbaarheid van op Satellieten(GNSS) gebaseerde PNT applicaties zoals GPS.

5.1 **Location based services Profiles & Required Navigation Performance specifications for accuracy, integrity, availability and continuity**

In relation to the "Buiten Beter" project, this section contains the following three sub-sections:

- a) *Brief description of current PNT systems in use*
- b) *Creating User awareness of potential "Single-point of Failure" PNT system risks*
- c) *Reducing Vulnerabilities & Risk Considerations re. PNT system robustness*

a) Brief description of current PNT systems in use

In principle, we can determine **2 types of Positioning, Navigation & Timing (PNT)** technologies:

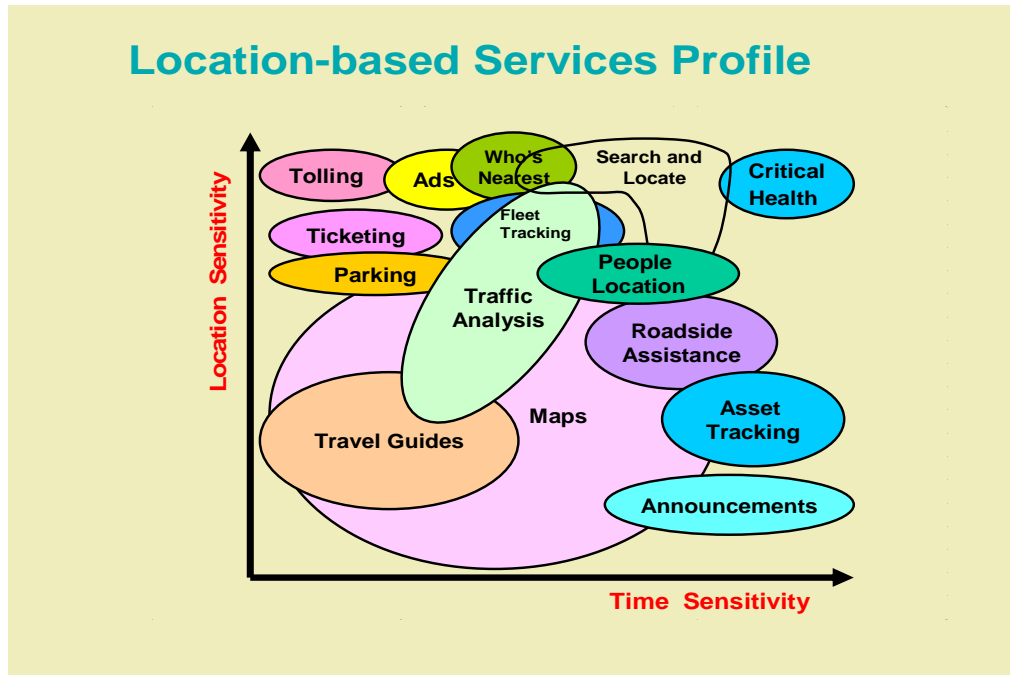
- *Wide-area multi-modal Radio-frequency based network infrastructure PNT systems*
- *Autonomous Sensor based Inertial/Dead Reckoning PNT systems*

Today, there are 3 classes of **Wide-area multi-modal Radio Positioning network systems** available, in the first place the Satellite-based network PNT systems (GNSS) like the United States GPS and the Russian GLONASS, secondly the Terrestrial-based network PNT systems such as Loran-C, the Russian equivalent Chayka and in the last place, mobile Telecommunication Cell-ID networks. Taken strictly; the latter Cell-ID network infrastructures where position determination is based on triangulation calculations between individual GSM/GPRS /UMTS/HSDPA Cell base stations, each especially fitted out with appropriate Location intelligent software algorithms; are -by the professional PNT community- **not considered to be “dedicated” PNT Radio Positioning network systems**. In principle, mobile terrestrial Telecommunication Cell-ID network infrastructures such as GSM/GPRS/UMTS/HSDPA etc. are *primarily designed and built* to offer mobile RF based transmission bandwidths and speed to facilitate transport and distribution of speech, data and video content, and are in principle **NOT** designed and optimized for Positioning, Navigation & Timing (PNT) functions! The fact, that terrestrial mobile Cell-ID Telecommunication network infrastructures can however assist and facilitate PNT functions by means of triangulation calculation algorithms is accepted, as long as users realise and are also prepared to accept *some drawbacks regarding accuracy and integrity of the PNT information provided*; in particular when considering critical civil applications in for instance *Security and Safety environments*, where risks of vulnerability and interference of RF Satellite PNT signals - if possible- must be avoided or augmented with a dissimilar i.e. Non-satellite based PNT system. To put it differently; although it is basically possible to use Cell-ID Tele-communication network infrastructures for position determination, this infrastructure is not optimised for PNT.

In addition to RF based network infrastructure PNT systems, we also consider **Autonomous micro-electromechanical (MEMS) PNT systems i.e. Inertial/Dead Reckoning systems**, as an enabling technology for position determination. Dead Reckoning Technology is -to date- primarily used in motorised vehicles. In combination with GNSS (GPS) modules, built-in Dead reckoning technology will ensure 100% road coverage. Continuous coverage allows GNSS (GPS)-enabled applications such as Car navigation, Emergency vehicles services, Asset and Vehicle tracking products and Road-pricing systems, which require accurate, uninterrupted navigation.

Dead reckoning technology uses sensors that detect travelled distance and turn rate, supplementing GNSS (GPS) data and thus providing an accurate position in tunnels, indoor parking facilities, roofed logistics centres, urban canyons and any other environment where *obstructed GNSS (GPS) signals* hinder positioning. Depending on the quality of the GNSS (GPS) signal and on how well the Dead Reckoning sensors are calibrated, the technology uses a weighted mix of both data, generating optimal accuracy and coverage results. This algorithmic “back-up” approach also eliminates multi-path effects caused by high-rise buildings, position inaccuracies and distortions from jamming sources. In the next sub-section; we will elaborate on Vulnerability issues in more detail.

When considering sensitivity issues re. Location and Time functions for Position determination, it is fundamental to define a profile for the Location-based Services to be offered in project “Buiten Beter”. The overview depicted below is a helpful tool to do so. As indicated earlier, within the framework of project “Buiten Beter”, WP4 will primarily focus it’s attention on Fieldwork applications requiring **Wide-area multi-modal Radio-frequency based network infrastructure PNT systems**.



Tabel: A

Although both dedicated *Satellite-based network PNT systems*(GNSS and *Terrestrial-based network PNT systems*) use the same principles of determining one's position and the precise time, the technology applied and the performance that can be achieved differ considerably. Performance requirements are usually based on user needs and are in general defined by the *Required Navigation Performance (RNP) specifications*, which consist of four performance specifications, *accuracy, integrity, availability and continuity*. The definitions of these specifications are:

Accuracy

The degree of conformance of the determined position with the true position of a person or object at that time. This class of accuracy is called 'absolute accuracy'. Widely used is also the term 'repeatable accuracy' which specifies the conformance of the determined position with the determined position at the same location but established at an earlier time. Also often used is the term 'relative accuracy' which specifies the determined position relative to e.g. a runway or a harbour entrance.

Integrity

The ability of the system to provide timely warnings to users when the system should not be used for position determination.

Availability

The percentage of time that the services of the system are usable at the specified levels of accuracy, integrity and continuity.

Continuity

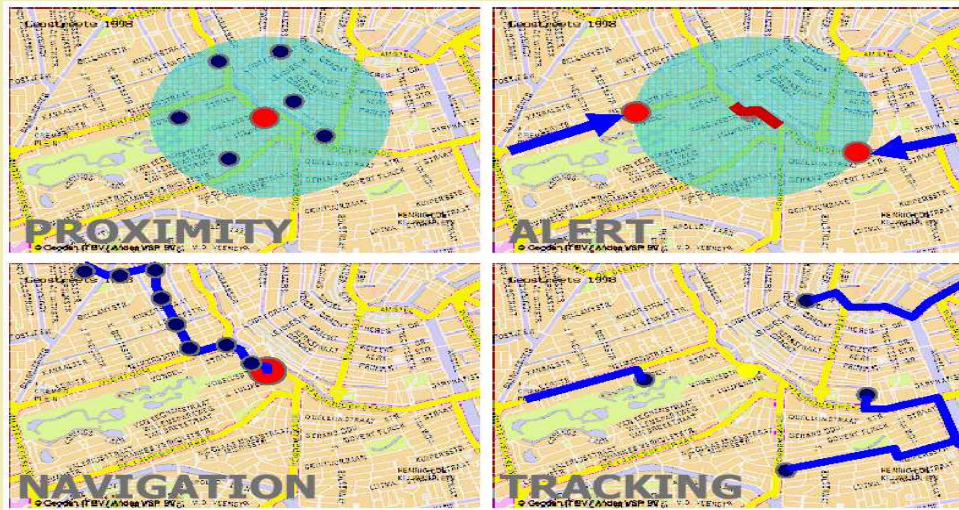
The ability of the system to perform its function without interruption during the intended operation, if it did so at the beginning of the operation.

The above definitions stem mainly from the aviation world and might therefore slightly differ from definitions originating from, for example, the land mobile world. However, the above given definitions are well understood by most users and will, therefore, be used throughout this report.

The reader might get confused by the terms *navigation* and *position determination*. *Navigation* is the entire process of planning a route, determining the current position and velocity/course of a person or object, generating commands or sending relevant information to the electronic PNT guidance system, and finally monitoring the navigation process as it develops with time. In daily life, the term *navigation* is often incorrectly

used when Position determination is actually meant. This is not a problem as long as the reader understands how to interpret these words.

Basic services - Outdoor



Tabel: B

Concluding this sub-section; for sake of convenience and comprehension we depict in table B above, the 4 basic PNT functions for Outdoor basic services usually required in applications:

b) Creating User awareness of potential “single-point of failure” PNT system risks

For many decades it has been good and common practise that safety-critical operations shall never rely on a single system. Systems can fail, and such a mishap shall not lead to a catastrophic so-called **Single-point of Failure** of the entire navigation process.

When GNSS (GPS) was reaching its operational status, many authorities and operators of safety-critical transports assumed that the above basic safety rule could be lifted, leading to potential significant cost savings. Fortunately, this attitude vanished before irreversible decisions in planning, building and operating radio navigation aids have been made.

In General: the Sole-Means GNSS (GPS) Question

Some ten years ago the general opinion, strongly stimulated by the United States, was that GNSS(GPS) would make all terrestrial systems superfluous and could therefore be decommissioned thereby saving large amounts of costs for operation and maintenance of the terrestrial infrastructure. This led to the intention to shut down various PNT networks & systems such as ILS, VOR/DME, radio beacons and many others. So, completely in line with this thinking, the US officially published in its 1996 Federal Radio-navigation Plan¹ that Loran-C in the United States would terminate operation of the Loran-C system by December 31, 2000. It was seen as an old and inaccurate system which should be considered as a once excellent but as a historical item today. Although, the military had already been aware of the vulnerability of the splendid GNSS (GPS) satellite system, these worries were not widely published, understood or anticipated, and therefore largely ignored.

A few years earlier, the President's Commission on Critical Infrastructure Protection was established in July 15, 1996. The Commission conducted a 15-month inquiry into a broad range of infrastructure vulnerabilities, including those of the information and communications infrastructure. Among the most significant projected

¹ 1996 Federal Radionavigation Plan, DOT-VNTC-RSPA-97-2/DOD-4650.5, page 3-14.

vulnerabilities found by the Commission, was the plan to adopt GNSS (GPS) as the *sole basis for Radionavigation* in the United States by 2010. In October 1997, the Commission recommended an assessment of the vulnerability of the transportation sector relying on the use of GNSS (GPS). The outcome of the study was made public in the so-called Volpe Report² on September 10, 2001, just one day before the dramatic attack on the Twin Towers in New York City and the Pentagon in Washington DC.

A blue rectangular slide with rounded corners. At the top center is a logo for the U.S. DOT/Volpe Center, featuring a circular emblem with a globe and the text 'U.S. DOT/Volpe Center'. Below the logo, the title 'Vulnerability Assessment' is written in a large, bold, 3D-style font. Underneath the title is a bulleted list of five points in white text.

- Threat of interference, unintentional and jamming
- Can be spoofed to give misleading information
- Risks can be reduced but not eliminated
- Tempting target for those hostile to the US
- Consequences severe for safety, economic damage

Tabel: C

Another major step was taken again by the United States during the ICAO meeting at Rio de Janeiro in December 2000, with the statement that GNSS (GPS) should not be longer seen as a sole-means navigation system for safety-critical operations. Slowly, the user community got aware that there could be an interference problem with GNSS (GPS). Many articles in the navigation literature and public presentations on conferences mentioned the easiness of jamming GNSS (GPS) with simple instruments freely available on the market. Circuit diagrams including companies and addresses where the required components can be achieved are found on the Internet which makes that many telecommunications students or experienced radio amateurs will be able to deny GNSS (GPS) to large groups of users while remaining nearly invisible themselves.

One can observe, that it is the United States who leads the rethinking on the vulnerability of GNSS (GPS) and all processes depending on the correct functioning of the satellite system. Nowadays, many groups are expressing their deep concerns about decommissioning terrestrial radio navigation systems by mostly governmental bodies in order to save money. This is most prominently seen with the discussions about continuation of Loran-C. In March 2004, the US' FAA published the report 'Loran's Capability to Mitigate the Impact of a GNSS (GPS) Outage on GPS Position, Navigation, and Time Applications'³. The main research tasks focused on the question were whether Loran-C could cost-effectively meet recently defined HEA (Harbour Entrance and Approach), NPA (Non-Precision Approach) and Time/Frequency requirements. According to the Report, all these requirements can be met.

² Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System, Final Report, August 29, 2001. John A. Volpe Transportation Systems Center, Office of the Assistant for Transportation Policy U.S. Department of Transportation.

³ 'Loran's Capability to Mitigate the Impact of a GPS Outage on GPS Position, navigation, and Time Applications', Prepared for the Federal Aviation Administration, Vice President for Technical Operations, Navigation Services Directorate, submitted by Mr. Mitchell J. Narins, Program Manager, March 2004.

The situation in Europe is very different. Comments on GNSS (GPS) vulnerability can be heard saying that the problem will be solved or at least be diminished as soon as the new European GNSS Galileo system will reach its operational condition. This attitude can be partly understood by realising that after European governments decided to continue the costly development of Galileo; that it is considered far from helpful, if at the same time public doubts concerning potential vulnerabilities are fuelled and therefore should not be encouraged. In contrast to these governmental positions, rather different opinions can be extracted from the Helios-Technology study on request of the EC-Dg-TREN^{4, 5}. On page 19 of reference 4, the report states that 137 GNSS (GPS) applications have been analysed. Fewer than 40 would remain operational following the loss of GNSS (GPS) and its augmentation systems. On page 100 it is said that "Loran-C services are capable and ideally suited to mitigate: system, service and user vulnerabilities that are currently dependent on GNSS (GPS) and its augmentations".

... fewer than 40 of the 137 applications analysed would remain operational following the loss of GPS and its augmentations ...

HELIOS
TECHNOLOGY

Recommendations towards the development of a European Union Radio-Navigation Plan (ERNP)

http://europa.eu.int/comm/dgs/energy_transport/galileo/documents/doc/2004_12_22_ernp_study_en.pdf

© David Last

Tabel: D

On page 14 of reference 5, the report says "*Loran-C is the only real stand-alone alternative to satellite radio-navigation services for many market sectors*". The latter, is in particular applicable to **safety & security critical operations**.

A number of professional user groups, institutions and academic papers made public statements to express their worries on the increasing dependence on satellite navigation. **See Appendix A.**

The following section pays attention to the *technical description* of *Vulnerability aspects to Wide-area multi-modal Radio-frequency based network infrastructure PNT system providers and user's receivers*

GPS, Galileo, Loran-C and Telecommunication Cell-ID; Wide area Radio-frequency based PNT network infrastructures & systems, broadcast radio(RF) signals that are received and processed in user equipment to determine the position of the receiver antenna. The well functioning of the receiver depends on the correctness of the broadcast as well as the capability of the receiver to receive and process the navigation signals. Disruption of this process may be caused by physical damage to the transmitter or to the receiver. Satellites are operating in a rather safe environment. Only high-tech and commercially powerful countries will ever be capable to physically disable a satellite. Another approach could be to attack the ground control cen-

⁴ 'System Qualification, Development of the European Radio-Navigation Plan', Deliverable D2, Produced for the European Commission, Directorate General for Energy and Transport, Directorate for Inland Transport, contract ETU-B57000A-E4-193-2003 S07.26312-ERNP, Document reference P377D005-0.98, 1st July September 2004.

⁵ 'System Implementation, Development of the European Radio-Navigation Plan', Deliverable D3. See also ref. 4 above.

tres of either the satellite and/or terrestrial system as these centres are crucial for the correct functioning of the entire system. Although these stations are often located in relatively safe underground facilities in often mountainous terrain and, in addition, are generally heavily protected by military forces, the new satellite generation GPS-III is taking even this minor risk into account by linking the satellites to a space-based inter-satellite communication network. This makes autonomous operation of the satellites possible for an extended period of time without support from any ground station.

Terrestrial based Loran-C and Telecommunication Cell-ID base stations are more vulnerable to physical damage. The 200 meters tall Loran-C towers and/or Cell-ID Base station antennas can be relatively easily destroyed. Repairing such damages may take considerable time causing the stations being of air for quite some time. From the provider side, making a terrestrial RF networked PNT system fully non-operational, more than a single station has to be destroyed. These systems have more stations on air than are strictly needed. However, if a station will go off-air, the performance of the system will most likely decrease.

A more 'elegant' way of 'destroying' the navigation functionality is by broadcasting other signals either to jam, to spoof or to meacon the real navigation signals. What do those interference terms exactly mean?

Jamming is broadcasting signals in the same frequency band and which are relatively strong compared to the real navigation signals. Jamming satellite wide area RF signals can easily block the receiver by overloading the linear part of the GNSS (GPS) receiver or by disrupting the proper functioning of the GNSS (GPS) or Loran-C signal processing circuits which normally extracts the navigation signals to e.g. measure the time of arrival. Such jamming signals can be non-intentionally or intentionally being broadcast. Unintentional GNSS (GPS) jammers could be spurious harmonics from TV stations, communication links, onboard electronic equipment, and many others. The same type of jammers with Loran-C can be electric circuits in cars, luminescent lighting, and overhead power lines.

Intentional jammers are far more dangerous as these signals are made with the intention to disrupt the system. In that case the signal frequency and modulation types are optimised to achieve the most annoying effect with the lowest possible radiated power to avoid tracking down the jammer.

Unfortunately, it is quite simple to design and build jammers for GNSS (GPS) which can be effective over large areas. Jammers that can disrupt Loran-C over large-area are much more difficult to construct.

Spoofing signals are different as these signals are look-alikes of the real navigation signals. If done in a smart way, the receiver will not notice that false signals are processed leading to wrong position determination. It is obvious that in case of GNSS (GPS) such techniques might be quite 'popular' in criminal and military environments. Fortunately, designing such equipment requires good knowledge of the system to spoof, and building such nasty instruments is not very simple. However, smart telecommunications students could do it, especially as they can acquire standard GNSS (GPS) test signal generators from the open market. An upcoming threat is GNSS (GPS).

Meaconing which means that received GNSS (GPS) signals are amplified, and via a cable of a certain length re-broadcasted by another antenna. If these signals are slightly stronger than the original GNSS (GPS) signals, then the receiver will track those faulty signals and will then 'find' the position of the meaconing receiving antenna instead of the user's antenna. If such signals are applied by DGPS reference stations, the high accuracy service essential for example to surveyors and pilots of large tankers, will become completely useless.

For the purpose of project "Buiten Beter" I choose to limit the issue to GNSS (GPS) jammers. An important question is to determine whether there really is a risk that people would like to jam GNSS (GPS) as this phenomenon was hardly ever heard before the GNSS (GPS) era. The reason could be that society never before relied so strongly on a single source of navigation and time. So, never before the 'bad guys' could disable our navigation and time source so easily and untraceably, and over such large areas. The last and third reason is that society in general does not recognise this interference vulnerability flaw of GNSS (GPS) and therefore doesn't take timely precautions.

Because GNSS (GPS) performs mostly so excellent and is so cost-effective, users are not very keen to admit that their operations might rely on a vulnerable system. Although most of us assume personally that our property or health will never be at risk because of fire, contagious diseases, burglary or floodings, our society is readily willing to invest in fire fighting, vaccination, police and dikes. This willingness is based on former bad experiences and on the wish that such will not occur once more. This mental acceptance step has, unfortunately, not become visible as yet in respect of GNSS (GPS) dependent processes. Although the author does not propose to set up a GNSS (GPS) -failure based accident or any other mishap at all, it is most likely

that such an accident might help to make society aware of the potential risks all of us should face. A few likely groups of potential risks can be identified with a certain probability that it may happen once.

The first group is based on hackers, the same type of people who design and distribute software viruses. The likely chill for these guys is, that they can cause large and costly problems in private or industry computer systems. An identical chill could be achieved by disrupting navigation and timing services essential for the proper functioning of many transportation and telecommunication infrastructures. A second group could emerge in the road-tolling area. Users are going to pay significant amounts of money to be allowed to enter large cities or to use highways. So, fraud through misleading or denying GNSS (GPS) may become a potential issue. Another group(3) to consider are thieves who are hindered in their business by all kinds of GNSS (GPS)-based systems to protect expensive automobiles or high-value cargo. If thieves can simply disable GNSS (GPS) receivers, their success score may increase. The fourth and likely also the most dangerous group is formed by terrorists and criminals.

Consequences of GNSS (GPtS) Loss / Degradation

Depending on ...

- Application Mode Involved
- Duration of GPtS Loss/Degradation

Impact Can Be

- Minimal - Quick Recovery
- Operational - Reduced Effectiveness & Efficiency
- Safety - Potential Loss of Life, Environmental, Economic Damage

Timing & Synchronization

- GPtS Outage can disrupt Communications/Networks



Tabel: E

There are numerous potential targets. Some examples to be mentioned are protection of VIPs, tracking criminals, navigation of large crude oil tankers through the rather narrow sea lanes on the North Sea, and the distribution of precise time to keep TDMA telecommunication networks running. The latter, target only applies; based on the assumption that GNSS (GPS) clocks ARE used as a sole means for precise time keeping in these telecommunication networks used for instance for financial money payment transfer systems.

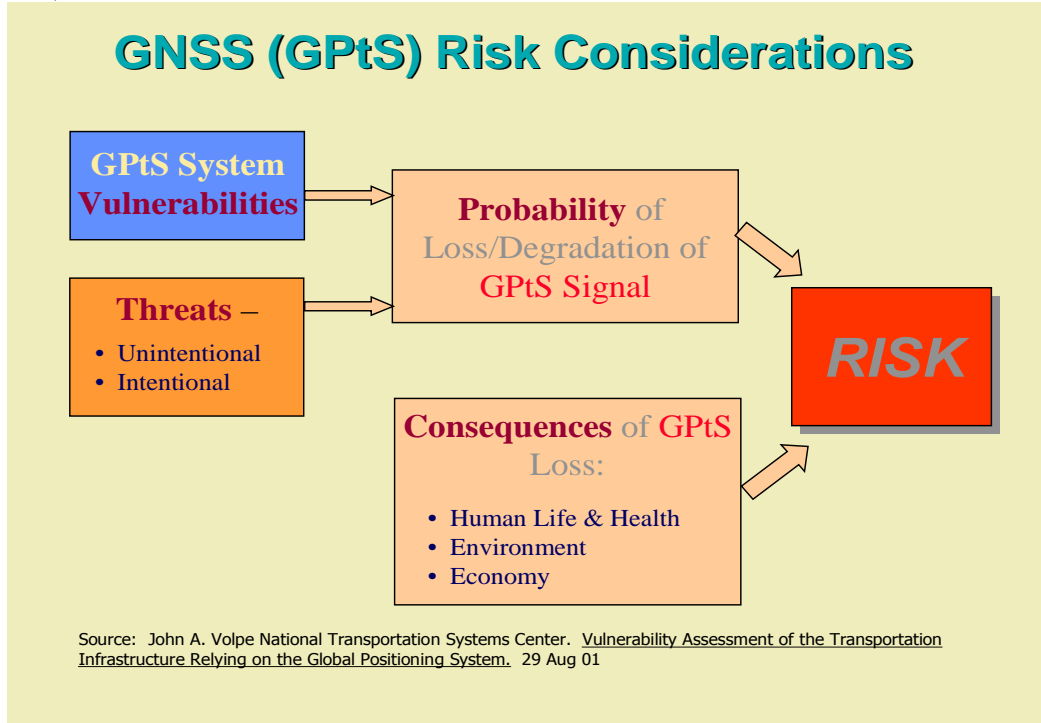
In conclusion, *there is no simple, cost-effective way to get around GNSS (GPS) jammers available yet. The only escape is either to use another dissimilar i.e Non-Satellite based Radio-navigation system or applying autonomous Inertial techniques to counteract temporary outages of GNSS (GPS) due to jamming/spoofing.*

On 22nd of October 2004 Dutch national TV News program: “**Twee Vandaag**”, broadcasted a very explicit and eye-opening video titled: “**GPS signaal extreem kwetsbaar**” – See:

http://www.tweevandaag.com/call.php?module=PX_Video&func=view&vid=18457&startvideo=1 this, with the sole objective to draw attention and create public awareness to the issue of **Single-point of Failure** risks of GNSS (GPS) based Positioning, Navigation & Timing (PNT) network infrastructures and related applications.

C) Reducing Vulnerabilities & Risk Considerations re. PNT system robustness

This section pays attention to a number of techniques to mitigate the disturbing effects of interference on the performance of the total Positioning, Navigation & Timing (PNT) determination system. This can be achieved in Four (4) basically different ways. The first(1) approach is to use more advanced receivers that can withstand large amounts of interference. The next possibility(2) is to integrate the two very different(dissimilar) but **dedicated** Wide-area multi-modal Radio Positioning network systems i.e. one Satellite-based network PNT system(GNSS) alike the United States GPS and the Russian GLONASS, with a second Terrestrial-based network PNT system such as Loran-C, the Russian equivalent Chayka, which will offer an improvement in all cases where both systems are not denied at the same time and at the same location. A third(3) possibility is to integrate a dedicated Satellite-based network PNT system(GNSS) with a **non PNT dedicated** terrestrial Wide-area multi-modal Radio Positioning network system, such as a mobile Telecommunication Cell-ID network i.e. GSM/GPRS/UMTS/HSDPA etc. The latter possibility only makes sense, on the strict condition that GNSS (GPS) clocks are NOT used as a sole means for precise time keeping in these telecommunication networks, for instance to support financial money payment systems. The fourth (4) and last possibility is to apply autonomous micro-electromechanical (MEMS) PNT systems i.e. Inertial/Dead Reckoning systems i.e. Inertial (INS) systems that are completely immune to radio interference. As the error of inertial systems grows with time, calibration techniques must be available. This can be achieved by comparing the driven trajectories with digital maps (Map matching) or by intermittently using GPS, Loran-C or Cell-ID to calibrate the inertial sensors.



Tabel: F

Inertial navigation systems in cars use primarily a rotation rate sensor measuring the turn rate, and wheel sensors to acquire the distance travelled. For pedestrian applications the same principles apply, based on step technology.

Combining both gives a trajectory driven/walked which may show errors in the distance or errors in curvature. Both can relatively easy be corrected by GNSS (GPS). This calibration, however, is losing its validity rather quick. The better the inertial sensors, the longer will be the time that re-calibration is needed. As usual, this is also a matter of costs. The advantage of inertial-aided navigation is that it is very robust in all areas where GNSS (GPS), terrestrial Loran-C or Cell-ID RF signals are not well receivable.

The following reference table shows a summary and gives - *not more than an indication* - of vulnerability related issues of GPS, Loran-C and Inertial (INS) and Cell-ID, PNT networks

	GPS	Loran-C	Inertial	Cell-ID*
Accuracy	++	+	- +	-+
Vulnerability to local jammers	++	+	n/a	+
Vulnerability to high-power large-area jammer	+	--	n/a	-+
Easiness to jam locally	++	+	n/a	+
Easiness to jam large area	+	--	n/a	-+
Mitigating local jammer	--	- +	n/a	-+
Mitigating single-source high-power jammer	- +	++	n/a	-+
Detection capability of low-power local jammer	--	- +	n/a	-+
Detection capability of high-power wide-area jammer	+	++	n/a	++
Detection capability of multiple low-power jammers	--	- +	n/a	-+

*Note: General overview various versions Cell-ID telecom networks and on the *strict condition* that GNSS (GPS) clocks are NOT used as a sole means for precise time keeping in these telecommunication networks

Above vulnerability overview table can be briefly elaborated as follows:

Integration of ‘Dedicated’ but dissimilar PNT systems such as GNSS (GPS) and Loran-C

Integration makes sense if there are dissimilarities in frequency, power levels and signal structure which may lead to decorrelation of failure mechanisms. For example, if a GNSS (GPS) RF signal is blocked by buildings and a Loran RF signal not, then integration leads to a larger availability of the navigation functionality. In the case of this project the focus is on jamming. Therefore, it must be analysed whether there are GNSS (GPS) jamming conditions where Loran is not supposed to be jammed or vice versa. The table in section 3 indicates that when large area GNSS (GPS) jamming might occur, Loran is likely still functional and navigation can continue albeit with less accuracy. In case of intentional jamming nearby (within 5 metres) receivers then (GNSS) GPS as well as Loran will cease operation.

Integration of ‘Non-dedicated’ but dissimilar PNT systems such as GNSS (GPS) and Cell-ID

Also here, integration makes sense if there are dissimilarities in frequency, power levels and signal structure which may lead to decorrelation of failure mechanisms. However, one has to understand that Cell-ID network infrastructures where position determination is based on triangulation calculations between individual GSM/GPRS /UMTS/HSDPA Cell base stations, each especially fitted out with appropriate Location intelligent software algorithms; are -at least by the professional PNT community- *not considered to be ‘dedicated’ PNT Radio Positioning network systems*. In principle, mobile terrestrial Telecommunication Cell-ID network infrastructures such as GSM/GPRS/UMTS/HSDPA etc. are *primarily designed and built* to offer mobile RF based transmission bandwidths and speed to facilitate transport and distribution of speech, data and video

content, and NOT optimized for Positioning, Navigation & Timing (PNT) functions! The fact, that terrestrial mobile Cell-ID Telecommunication network infrastructures can however assist and facilitate PNT functions by means of triangulation calculation algorithms is acceptable, BUT only on the strict condition that in the telecommunication network uses atomic or other clocks and NOT GNSS (GPS) clocks for precise time keeping in these telecommunication networks.

Integration of radio systems with inertial (INS)

Inertial systems bring navigation outside the radio world (i.e. do not use RF signals) which could make the system very hard to disturb. Unfortunately, low-cost INS shows rather poor performance when it is not frequently calibrated; at least once per couple of minutes. In situations where (GNSS) GPS is not continuously jammed, this might be a valuable option. Integration of GNSS (GPS) and INS can also make receivers more jam proof as the tracking bandwidth can significantly be reduced thereby limiting the probability that the jamming signal kills one or more of the frequency components of the complex GNSS (GPS) radio signal spectrum. This type of integration, so called tightly coupled integration, increases the complexity of the receiver which raises the costs. This type of integration can also be done with Loran-C albeit with less accuracy than with GNSS (GPS).

Integration of GPS, INS and map matching

Many built-in car navigation systems use GNSS (GPS), inertial sensors and map matching to determine accurately the car's position. This technique is well known and produced in millions. Although the performance is impressive, the system will only correctly operate as long as the user is on one of the roads stored on the digital map. Otherwise map matching cannot be achieved. There is also an advantage to this limitation, the dispatcher is able to monitor when one of the fleet cars is leaving the regular road. Although this integration can also be done with Loran-C, the final performance will not be as good as with GNSS (GPS). As GNSS (GPS) is quite accurate, many new PDA & Smartphone based systems are on the market today. Basically, these units are based on GPS and map matching only and therefore in case of civil Non Safety & Security critical applications , do not require the need for any output from supporting inertial sensors.

Laws

A formal approach to mitigate intentional jamming is by law. An interesting example of such a law is seen in Australia⁶. Some parts of this law are shown below:

Quote:

Devices that can be used to jam global positioning systems GNSS (GPS) have been prohibited under section 190 of the Australian Radio-communications Act 1992.

*From today, a person who supplies, or possesses a jamming device for the purpose of supply, can be prosecuted under the Act. Penalties range from fines of up to **\$165, 000**, to **imprisonment**. It is already an offence to operate or possess such devices.*

The ban on the devices, also known as Radio-navigation-Satellite Service (RNSS) jammers, was announced by the Australian Communications Authority (ACA) today.

RNSS is a system of satellites, with supporting infrastructure, which provides accurate positioning, velocity and timing data. GNSS (GPS) is the most well known of these systems.

*"While interference caused by RNSS jamming devices is not a concern at the moment, the relative ease with which a jammer could be built, and the **potential for significant disruption to a wide range of services**, warrants these devices being prohibited," ACA Acting Chairman Dr Bob Horton said today.*

*Dr Horton said that using an RNSS jamming device could not only inconvenience RNSS users but also presented a **real threat to public safety**.*

Unquote

Comment: It is questionable whether criminals or GNSS (GPS) hackers will be impressed by this law.

⁶ See www.agcc.gov.au

Conclusion

Civilian systems rely heavily on GPtS

- Potential applications of GPtS are vast and *nowhere near maturity*
- *Potential serious economic and potentially fatal consequences* if signals are disrupted

GPtS is a tempting target for adversaries

- *Continues to penetrate* civil infrastructure
- GPtS Users are *Vulnerable to Signal Loss or Degradation risks*
- The Vulnerability will *Not be fully Eliminated*
- *Awareness & Planning* can mitigate the Worst Vulnerabilities

Tabel: G

Intentional jamming GNSS (GPS) is a serious matter as it can easily be practised and the effects may be enormous. GNSS (GPS's) role in a large part of the technical infrastructure of our country is growing every day while *useful backup systems are hardly available*. The negative effect of loss of position or time data depends on the application. It is a disappointing fact that many professional organisations apparently do not yet fully realise the potential risks they face in case GPS would become suddenly unavailable over the entire, or parts of the country.

Selecting an alternative solution for GNSS (GPS) to mitigate its potential loss depends on the application. Whether this will be Loran-C, Inertial navigation or Cell-ID is not simply answered. Careful analysis of the risk of each PNT Sole-means GNSS (GPS) dependent operation is required to be able to come up with a useful alternative. As the diversity of applications is so incredibly large, **a general solution can, unfortunately, not be given.** However, a large step forward would be achieved when the experts in all these GNSS (GPS)-dependent fields would realise that the beauty of GNSS (GPS), and of the future Galileo, has also some very risky aspects. Therefore, the message to Civil GNSS (GPS) user communities is:

GNSS (GPS) provides many benefits to civilian users. However, it is vulnerable to interference and other disruptions that can have harmful consequences. GNSS (GPS) Users must ensure that adequate independent and dissimilar backup systems or procedures can be used when needed. The latter is very important, when considering applications for safety & security environments.

SOURCES:

Interagency GPS Executive Board. [GPS policy, applications, modernization, international cooperation](#). Febr. 2001
European Commission DG TREN: [Recommendations Towards the Development of a European Union Radionavigation Plan \(ERNP\)](#) – December 2004

Recommendations:

Recommendations to “Buiten Beter” project participants when considering definitions & technical implementation of PNT functions:

Study Vulnerabilities to Determine Tolerable Levels of Risk and Cost for Critical Infrastructure Applications

- Determine *Costs of Lowering Risks* to an Acceptable Level
- Implement Appropriate *Mitigation Strategies*
- *Jamming & Spoofing* testbed demo is an opportunity to get started

For Each Application, Choose or Maintain Appropriate Backup System or Procedure

- Reflect Interference Impact in *Application Designs*
- Implement Systems to *Monitor/Report/Locate Interference*
- Assess Applicability of *Military Anti-Jam Technology*
- Be conscious of *Timing Applications*
- Re. *augmentations* to space-based PNT systems; the term "*interoperability*" needs rigorous interpretation as "interchangeability"

Encourage User Training and Use of Backup Systems

Beantwoording Onderzoeksvraagstellingen: "Buiten Beter" aspecten Positiebepaling, Navigatie & Tijdsynchronisatie (PNT) functies in het veld mbt. Kwetsbaarheid/Integriteit van GNSS-GPS Radio Frequentie signalen

Vraag: Welke verbeteringen zijn gewenst met betrekking tot mobiele PNT functies (In-Car en/of Personal) ter ondersteuning van GEO-ICT applicaties bij inspectie en handhaving?

Antwoord: Een duidelijke verbetering die voor alle "*Kleur sporen*" geldt en gewenst zou zijn, is dat de milieu-opsporingsambtenaren dynamische route-informatie aanwijzingen ontvangen, hoe het beste naar een opgegeven Veld lokaties cq. plaats van delicten te komen. M.a.w. lokaties die niet in standaard topografische digitale kaarten (TeleAtlas/Navteq) zijn weergegeven op basis van Straatnaam/huis.nr. en/of Postcode zijn te vinden. Op de in PDA beschikbare kaarten zien de milieu-opsporingsambtenaren wel de opgeslagen lokatie, maar is de weg naar de lokatie toe niet altijd even duidelijk. Eea. is natuurlijk afhankelijk van de "*Kleur spoor*" en de aard van het delict meer of minder relevant. In het kader van betrouwbaarheid van de verstrekte informatie is verder gebleken, dat lang niet altijd vast staat hoe een bepaalde lokatie door een milieu-opsporingsambtenaar digitaal is ingevoerd? Dit laatste geldt vooral indien geen GPS signaal beschikbaar is. Ook hierin is verbetering mogelijk. M.a.w. ter ondersteuning van Positie, Navigatie & Tijdsynchronisatie (PNT) functies is het wenselijk, dat er beter ondersteunend kaartmateriaal en slimmere algoritmes worden gebruikt; waarbij de mogelijkheid bestaat een overzicht te krijgen van geïntegreerde routes variërend van wandel/bospaden, landbouw-en openbare wegen, stedelijke voetgangerspaden, industriewijken enz.

Vraag: Hoe operationeel kritisch zijn PNT functies bij GEO-ICT applicaties bij inspectie en handhaving?

Antwoord: In het algemeen gesteld, is gebleken dat voor het project "Buiten Beter" met referentie aan Tabel A op blz. 7 uit sub-Hoofdstuk 5.1, in de plaats- en tijdsgevoeligheds beschreven matrix "Location Based Services Profiles" applicaties / functies mbt. *preventieve* opsporing en handhaving; dat de diverse "*Kleur sporen*" eerder Plaatsgevoelig dan Tijdsgevoelig zijn en dus moeten deze worden gepositioneerd in de buurt van de "Who's nearest" (groene) en "Search & Locate" (transparante) ballonetjes in deze matrix grafiek. In uitzonderlijke gevallen zijn Operationeel kritisch - qua reactietijd en plaats-, alleen ernstige "real-time" milieurampen bij alle "*Kleur sporen*", waarbij sprake is van een grootschalige lucht, water en/of grond verontreiniging. Bij deze laatste Noodsituaties, mogen de BOA's (Bijzondere Opsporings Ambtenaren) alleen ondersteunend optreden en ligt de eindverantwoordelijkheid en bevelvoering in eerste instantie bij de Brandweer commandant van desbetreffende regio(s). Er is dan sprake van de inwerkingtreding van het Milieu Incidenten Plan (MIP), m.a.w. BOA's handelen delicten af, die qua tijdsgevoeligheid enig uitstel kunnen dulden.

Vraag: Gelet op het "Single Point of Failure" risico, dienen PNT GEO-ICT systemen enkel- of dubbelvoudig te worden uitgevoerd? En dient hierbij een onderscheid gemaakt te worden tussen In-Car en Personal PNT gebruikers?

Antwoord: Op dit ogenblik, vertrouwen de gebruikers in het project "Buiten Beter" mbt. verkrijging van Positie, Navigatie & Tijdsynchronisatie (PNT) functie informatie, enkelvoudig op het wereldwijd dekken-de Radio Frequentie Satelliet netwerk GNSS-GPS en die bij gebruik -in het veld- over het algemeen

gesproken, voldoende betrouwbaar en accuraat werkt. Ter voorkoming van het zg. “*Single Point of Failure*” risico’s; met name van belang bij slechte tot matige ontvangst van GNSS –GPS RF signalen in stedelijke gebieden(indoor), meteorologisch ongunstige invloeden, dicht beboste omgevingen enz.; is op termijn de wens aanwezig om op een GNSS Back-up systeem/netwerk terug te kunnen vallen (*dubbelvoudig*); echter op dit moment gaat de voorkeur uit naar een telecom Cell-ID back-up netwerk met GPS = zg. Assisted GPS (A-GPS) keuze, die middels een 3- hoeksmeting rekenmethodiek van kruispeilingen tussen de zend/ontvangst masten in de cellulaire keten van basisstations in het netwerk, de plaatsbepaling van gebruikersterminals (o.a. PDA’s) kan berekenen. Afhankelijk van het gekozen telecom netwerk (GSM, GPRS, UMTS, HSDPA) zal verstrekking en accuratesse van locatie-informatie verschillen. Eea. heeft te maken met de dichtheid van zend/ontvangst masten van het gekozen telecom netwerk operators alsmede de toegepaste software algorithmen van 3- hoeksmeting rekenmethodieken in de telcomnetwerk basisstations. Een extra punt van aandacht is hierbij wel; dat door de gebruikers in het project “Buiten Beter” bij de keuze van telecom netwerkoperator navraag moet worden gedaan; *welke tijds klok ivm. tijdsynchronisatie van verstuurd digitale gegevens* in het telecom netwerk wordt gebruikt?? M.a.w. als blijkt dat dit een klok is die gesynchroniseerd wordt door gebruik te maken van de RF signalen van bijv. GNSS-GPS; dat zou men tot de ontdekking kunnen komen dat ivm. Kwetsbaarheids/Integriteits aspecten; dat de gekozen Back-up PNT netwerk NIET robuust dus betrouwbaar genoeg is om bepaalde afgesproken Service Level Agreement(SLA) criteria te halen ???

Hier kunnen zich immers dan dezelfde problemen voordoen, als eerder is beschreven in sub-paragraaf B(blz. 8 en verder) van dit rapport.

Mbt. de vraag of onderscheid gemaakt moet worden tussen In-Car en Personal PNT gebruikers binnen het project “Buiten Beter”, is het *Antwoord*: nauwelijks, want gebleken is dat milieu-opsporingsambtenaren bijna-zonder uitzondering- een personal Handheld Computer(PDA) gebruiken en deze zowel buiten of in de auto kunnen gebruiken; waarbij wel gelet moet worden op evt. slechtere ontvangst van GNSS-GPS RF signalen als gevolg zg. “Kooi van Faraday” effecten. Eea. is makkelijk te verhelpen mbv. externe Bluetooth GNSS-GPS antennes die vervolgens in verbinding staan met PDA’s en/of Smartphones, die eveneens voorzien zijn van een Bluetooth “near field communication” module. Overheersend, is het persoonlijk gebruik; buiten de auto in het veld.

Vraag: Wat is qua robuustheid & integriteit, de meest optimale keuze-mix van RF-PNT netwerk en/of autonome systeem ten behoeve van gebruikers in het project “Buiten Beter”?
Conformiteitscheck zinvol/noodzakelijk ? mbt het European Radio Navigation Plan (ERNP) Beleids & strategie document in Europa.

Antwoord: Gelet op de hierboven beschreven uitgangspunten en werkmethodeken van het Project “Buiten Beter” bij preventie & handhaving: activiteiten niet tijd- maar juist meer plaats kritisch zijn, alsmede ook het gegeven van een persoonlijk gebruik van PDA’s buiten de auto in het veld; lijkt vooralsnog, de meest optimale keuze-mix *tbv. applicaties en functies voor Positie, Navigatie & Tijdsynchronisatie(PNT)*, gebruik te blijven maken van het GNSS-GPS satelliet netwerk met waar nodig ivm. evt. Robuustheid/ Integriteit wensen van de gebruikers, een PNT Back-up voorziening van een gecombineerd en geïntegreerd WIFI (stedelijk) met UMTS(wide-area) A-GPS Cell-ID telecom netwerk. Mbt. de toekomst (ca. 2013) zou wel eens het navolgende scenario kunnen gelden: 1st lijns PNT netwerk systeem gebaseerd op GNSS-Galileo met 2^e lijns maar nu vooral ook bij TIJD- en PLAATS kritische toepassingen een Back-up scenario met e-Loran RF netwerk of met autonoom Inertial/ Dead Reckoning (gegist bestek) technieken, gebruik makend van micro-electromechanical (MEMS) PNT systemen.

Een Conformiteitscheck mbt het European Radio Navigation Plan (ERNP) Beleids & strategie document in Europa, lijkt op dit ogenblik niet echt zinvol/noodzakelijk omdat deze weliswaar belangrijke Europese PNT richtlijn – in wording- voor een deel gedateerd (CE-Dg-TREN, dec. 2004) en dus achterhaald is. Medio 2008 zal in het kader van het EC-7th Framework R&D Programme in het kielzog van de EC-GNSS-Galileo Applications Green Paper; een nieuw ERNP Recommendations en Policy document verschijnen.

Tot slot van dit Hoofdstuk 5 zie **Appendix B**: voor Nuttige Internet Website adressen mbt. publicaties en Referentielijst van rapporten over *Plaatsbepaling, Navigatie en Tijdsynchronisatie(PNT)*.

6 **ORGANISATIE MODEL: BEVORDEREN VAN GEO-ICT GEBASEERDE "ONE-STOP SOLUTION" PNT, LOCATION INTELLIGENT BUSINESS SERVICES SUPPLY-CHAIN PARTNERSHIP SAMENWERKINGSVERBANDEN**

Uitdieping onderzoeksvraag:

Zijn gebruikers in het project "Buiten Beter" gediend bij het aanbod van een organisatorisch Geo-ICT gebaseerde "One-Stop Solution" PNT Location Intelligent Business Services Supply-chain Partnership samenwerkings- en informatie model?

Om deze vraag te kunnen beantwoorden hanteren wij als uitgangspunt de **ZV's** van *Visie t/m Verspreiden* bij ICT Beheer & Procesdenken van Prof. Dr. Ir. Nico Baken – deeltijd Hoogleraar Bedrijfscommunicatie aan de Faculteit Informatie Technologie & Systemen aan de Technische Universiteit te Delft(TU Delft). Deze zijn:

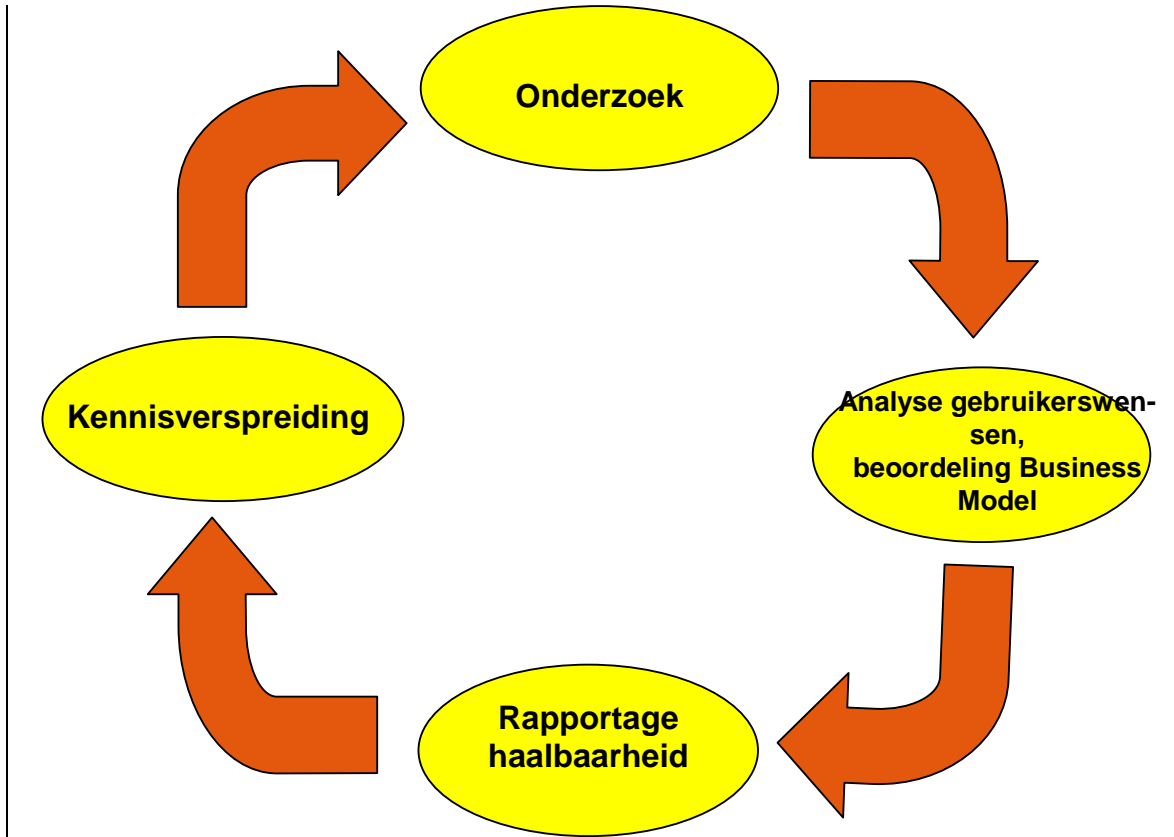
- **Visie:** alles valt of staat met een visie
- **Verstaan:** een missie met meerdere partijen; die moeten elkaar wel goed verstaan
- **Vertrouwen:** een gemeenschappelijk doel ontdekken, empathie voor elkaars rollen ontwikkelen en ontdekken wat reële waardeketens zijn
- **Vergelijken:** benchmarken met andere branches of over de landsgrenzen heen toetsen
- **Verwezenlijken:** kleinschalig beginnen met een "Transitie-arena", een pilot-project met meerdere partijen tegelijk
- **Verifiëren:** zit men wel op dit idee te wachten? Klanteisen verifiëren
- **Verspreiden:** de fase van kennis disseminatie. Gebruik de voorsprong en doe aan kennisdeling om snel draagvlak te creëren

Zoals is aangegeven; draait het bij Geo-ICT beheer vooral om het **Procesdenken**. Hierbij zijn 4 hoofd aandachtsgebieden te onderkennen, die een onderlinge afhankelijkheid hebben, namelijk:

- organisatie en besturing van de Geo-ICT beheerorganisatie;
- processen in de Geo-ICT-beheerorganisatie;
- producten en diensten die de Geo-ICT-beheerorganisatie voortbrengt ;
- expertise en middelen die de Geo-ICT-beheerorganisatie nodig heeft.

Tussen voornoemde aandachtsgebieden bestaat een onlosmakelijke wisselwerking. Processen worden niet gestructureerd als doel op zich, maar om op efficiënte en contoleerbare wijze concrete producten te leveren en resultaten te bereiken!

Eea. kan schematisch als volgt worden weergegeven:



Tabel: H

Stelling:

Geo-ICT toepassingen schuiven steeds meer op van systeemgecentreerde naar netwerkgecentreerde oplossingen. Het gaat allang niet meer om alleen Internet toegang. Er zijn al tal van functies die nu al in het netwerk worden belegd, zoals storage, betalen en security. We gaan naar een wereld waarin netwerken een steeds centralere rol gaan spelen. Deze “vernetwerking” van onze wereld ontwikkelt zich in 3 fasen:

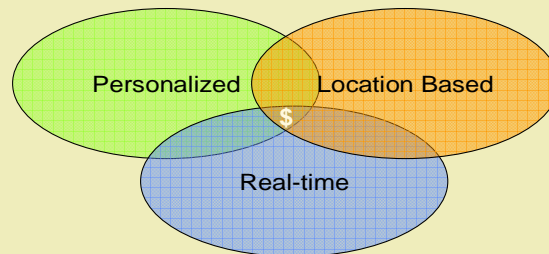
- *Convergentie* van data, spraak en video; we zitten nu middenin deze fase
- *Virtualisatie* van netwerken, storage- oplossingen, servers en beveiligingsdiensten; deze fase is inmiddels aangebroken
- *Application oriented networking(AON)* – ofwel het intelligente netwerk m.a.w. een nieuwe technologie om de communicatie tussen bedrijfsapplicaties te verbeteren door intelligentie(lees: slimme software) in het netwerk toe te voegen; deze fase is grotendeels nog toekomstmuziek.

Het INTERNET blijft in alle fasen de verbindende schakel (infrastructuur); niet alleen tussen gebruikers thuis, op kantoor, vanuit en naar de auto toe maar ook in het project “Buiten Beter” bij **toezichthouders en opsporingsambtenaren in het veld!**

Geo-Informatie uitwisseling tussen gebruikers ter ondersteuning van functies voor Positiebepaling, Navigatie & Tijdsynchronisatie (PNT) zal in toenemende mate gebruik gaan maken van decentrale vaste alsook mobiele Internet “network centric Server-based” Geo-ICT proces architecturen en netwerken om applicaties en content op een zo persoonlijk mogelijke wijze – in real-time - met elkaar te kunnen communiceren. De keuze van ICT netwerkinfrastructuren en systeem technologieën is belangrijk, maar zal ondergeschikt (faciliterend) dienen te zijn en blijven aan gebruikers applicaties en informatie –inhoud(content). Zie onderstaande afbeelding.

Vision: The Information Society

The Mobile Information Society will be driven by *Personalized* **Mobile Location & Timing** **conscious** *Network-centric* based **Applications & Content**, not technology.



Tabel: I

Business Development en Marktpositionering issues:

Uitgaande van de bereidheid van de projectpartners in "Buiten Beter" om bestaande en toekomstige klanten middels het "*Ketenprocesdenken*" gekoppeld aan "One Stop Solution" oplossingen met een "Single point of Contact" mogelijkheid te gaan bewerken cq. te werven, alsmede de wil om hechte (exclusieve) samenwerkingsverbanden (consortia) met (derden) supply-chain partners aan te gaan (denk bijv. aan de B2C Senseo / Beertender Business modellen !!); zijn wij ervan overtuigd dat de project partners in "Buiten Beter" vanuit het oogpunt van Business Development en Marktpositionering in staat moeten zijn gezamenlijk hun marktaandeel nog succesvoller, sterker en versneld te kunnen uitbouwen.! Dit laatste met als ultiem resultaat: de verkoop een sterke en positieve impuls te geven!

De 3 Kernprincipes die bij de rolverdeling binnen bijv. Geo-ICT gebaseerde "One-Stop Solution" Business Supply-chain Partnership samenwerkingsverband die door iedere ketenschakelpartner met elkaar onderling moet worden afgestemd en gedeeld zijn een combinatie van een 3-tal uitgangspunten:

- specifieke bedrijfseigen expertise te vertalen in de kreet: "*Schoenmaker houd je bij je leest*";
- vervolgens afstemming van de totale verantwoordelijkheid voor de te leveren producten/diensten: m.a.w. de keuze bij welke Ketenpartner de "Customer Loyalty functie" naar de eindgebruiker(klant) toe neer te leggen en te vertalen in de kreet: "*Samen uit, samen thuis*"
- en tot slot; goede afstemming tussen en met de Supply-chain ketenpartners mbt. de verdeling van de onderlinge kosten & opbrengsten en te vertalen in de kreet: "*Eerlijk zullen we met en tussen elkaar alles delen*".

Op deze wijze ontstaat in korte tijd een bijna onverslaanbare marktpositie van het samenwerkings-verband (bijv. vorming van een exclusieve consortium), die rekening houdt met de complexe samenhang van ICT producten, content, netwerken en diensten en die bovenal ook in tijd uitgedrukt, een behoorlijk sterke concurrentie voorsprong zal bieden!

Belangrijk hierbij is dat project partners in "Buiten Beter" gezamenlijk een heldere en specifieke Markt- en Doelgroep focus ontwikkelen, afstemmen en overeenkomen.

Zoals eerder aangeven zal hierbij met name rekening worden gehouden met de inrichting van zg. **M- Commerce**: Back- en Frontoffice” omgeving alsmede met de grote keuze aan Mobile office Geo-ICT user platforms (PDA's & Smartphones), applicaties, content behoeften en bijbehorende telematica systemen (zie onderstaand Model).



Tabel: J

M- Commerce Model: "Back- en Frontoffice" alsmede Mobile office Geo-ICT applicaties en bijbehorende telematica systemen

Aanbevelingen voor het project "Buiten Beter" mbt. vertaling & implementatie van Klanten wensen:

Boodschap is: klanten wensen te vertalen rekening houdend met de navolgende uitgangspunten:

Modelleren: Concentreer je niet op één schakel in de keten, maar beschouw ook de aangrenzende omgeving: geen lokale problematiek, maar ketenproblematiek.

Programmeren: Modellen moeten passen en ingepast worden in het ICT-landschap van bedrijven, inclusief alle systemen en koppelingen.

Implementeren: Systemen moeten daadwerkelijk gaan functioneren: gebruikers moeten worden opgeleid, processen en instructies moeten worden aangepast. Binnen de Operations research en IT is er sprake van zowel een automatiserings- als een procesveranderings-traject.

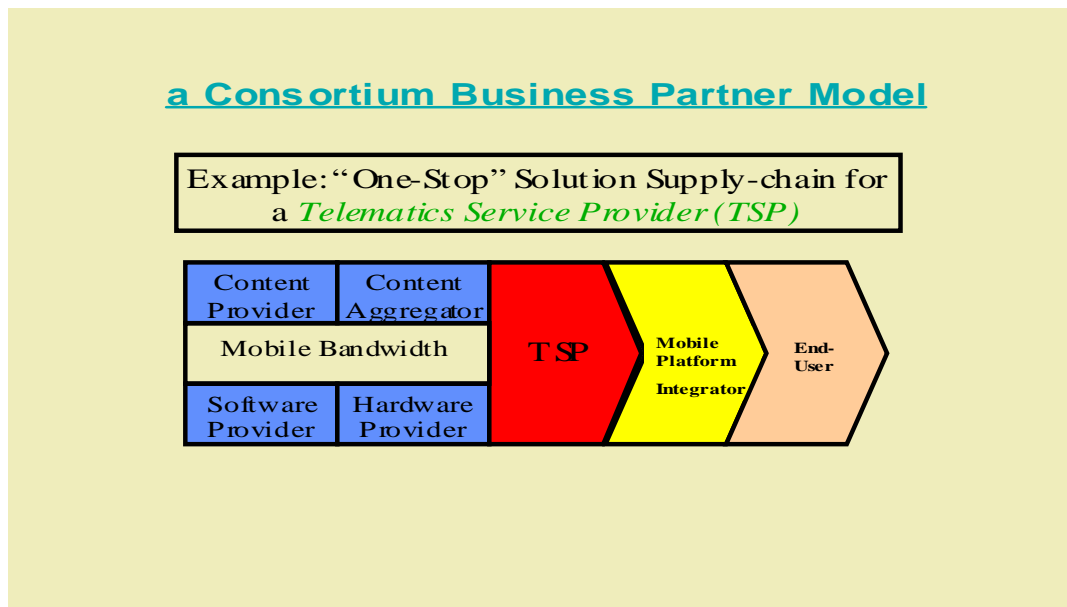
Binnen de groep van projectpartners betrokken bij het project "Buiten Beter" zal een keuze dienen te worden gemaakt wie van de Supply-chain partners de begeleiding & implementatie van voornoemde werkzaamheden op zich gaat nemen. Bij voorkeur is dit de partner die de sterkste "Customer Loyalty" band met de (potentiële) opdrachtgever heeft en tevens binnen het specifieke markt segment door gebruikers erkend wordt als een van leidende Geo-ICT leveranciers met een respectabele kennis en overtuigend marktaandeel in de betreffende markt! Deze partner wordt in principe door de mede-ketenpartners aangesteld als *consortium leider* en deze zal vervolgens namens de partnergroep de rol van *Telematics Service Provider* en verantwoordelijkheid op zich nemen om als "*Sparringpartner*" naar de opdrachtgever toe; *alle* hierboven aangegeven werkzaamheden in de breedste zin van het woord, operationeel (m.a.w. commercieel, technisch, PR, marketing enz.) adequaat te gaan coördineren, af te stemmen en te implementeren. M.a.w. de opdrachtgever heeft maar 1 loket om bij aan te kloppen bij invulling van zijn/haar wensen!

Taken die de Telematics Service Provider naar de Klant toe zal moeten aanbieden zijn o.a. vaststelling van de beste samenwerkingsvorm in het kader van vertaling en aanbod van de optimale (mobile) Geo-ICT pro-

ducten & diensten portfolio. Eea. binnen de met mede ketenpartners vast te stellen wensen en haalbare financiële kaders. Voornaamste oogmerk is: het blijvend motiveren en vergroten van Loyaliteit en Binding niet alleen naar met de opdrachtgever maar ook binnen de groep van Supply-chain partners(consortium) en deze toekomst bestendig en succesvoller maken! Dit laatste zal zeker lukken, indien ervoor gezorgd wordt dat de uiteindelijke opdrachtgever een permanent gevoel van **COMFORT** geboden kan worden!!

Als Aanbeveling aan de project deelnemers van “Buiten Beter” bij de vertaling en implementatie van klantenwensen bij toezichthouders en opsporingsambtenaren in het veld mbt. de keuze en samenstelling van het portfolio aanbod van (mobiele) Geo-ICT produkten & diensten; geven wij in overweging: gebruik te maken van navolgende Geo-ICT “One-Stop Solution” Solution Business Services Supply-chain Partnership procesmodel-: waarbij het uitgangspunt is: dat **EEN** van de huidige RGI-149 Geo Info- To Go project partners bereid is – in financieel economisch en technisch operationeel opzicht, zowel de rol en verantwoordelijkheden van “**Service Provider**” (zie rode Schakel TSP in onderstaand Ketenproces Partnership samenwerkingsmodel) aan te nemen cq. in te vullen?

Ketenpartnership samenwerkingsmodel: Geo-ICT “One-Stop Solution” Solution Business Services process Supply-chain voor een Telematics Service Provider (TSP)



Tabel: K

Beantwoording Onderzoeksvraagstelling: Organisatorische draagvlak/haalbaarheid “One-Stop” Solution Ketenpartner samenwerkingsmodel tbv Project deelnemers “Buiten Beter”

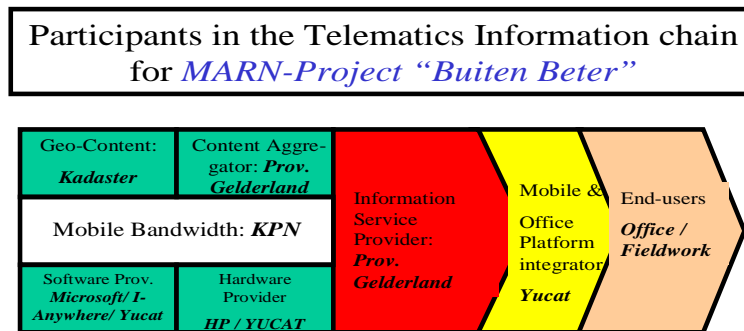
Vraag: Zijn gebruikers in het project “Buiten Beter” beter gediend bij het aanbod van een organisatorisch GEO-ICT gebaseerde “One-Stop Solution” Location Intelligent Business Services Supply-chain Partnership samenwerkings- en informatie consortiummodel? En zou **EEN** van de huidige RGI-149 Geo Info- To Go project partners bereid zijn; in financieel economisch, organisatorisch en technisch operationeel opzicht, zowel de rol en eindverantwoordelijkheden van die van “**Service Provider**” aan te nemen cq. in te vullen?

Antwoord: Na verkennende gesprekken met Henk Janssen; Coördinator Handhaving Milieusamenwerking & Afvalverwerking Regio Nijmegen(MARN) en Barry Peet; Mede-Directeur YUCAT, bleek in het kader van een verdere Doelontwikkeling, Opschaling en Bijscholing (DOB) van betrokkenen bij het Project “Buiten Beter”, behoefte te bestaan aan een gewijzigde aanpak van het huidige, overwegend uit provinciale en gemeentelijk instanties bestaande samenwerkingsverband. Hierbij wordt gesuggered dat mogelijk het extern aanbesteden en outsourcen van die taken en functies die qua kennis en inhoud niet direct met de maatschappelijke uitvoering en handhaving van MARN gerelateerde gebie-

den te maken hebben een wenselijke oplossingsrichting is. M.a.w. MARN zegt: “Schoenmaker, Houdt je bij je leest” en besteed meer en gerichtere aandacht mbt. inhoudelijke Doelontwikkeling, Opschaling en Bijscholing van Milieu-opsporingsambtenaren in het veld als ook van het centrale provinciale Coördinatie centrum met de daaraan gekoppeld de diverse gemeentekantoren organisaties ipv. minder specifiek opgeleide en ervaren eigen mensen bijv. ondersteunende Geo-ICT technisch operationele netwerk & systeem applicatie help-desk diensten 24x7x365 per jaar, te laten uitvoeren. Eea. zou een behoorlijke verbetering kunnen betekenen voor de onderlinge productiviteit, inhoudelijke actualisatie van specifieke milieu werkkennis binnen en tussen de verschillende milieu “*Kleur Sporen*”, alsmede bijna zeker ook de werkvreugde van betrokkenen.

Een voorstel zoals in dit hoofdstuk 6 is beschreven mbt. invoering van een **Ketenpartnership samenwerkingsmodel** naar voorbeeld van een Geo-ICT “One-Stop Solution” Solution Business Services process Supply-chain concept, onder leiding van een nader te selecteren Telematics Service Provider (TSP) die als **een centraal loket** naar de opdrachtgever, de algehele Geo-ICT gerelateerde organisatorische en technische eindverantwoordelijkheid draagt, is zeker bespreekbaar en behoort tot de mogelijkheden voor aanbesteding/outsourcing van toekomstige werkzaamheden
Vertaald naar de huidige organisatie, taken, verantwoordelijkheden en werkzaamheden , ziet het Geo-ICT Ketenpartnership samenwerkingsmodel er ongeveer als volgt uit:

Mobile Telematics Information Services Business Model



Tabel: L

Appendix A

Organisations & reference Reports that expressed concerns about the reliability of Radio-navigation systems

International Maritime Pilots' Association (IMPA), IMPA Resolution 'Vulnerability of Satellite Navigation Systems (GNSS) – 12, August 2nd, 2002.

Royal Institute of Navigation (RIN), Statement from NAV02, 'In order to ensure that Galileo can contribute to a robust global navigation and timing infrastructure, this conference strongly recommends that European Administration recognise the key findings of the US Volpe Report, the NAV02 proceedings and other studies of the significant vulnerability of GNSS to loss of signal, interference and jamming. The conference noted that many of these concerns apply to Galileo as well as GPS', 5-7 November 2002.

Royal Institute of Navigation (RIN), 'Council Statement on the vulnerability of GNSS and the desirability of providing a terrestrial backup', March 31, 2004. and RIN - Annual General Meeting; 29 June 2007

Confederation of European Shipmasters' Associations (CESMA), Resolution No 2 'LORAN-C as Backup for Satellite Navigation Services', 9th Annual General Assembly, Bilbao, Spain, June 19, 2004.

IALA, International Association of Lighthouse Authorities: Loran-C and Chayka in the 21st Century, 13-14 September 2004.

IALA, IALA Recommendation R-129 on GNSS Vulnerability & Mitigation Measures, Edition 1, December 2004.

Netherlands Institute of Navigation (NIN), Letters regarding decommission of NELS to the six ministers of Transport, of Economy, of Interior affairs, of Foreign Affairs, of Justice, of Defence, of Finance, and of Agriculture, respectively. May 12, 2004

US National Space-Based Positioning, Navigation and Timing (PNT) Advisory Board; Ronald Reagan Building and International Trade Center; 1300 Pennsylvania Avenue, NW, Polaris Suite Washington, D.C. 20004 - March 29-30, 2007

VAISALA: LORAN-C Based Windfinding in Meteorology, Juhana Jaatinen; Sakari Kajosaari & Ari Meskanen, presented by Kenneth Goss- 2005

Marc Clerens and Ralf Steinemann, ELSIS AG, Germany-presentation "e-Trackers"; Loran + GNSS + GSM based Container & Goods Tracking at at European Navigation Conference(ENC) 2006 in Manchester, UK

Ministry of Transport, Infrastructures, Tourism, and the Sea- France; mr. Jacques MANCHARD, Head of the Maritime Ads to Navigation Division (Phares et Balises) at (ENC) 2006 in Manchester, UK

Dr Sally Basker, Radionavigation Strategy Director Trinity House, Tower Hill, London, EC3N 4DH, UK at Trinity House CGSIC Meeting, September 2005, subject: e-Navigation: The way ahead for the maritime sector

IMO Sub-committee on Safety of Navigation ; 20 April 2007- NAV 53/13 : Development of an e-navigation Strategy; Report of the correspondence Group on e-navigation, Submitted by the United Kingdom

EUGIN (European Institutes of Navigation), Chairman Drs. R. van Gooswilligen at GNSS-ENC 2006 in Manchester & GNSS- ENC 2007 in Geneva.

Vulnerability of currently available position determination systems for use by the sector 'Openbare Orde en Veiligheid', 20 June 2005; Prof.dr.ir. D. van Willigen – Reelektronika b.v.

Aug. 2006, Strategy & Policy Report "White Paper" for US Federal Aviation Authority (FAA), title: "GPS Back-up for Position, Navigation & Timing"

Nov. 2006 ,Dissertation titled: "New Potential of Low Frequency Navigation in the 21th Century"by Dr. W. J. Pelgrum

Juli 2007, US report on Satellite Navigation Back-up Study Report for Next Generation Air Transport System(NGATS) Institute, issued by ITT Advanced Engineering & Sciences.

Appendix B

Nuttige Internet Website adressen:

- 1) Kwetsbaarheid / Integriteit van netwerken voor Satelliet Radio signalen mbt. Navigatie, Plaatsbepaling & Timing (NPT) functies **the US VOLPE report**, available to the public on the US Coast Guard Navigation Center website: <http://www.navcen.uscg.gov/archive/2001/Oct/FinalReport-v4.6.pdf>
- 2) de **verhelderende video** met titel: "GPS signaal extreem kwetsbaar" - op TV uitgezonden op 22 oktober 2004 tijdens het actualiteiten programma: **TweeVandaag**, zie http://www.tweevandaag.com/call.php?module=PX_Video&func=view&vid=18457&startvideo=1
- 3) de door de Europese Cie. in de herfst van 2005 te "releasen" **White Paper "European Radio Navigation Plan" (ERNP)** voor de totstandkoming binnen Europa van een uniforme strategie, beleid en standardisatie mbt. Navigatie, Plaatsbepaling en Timing infrastructuur, applicaties & diensten. Zie ook www.helios-tech.co.uk/ernp of http://europa.eu.int/comm/dgs/energy_transport/galileo/whatsnew/index_en.htm
- 4) **EU- IST 6^e Kader Telematica programma's voor Safety & Security** (o.a. E-Call 112 Driving Group en **Global System for Telematics (GST)**- Open Architectures met o.a. sub-projects (*Rescue, Floating Car Data, Security, Service payments & Safety Channel*)
- 5) **EUGIN (European Institutes of Navigation)** : http://www.rin.org.uk/bfora/systems/xmlviewer/default.asp?arg=DS_RIN_ABOUTART_69/ list.xsl/92
- 6) **Het Nederlands Instituut voor Navigatie (NIN)**: <http://www.navnin.nl/> is een non-profit vereniging met als doel het bevorderen, ontwikkelen, verdiepen, bundelen en verbreiden van kennis op het gebied van plaatsbepaling, navigatie en tijdmeting (PNT). De vereniging is al 20 jaar actief in alle sectoren die gebruik maken van de technologische ontwikkelingen op dit terrein: te land, ter zee, in de lucht, en in de ruimte.