SPEZIELLE ANFORDERUNGEN ZUR INTEGRATION MILITÄRISCHER GPS EMPFÄNGER IN NAVIGATIONSSYSTEME

Th. Löffler
Diehl BGT Defence GmbH
88662 Überlingen, Alte Nussdorfer Strasse
Deutschland

1. ÜBERSICHT

Das Globale Satelliten Navigationssystem NAVSTAR-GPS (**NAV**igation **S**ystem with **T**iming **A**nd **R**anging **G**lobal **P**ositioning **S**ystem), das vom U.S. Department of Defense (DoD) entwickelt wurde und zur Zeit von zivilen und militärischen Nutzern gleichermaßen genutzt wird, ist aus militärischen Fahrzeugen wie Flugzeugen aller Art, Schiffen und auch Landfahrzeugen nicht mehr wegzudenken. Neben diesen klassischen militärischen Einsatzgebieten, zu denen auch Langstrecken- und Mittelstreckenraketen gehören wird GPS immer stärker in den Bereich der Kurzstreckenraketen eingesetzt. Aufgrund der recht kurzen Einsatzdauer und begrenzten Reichweite der Kurzstreckenraketen ergeben sich besondere Anforderungen an die zu verwendenden GPS Empfänger.
Dieser Beitrag diskutiert die entsprechenden Anforderungen, die es ermöglichen ein GPS gestütztes Navigationssystem in Flugkörpern mit relativ kurzer Einsatzdauer und begrenzter Reichweite einzusetzen.
Diese Anforderungen werden von der neusten Generation der militärischen PPS GPS Empfänger, den so genannten SAASM (**S**elective **A**vailability **A**nti-**S**poofing **M**odul) basierten GPS Empfängern erfüllt.
Aufgrund des Einsatzes des Flugkörpers in einer nicht kooperativen Umgebung muss von Störmaßnahmen durch den Gegner zumindest im Zielgebiet ausgegangen werden. Dadurch muss das Flugkörpernavigationssystem neben einem GPS Navigationssystem zumindest noch ein Inertialnavigationssystem enthalten. Dieser Artikel diskutiert die beiden, zur Zeit bei der Fa. Diehl BGT Defence verwendeten Koppelungsverfahren, das „loosely-coupled“ GPS/INS Navigationssystem und das „tightly coupled“ GPS/INS Navigationssystem

Schwerpunkt dieses Artikels ist die Integration eines GNSS (Global Navigation Satellite System) in ein Navigationssystem für eine Flugkörperanwendung. Weitere Stützverfahren, bzw. Stützsensoren, die die Leistungsfähigkeit des Flugkörpers weiter steigern, werden im Rahmen dieses Artikels nicht diskutiert.

2. SPEZIELLE MILITÄRISCHE GPS ANFORDERUNGEN

Nachdem in Zeiten des „Kalten Krieges“ eine künstliche Verschlechterung, das so genannte SA (Selective Availability) dafür sorgte, dass potentielle gegnerische Nutzer das GPS Signal (ziviles Signal) nur mit reduzierter Genauigkeit verwenden konnten (horizontal ca. 100m, vertikal ca. 150m), hat sich die Situation mit Abschalten des SA im Mai 2000 verändert. Heutzutage hängen ganze Kommunikationsnetze, Vermessungs- und Positionierungsaufgaben, sowie die Schifffahrt oder der zivile Flugverkehr mehr oder weniger stark von der z. Zt. Verfügbaren GPS Genauigkeit (ohne SA) ab. Eine künstliche Verschlechterung oder gar weltweite SA Abschaltung hätte immensen Einfluss auf all diese zivilen Anwendungen und ist somit praktisch kaum realisierbar. Aus diesem Grund soll zukünftig, dass das zivile GPS Signal in einer bestimmten lokal begrenzten Region im Krisenfall nicht mehr verfügbar sein.
BILD 1 zeigt die geänderte Anforderung durch den Wechsel vom „Strategischen Konflikt“ zum „Lokalen Konflikt“. Diese Nichtverfügbarkeit des zivilen Signals im Krisengebiet bedeutet automatisch, dass der militärische GPS Empfänger in der Lage sein muss, direkt das militärische Signal zu akquirieren. Z. Zt. akquirieren die meisten militärischen GPS Empfänger zuerst den zivilen C/A-Code und wechseln anschließend mit Hilfe des HOW (hand over words) zum militärischen P(Y)-Code.

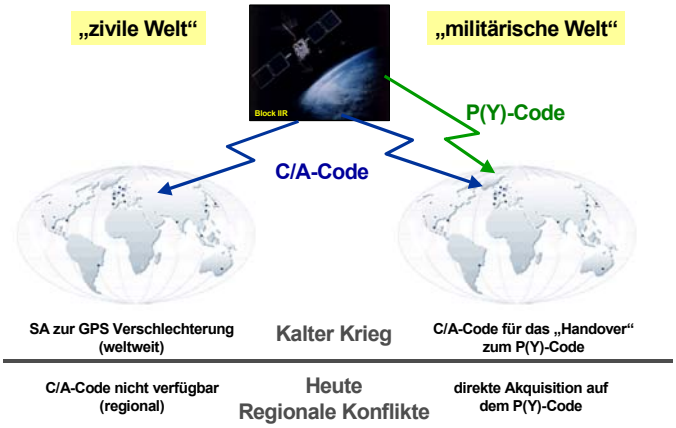

BILD 1: Geänderte Konfliktsituation

Ein typisches Einsatzszenario eines Flugkörpers ist in BILD 2 dargestellt. Dabei ist es natürlich unwesentlich, ob es sich bei der den Flugkörper tragenden Plattform um ein Schiff, ein Flugzeug, oder ein Landfahrzeug handelt.

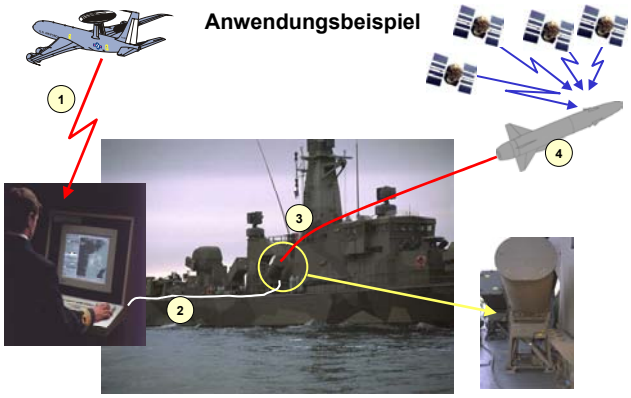

BILD 2: Typisches Flugkörper Einsatzszenario

1. Die Feuerleitung des Fahrzeuges erhält einen Feuerbefehl, mit diversen Zieldaten.
2. Das Feuerleitsystem aktiviert den Flugkörper und überträgt alle notwendigen Einsatzdaten
3. Der Flugkörper in einem Kanister wird nach seiner Initialisierung gestartet.
4. Nach kurzer Zeit muss der GPS Empfänger im Flugkörper direkt den militärischen P(Y)-Code akquirieren können.

Zusammenfassend kann gesagt werden, dass bei militärischen Flugkörperanwendungen an den, im Rahmen eines GPS/INS Navigationssystems integrierten GPS Empfänger, folgende Anforderungen gestellt werden.

- Der Empfänger muss sehr schnell Satelliten akquirieren.
- Der Empfänger muss direkt den militärischen Code (P(Y)-Code) akquirieren können (= D/Y acquisition)
- Der Empfänger muss resistent bzgl. Störung und Täuschung sein
- Der Empfänger muss neben den PVT-Daten (position, velocity, time)auch die kompletten „Rohdaten“, PR- (pseudo range) und DR- (delta range) Daten liefern.

3. AUFBAU EINES SAASM BASIERTEN GPS EMPFÄNGERS

Neben der oben dargestellten Notwendigkeit, dass die militärischen GPS Empfänger der neusten Generation direkt den militärischen P(Y)-Code akquirieren müssen, zeigte sich in der Vergangenheit, dass die bisherige militärischen GPS Empfänger der 2-ten Generation noch gewisse „Schwächen“ aufweisen.

So musste z.B. am 01. April 2001 ein US-Aufklärungsflugzeug vom Typ EP-3 Aries II nach einer Kollision mit einer chinesischen Maschine auf dem chinesischen Luftstützpunkt Lingshui notlanden.

BILD 3: Notgelandete US Maschine in China

Dies führte dazu, dass 1 Woche nach diesem Zwischenfall die GPS Kryptoschlüssel gewechselt wurden, da die Kryptosicherheit nicht mehr gewährleistet war.

Die neueste, d.h. die 3-te Generation der militärischen GPS Empfänger, die unter dem Schlagwort SAASM = **S**elective **A**vailability **A**nti-**S**poofing **M**odul bekannt geworden ist, zeichnet sich vor allem durch ein neues US Sicherheitskonzept aus.

Die wichtigsten Komponenten dieses Konzeptes sind:

- eine neue Sicherheitsarchitektur im Hardwaredesign des GPS Empfängers
- Anpassungen in den GPS Satelliten
- Definition neuer GPS Kryptoschlüssel

Nachfolgende Auflistung beschreibt kurz die wichtigsten Merkmale der SAASM Technologie.

1. Einführung der „Black Keys“, die im Gegensatz zu den bisher verwendeten „Red Keys“ nur noch als „unclassified – crypto“ eingestuft sind. Bei der Benutzung der „Black Keys“ müssen immer noch gewisse Vorschriften eingehalten werden. Im Vergleich zu der Nutzung der „Red Keys“ ergibt sich jedoch eine wesentliche Erleichterung. Gleichzeitig erhöht sich die gesamte Kryptosicherheit, da die „Black Keys“ selbst wieder verschlüsselt sind.

2. Einführung eines neuen Hardwaredesigns für die GPS Empfänger. Im Rahmen des neuen Sicherheitskonzeptes muss das Laden der sicherheitskritischen Software an einer zentralen Stelle erfolgen. So muss jeder Empfänger zur KLIF (KDP Loading and Installation Facility) nach Warner Robins Logistics Center, Georgia, um eine für die entsprechende Nation und Anwendung spezifische Software zu bekommen. Auf der anderen Seite bewirkt das neue Hardwaredesign, dass der GPS Empfänger auch dann „unclassified“ bleibt, wenn der GPS Schlüssel geladen wurde.

3. Einführung unterschiedlicher Kryptonetze. Dies bedeutet, dass jeder Nation ein eigenes primäres Kryptonetz zugeordnet ist. Somit haben z.B. Deutschland und Frankreich unterschiedliche Kryptonetze, die auch unterschiedliche GPS Schlüssel erfordern.

4. Fähigkeit der „direct-Y“ Akquisition nach einer entsprechenden Initialisierung. Neben der Bereitstellung der entsprechenden Initialisierungsdaten erfordert diese Funktion auch ein geeignetes Hardwaredesign. Dies wird vor allem dadurch erreicht, dass der GPS Empfänger die Akquisition mit Hilfe einer Vielzahl von parallel arbeitenden HW-Kollelatoren durchführt.

5. Der Erhöhung der Anti-Jamming Fähigkeit. Die Resistenz gegen Stör- und Täuschversuche des Gegners erfordert neben einem entsprechenden Hardwaredesign des Receivers auch ein geeignetes Design des Gesamtnavigationssystems, bestehend aus GPS Empfänger, Inertialsystem, GPS Antenne(n) und weiterer Stützsensorik.

BILD 4 zeigt einen Vergleich zwischen einem PPS-SM basierten militärischen GPS Empfänger der 2-ten Generation und einem SAASM basierten Empfänger der 3-ten Generation.

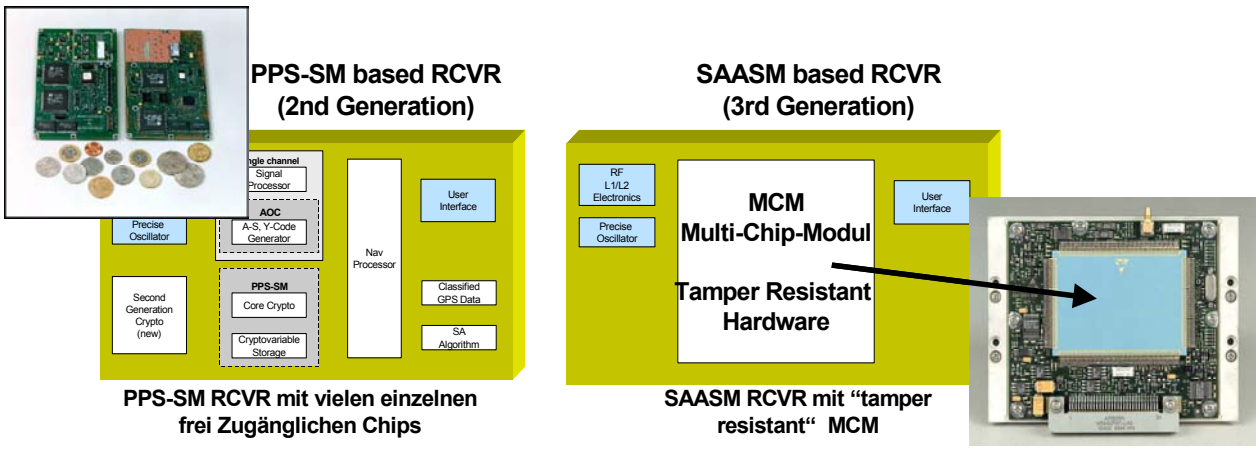

BILD 4: PPS-SM vs. SAASM Empfänger

BILD 4 verdeutlicht, dass der verbesserte Hardware Schutz in erster Linie darin besteht, dass alle sicherheitsrelevanten Funktionen, die bisher auf mehrere Hardware Module verteilt waren, in ein einziges „tamper resistant“ Multi-Chip-Modul integriert sind. Wie bereits erwähnt, bleibt dadurch auch der GPS Empfänger mit geladenem Schlüssel „unclassified“.

3.1. Initialisierung des GPS Empfängers

Ein kurzer Blick auf das Akquisitionsverfahren zeigt, warum ein GPS Empfänger, der direkt den militärischen P(Y)-Code akquirieren möchte sehr gut initialisiert werden muss. Unter der Voraussetzung, dass der übertragene verschüsselte Y-Code, entschlüsselt wurde (=P-Code) ist dieser, ebenso wie der übertragene zivile C/A-Code bekannt.
Das vom Satelliten gesendete Signal (Trägerfrequenz & modulierter Code) wird vom Empfänger „zeitversetzt“ und „doppler verschoben“ empfangen.

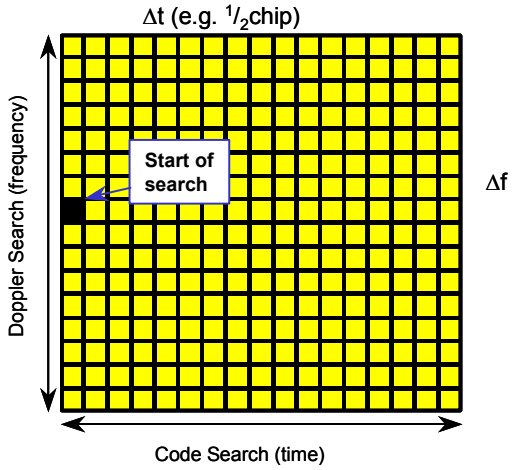

BILD 5: 2-Dimensionales Suchfeld

Im Rahmen eines 2-dimensionalen Suchprozesses (Korrelationsverfahren) gilt es nun diese Zeit- und die Frequenzverschiebung zu bestimmen. Es ist offensichtlich, dass die Größe des 2-dimensionalen Suchfeldes von der Genauigkeit der apriori Information abhängt. D.h. kennt der Empfänger seine eigene Position und Geschwindigkeit sowie die aktuelle GPS Zeit zusammen mit der Satelliten Position und Geschwindigkeit sehr genau, so kann die Größe des abzusuchenden Bereiches stark begrenzt und damit die Akquisitionszeit reduziert werden.

PRN-Code	P(Y)	C/A
Verschlüsselt	ja	nein
Periode	1 Woche; ~$6*10^{12}$chips	1ms; 1023chips
Chipping Rate [chips/s]	10.23M	1.023M
Chip Periode [□s]	0.09775	0.9775
„Entfernung“ pro Chip	29.3 m	293.0 m

TAB 1: P(Y)-Code und C/A-Code

Vergleicht man die Länge des P(Y)-Codes mit der des C/A-Codes in TAB 1, wird sofort klar, dass ohne eine deutliche Begrenzung des Suchbereichs durch eine entsprechende Initialisierung eine Akquisition in endlicher Zeit nicht erfolgreich sein kann.

Somit ist es für eine schnelle direkte Akquisition auf dem militärischen P(Y)-Code notwendig, dass der SAASM basierte GPS Empfänger mit folgenden Daten initialisiert wird:

- eigene Position und Geschwindigkeit
- sehr genaue aktuelle GPS/UTC Zeit (z.B. 1PPS-Signal, o.ä. Synchronisationsverfahren)
- Ephemeridendaten der Satelliten
- weitere Subframe-Daten, der Satelliten

Die oben genannten Daten kann z.B. ein geeigneter GPS Empfänger in geforderter Form liefern.

Zusätzlich ist natürlich auch der „richtige“ GPS Schlüssel notwendig, so dass der P(Y)-Code auch entschlüsselt werden kann, d.h. dass der Y-Code in den im Empfänger bekannten P-Code überführt werden kann.

3.2. GPS Schlüssel „crypto variables“ zur Nutzung des P(Y)-Codes

Wie in Kapitel 3 beschrieben besitzt der SAASM basierte GPS Empfänger ein tamper resistant Multi-Chip-Modul, das alle sicherheitskritischen Funktionen beinhaltet. Gleichzeitig besitzt der GPS Empfänger ein spezielles Interface, an das ein genehmigtes und eingeführtes Ladegerät zum Übertragen der GPS Schlüssel angeschlossen werden kann. Diese Standardprozedur setzt voraus, dass der GPS Empfänger mit Strom versorgt wird.
Für das in Kapitel 2 dargestellte Anwendungsbeispiel ist dieses Verfahren ungeeignet. Eine Grundvoraussetzung für den erfolgreichen Einsatz des Flugkörpers ist eine sehr schnelle Reaktion bei entsprechender Bedrohung.
Somit ist es z.B. nicht möglich die GPS Schlüssel schon beim Beladen der Kanister in den GPS Empfänger zu laden, da in diesem Fall der GPS Empfänger immer mit Spannung versorgt werden müsste, und im Falle eines abgelaufenen Schlüssels der Flugkörper wieder entladen werden müsste. Es ist unter operationellen Gesichtspunkten ebenfalls nicht möglich den entsprechenden GPS Schlüssel unmittelbar vor jedem Einsatz zu laden. Als einzige Alternative bleibt die Möglichkeit den GPS Schlüssel im Rahmen des Feuerleitsystems zwischenzuspeichern. Diese Lösung setzt jedoch ein mit entsprechenden Behörden abgestimmtes Hardware- und Software-Design voraus. Dabei muss der gesamte Hardware und Software Entwurf anhand vorgegebener US Vorschriften überprüft werden.

4. GEKOPPELTE GPS/INS NAVIGATIONS-SYSTEME

Es ist allgemein bekannt, dass die Kopplung eines Inertialnavigationssytems mit einem Satellitennavigationssystem (z.B. GPS) durch das komplementäre Systemverhalten besonders erfolgreich ist (siehe TAB 2).

	INS	GPS
Autonomie	hoch, bei bekannter Startposition	abhängig von SV Sichtbarkeit
Dynamik	sehr hoch	begrenzt
Fehlerverlauf	stark zunehmend mit t	konstant

TAB 2: Komplementäres Systemverhalten

Je nach Art der Kopplung kann man zwischen 3 Grundarten der Kopplung unterscheiden.

- Loosely coupled GPS/INS System
- Tightly coupled GPS/INS System
- Deeply coupled GPS/INS System

Hierbei muss angemerkt werden, dass unterschiedliche Autoren auch unterschiedliche Einstufungen verwenden, so ist in entsprechender Literatur auch Closely coupled GPS/INS System beschrieben. Meiner Meinung nach reichen diese 3 Einstufungen prinzipiell aus, wobei es dann natürlich auch gewisse Mischformen gibt.
Im Rahmen der Flugkörperanwendungen wird bei Diehl BGT Defence hauptsächlich das so genannte „Tightly Coupled“ GPS/INS System realisiert.

4.1. Loosely-Coupled GPS/INS Systeme

Ein “Loosely Coupled” GPS/INS besteht im Prinzip zwei eigenständige Navigationssysteme. Aus den Navigationslösungen (Position und Geschwindigkeit) der beiden unabhängigen Systeme wird mittels eines extended Kalman Filters eine „optimale“ Position und Geschwindigkeit berechnet. (siehe BILD 6).

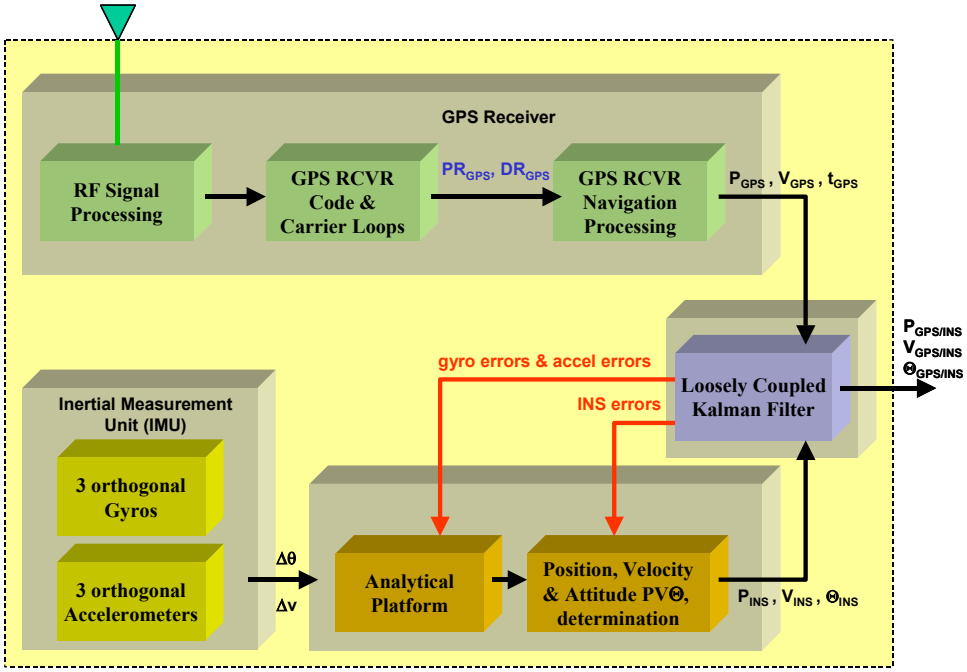

BILD 6: Loosely Coupled GPS/INS System

Mit einem Loosely Coupled GPS/INS System erreicht man bei einem gut überschaubaren Systemansatz,

+ hohe Genauigkeit, falls eine ausreichende Zahl an Satelliten getrackt werden
+ große Unabhängigkeit der einzelnen Navigationssysteme,

wobei

- der GPS Empfänger immer mind. 4 Satelliten empfangen muss.
- die Störresistenz und Dynamikfähigkeit des GPS Empfängers nicht gesteigert wird.

4.2. Tightly-Coupled GPS/INS Systeme

Kennzeichen des Tightly coupled GPS/INS System ist, dass für die Kopplung der beiden Systeme interne Messgrößen, wie die Pseudoentfernung (PR: Pseudo Range) und die Änderung dieser PR (DR: Delta Range) des GPS Empfängers genutzt werden. Gleichzeitig erhält der GPS Empfänger Informationen vom Inertialsystem zur Stützung seiner internen Regelkreise, so dass er wesentlich unempfindlicher gegenüber absichtlichen und unabsichtlichen Störungen wird.

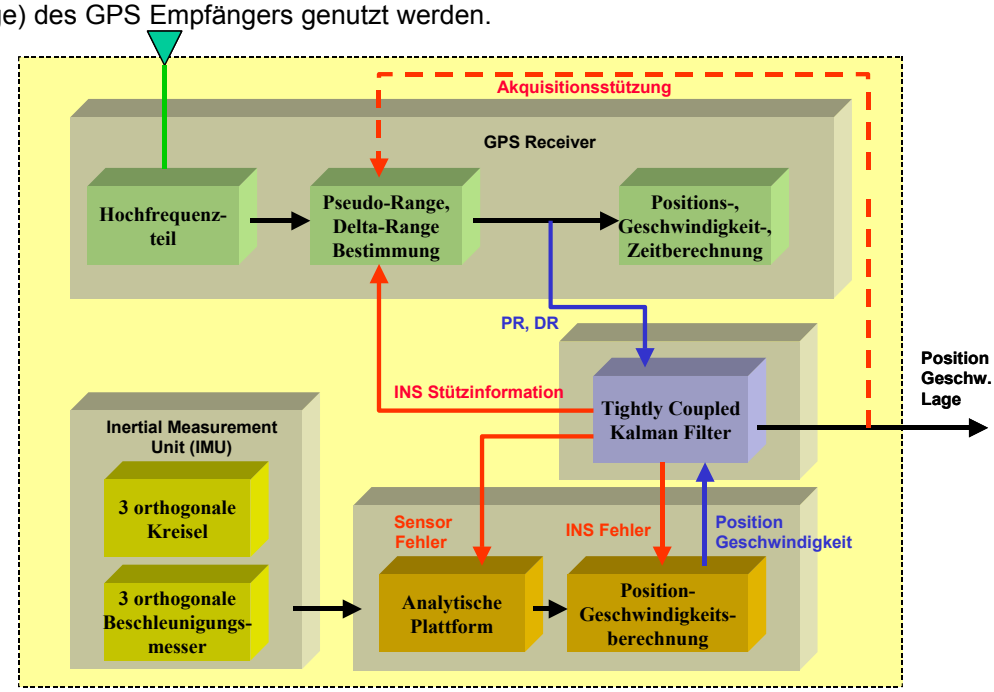

BILD 7: TightlyCoupled GPS/INS System

Mit einem Tightly Coupled GPS/INS System erreicht man

+ Positionsstützung auch bei weniger als 4 Satelliten,
+ größere Störresistenz, durch Stützung des GPS Empfängers mittels des INS, und individueller Bewertung der Messungen (PR, DR) mittels eines MAIM (Missile Autonomous Integrity Monitoring) Systems
+ Steigerung der Fähigkeit Satelliten auch bei hoher Missionsdynamik zu tracken,

wobei

- der GPS Empfänger interne Daten (PR, DR) über die Schnittstelle liefern muss.
- der Systementwurf deutlich aufwendigerer ist.

4.3. Deeply GPS/INS Systeme

Während die beiden oben erwähnten Systeme bereits in vielen Anwendungen implementiert sind oder zur Zeit werden, wird an der nächsten Integrationsstufe gearbeitet. In diesem Fall greifen die INS Stützdaten direkt in die Regelkreise des GPS Empfängers ein. Somit lässt sich die Dynamikfähigkeit und die Störresistenz nochmals steigern. Gleichzeitig verschmelzen aber die beiden Systeme untrennbar zu einem System. Das Deeply Coupled System ist dadurch sehr eng mit dem Soft- und Hardwaredesign des GPS Empfängers verknüpft.

4.4. GPS/INS Systeme bei Diehl BGT Defence

In den neunziger Jahren realisierte BGT die Fahrzeugnavigationsanlage GPA als Loosely Coupled GPS/INS mit dem militärischen „hand held“ Empfänger PLGR. Heute werden bei DBD für Flugkörperanwendungen moderne INS Systeme, meist bestehend aus faseroptischen Kreiseln (FOGs) und MEMS-Beschleunigungsmessern mit militärischen GPS Empfängern neuester Technologie (SAASM basiert) fusioniert. Hierbei werden „Loosely Coupled“ GPS/INS Systeme erweitert um eine INS Aiding Funktion, und vor allem „Tightly Coupled“ GPS/INS Systeme realisiert. Gleichzeitig beinhaltet das GPS/INS System, je nach Anwendung auch weitere Funktionen, wie einen Autopiloten oder eine Flugführung zu bestimmten Wegpunkten oder auch zu einem Zielpunkt. BILD 8 zeigt einen Auszug der bei Diehl BGT Defence entwickelten GPS/INS Systeme. Diese Systeme werden in nationalen und internationalen Programmen, die z.B. zusammen mit den USA oder Schweden durchgeführt werden eingesetzt.

BILD 8: GPS/INS Systeme bei Diehl BGT Defence (Auszug)

5. AUSBLICK

Meiner Meinung nach wird auch in Zukunft für alle militärischen Systeme, die in Krisenregionen zum Einsatz kommen können, das GNSS (Global Navigation Satellite System) NAVSTAR GPS der US Amerikaner Verwendung finden. Die erfolgreiche Verwendung der z. Zt. entwickelten Systeme, die auf SAASM basierten GPS Empfängern beruhen, ist über entsprechende Verträge über Jahre hinaus gesichert.

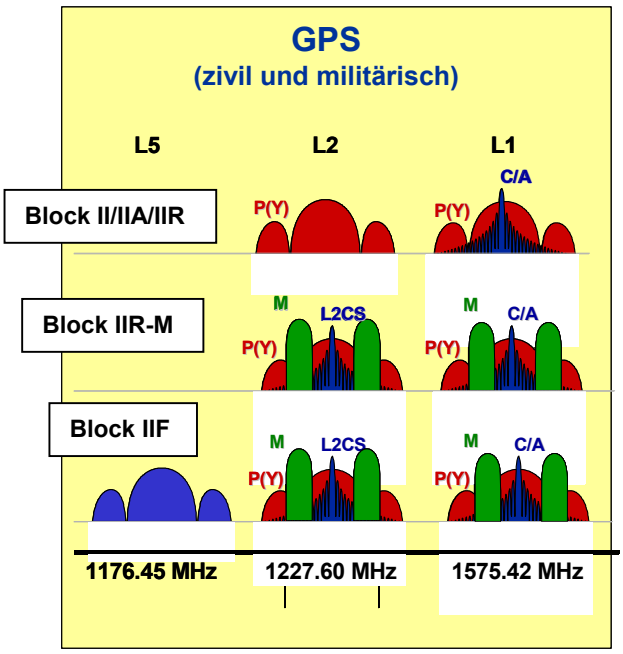

BILD 9: GPS Modernisierung

Eine deutliche Verbesserung, vor allen bzgl. des Akquisitionsverhaltens ergibt sich mit der Einführung des neuen militärischen M-Codes (siehe BILD 9). Der erste Satellit, der den neuen M-Code überträgt (Block IIR-M) wurde Ende 2005 in seine Umlaufbahn gebracht. Mit ersten Empfängern, die M-Code fähig sind ist 2009-2010 zu rechnen.
Der erste Start eines Block IIF Satelliten ist z.Zt. für das Jahr 2007 geplant, wobei sich aber alle in jüngster Vergangenheit geplanten Starts verzögert haben.

6. LITERATUR

[1] Elliott D. Kaplan, Christopher J. Hegarty
Understanding GPS, Principles and Applications (Second Edition)
ARTECH HOUSE, 2006

[2] Thomas Löffler, John Nielson
More Precise HARM, GPS/INS Integration to Improve Missile
GPS World, May 2002

[3] Hugo Fruehauf, Steven Callaghan
SAASM and Direct P(Y) Signal Acquisition
GPS World, July 2002

[4] Colonel Allan Ballenger
GPS Status Update
ION GPS 2005, Plenary, 13. Sept. 2005

[5] Thomas Löffler, John Nielson
A GPS/INS Application to Improve Missile Effectiveness and Minimize Fratricide
ION GPS 2001, 11.-14. Sept. 2001