NATO | NATO STANDARDIZATION AGENCY
OTAN | AGENCE OTAN DE NORMALISATION
NSA

25 October 2007 NSA/0975(2007)-C3/4580

STANAG 4580 (EDITION 1) – METHOD OF EXPRESSING NAVIGATION INTEGRITY

References:

a. AC/322(SC/8)DS(2007)0001, dated 18 April 2007 (NU)
b. AC/322(SC/8)N(2007)0011, dated 20 July 2007
c. AC/322(SC/8)N/101, dated 17 February 2001 (NU) - Ratification Request

1. The enclosed NATO Standardization Agreement, which has been ratified by nations as reflected in the **NATO Standardization Document Database (NSDD)**, is promulgated herewith.

2. The reference (c) is to be destroyed in accordance with local document destruction procedures.

ACTION BY NATIONAL STAFFS

3. National staffs are requested to examine their ratification status of the STANAG and, if they have not already done so, advise the NHQC3S, through their national delegation as appropriate of their intention regarding its ratification and implementation.

Juan A. MORENO
Vice Admiral, ESP(N)
Director, NATO Standardization Agency

Enclosure:
STANAG 4580 (Edition 1)

NATO Standardization Agency – Agence OTAN de Normalisation
B-1110 Brussels, Belgium Internet site: http://nsa.nato.int
E-mail: c3s@hq.nato.int – Tel 32.2.707.4311 – Fax 32.2.707.5709

STANAG 4580
(Edition 1)

NORTH ATLANTIC TREATY ORGANIZATION
(NATO)

NATO STANDARDIZATION AGENCY
(NSA)

STANDARDIZATION AGREEMENT
(STANAG)

SUBJECT: **METHOD OF EXPRESSING NAVIGATION INTEGRITY**

Promulgated on 25 October 2007

Juan A. MORENO
Vice Admiral, ESP(N)
Director, NATO Standardization Agency

RECORD OF AMENDMENTS

No.	Reference/date of Amendment	Date Entered	Signature

EXPLANATORY NOTES

AGREEMENT

1. This NATO Standardization Agreement (STANAG) is promulgated by the Director NATO Standardization Agency under the authority vested in him by the NATO Standardization Organisation Charter.

2. No departure may be made from the agreement without informing the tasking authority in the form of a reservation. Nations may propose changes at any time to the tasking authority where they will be processed in the same manner as the original agreement.

3. Ratifying nations have agreed that national orders, manuals and instructions implementing this STANAG will include a reference to the STANAG number for purposes of identification.

RATIFICATION, IMPLEMENTATION AND RESERVATIONS

4. Ratification, implementation and reservation details are available on request or through the NSA websites (internet http://nsa.nato.int; NATO Secure WAN http://nsa.hq.nato.int).

FEEDBACK

5. Any comments concerning this publication should be directed to NATO/NSA – Bvd Leopold III - 1110 Brussels - BE.

STANAG 4580
(Edition 1)

NAVY / ARMY / AIR

NATO STANDARDIZATION AGREEMENT
(STANAG)

METHOD OF EXPRESSING NAVIGATION INTEGRITY

ANNEX

A - Method of Expressing Navigation Integrity

AIM

1. The aim of the STANAG is to ensure that integrity of navigation will be expressed in a similar way throughout NATO to enable an easy comparison of integrity characteristics of navigation systems and the determination whether any particular system meets the integrity requirements of specific military operations.

AGREEMENT

2. Nations agree:

   a. to a common definition of Integrity for navigation systems.

   b. to a standard method of expressing integrity characteristics based on the use of a standard set of parameters.

DEFINITIONS

3. Applicable definitions are contained in Annex A.

GENERAL

4. The agreement contains one Annex. It provides definitions of integrity related terms and in particular those of the standard integrity parameters. In addition, the Annex contains guidelines on the use of the standard parameters to express integrity of a navigation system.

DETAILS OF AGREEMENT

5. Nations agree that:

   a. whenever integrity of navigation is expressed in NATO, the definition is the following one:

Integrity: The ability of a navigation system to provide timely warnings to determine if and when the system should not be used.

NOTE: In that definition "should" indicates a strong advice but not necessarily a mandatory action.

b. whenever integrity of navigation is expressed in NATO, the parameters used are the following ones:

(1) Alarm Limit
and/or
Marginally Detectable Bias and Marginally Detectable Error;

(2) Maximum Time to Alarm;

(3) Integrity Risk
or
Missed Detection Probability;

(4) False Alarm Rate
or
False Alarm Probability.

PROTECTION OF PROPRIETARY RIGHTS

6. Not applicable.

IMPLEMENTATION OF THE AGREEMENT

7. The agreement is implemented when a Nation has issued instructions that all national navigation integrity requirements will follow the provisions of this agreement.

ANNEX A

METHOD OF EXPRESSING NAVIGATION INTEGRITY

1. Summary

This annex provides definitions for terms used to express integrity of navigation systems and gives additional information to users on how to use the standard parameters to express integrity characteristics.

2. Definition of terms used to express integrity of navigation systems

a. Alarm:

Information given to the user that an (Integrity) Failure / Gross Error may exists.

b. Alarm Limit:

Maximum allowed difference between the output of the system and the true value without Alarm generation.

c. Failure rate:

Average number of (Integrity) Failure / Gross Error per unit of time

d. False Alarm (Type 1 Error):

Generation of an Alarm when no (Integrity) Failure / Gross Error exists.

e. False Alarm Probability:

Probability that an Alarm is generated when no (Integrity) Failure / Gross Error exists.

f. False Alarm Rate:

Average number of False Alarm per unit of time

g. Gross Error:

Gross Errors, or "Outliers", are errors other than random errors or systematic errors. They are often large and, by definition, unpredictable.

They are typically caused by changes in the prevailing physical circumstances, by system faults or by blunders.

h. (Integrity) Failure:

An (Integrity) Failure exists when the difference between the output of the system and the true value is greater than the specified Alarm Limit.

i. Integrity Risk:

Probability that an undetected (Integrity) Failure / Gross Error occurs per unit of time.

j. Marginally Detectable Bias (MDB):

The minimum size of the Gross Error in an observation that may be detected with given probabilities of type 1 (α) and type 2 (β). (NOTE: A type 1 error occurs when a correct observation is wrongly rejected, and a type 2 error occurs when an observation with a Gross Error is wrongly accepted).

k. Marginally Detectable Error (MDE):

The maximum (position) offset caused by a MDB in one of the Lines of Position or observations.

l. Missed Detection (Type 2 Error) Probability:

Probability that an existing (Integrity) Failure / Gross Error is not detected within the Maximum Time to Alarm.

NOTE: Integrity Risk = Missed Detection Probability * Failure Rate.
Or: Missed Detection Probability = Integrity Risk / Failure Rate.

m. Time to Alarm:

Elapsed time from occurrence of an (Integrity) Failure / Gross Error until an Alarm is given (A Maximum Time to Alarm would be specified as part of an integrity requirement).

3. **Additional definitions:**

a. Availability of integrity monitoring function:

Percentage of time that the integrity monitoring function is usable.

b. Continuity of integrity monitoring service:

Ability of the system to perform integrity monitoring function without interruption during a specified period.

4. **Guideline on the use of standard parameters to express integrity of a navigation system:**

The definitions given in this document are applicable to integrity aspects of all navigation systems. In order to assist users in expressing integrity requirement for navigation systems, the following examples are provided.

a. Generic system:

In the case of a generic system, the parameters used to express integrity requirements can be:

(1) Alarm Limit;
(2) Maximum Time to Alarm;
(3) Missed Detection Probability;
(4) False Alarm Rate.

The easiest values to determine are for the Alarm Limit and the Maximum Time to Alarm. Guidance on how to assess parameter values is provided hereafter:

(1) The Alarm Limit is the system error the user does not want to exceed without being informed of the existence of a problem. Under normal operating conditions of the system, the true position should be within this threshold from the navigation solution provided by the system. As the generation of an Alarm is based on a statistical analysis of the measurements made by the system, situations where the error is beyond the threshold and no Alarm is generated within the maximum Time to Alarm may however occur. Such situations must remain exceptional and their frequency must be extremely low (for example an Integrity Risk of less than 10^{-7} per hour).

(2) The Maximum Time to Alarm is related to safety margins and/or mission requirements. In most cases, it shall not exceed a few seconds.

(3) Missed Detection Probability has to be determined in order to calculate a very low Integrity Risk (for example an Integrity Risk of less than 10^{-7} per hour). To that end, some hypothesis must be made on the failure rate of the navigation system.

If the system has a failure rate around 0.0001 per hour, the Missed Detection Probability shall be 0.001 in order to achieve an Integrity Risk of 10^{-7} per hour.

(4) A low False Alarm Rate is required for most systems. To avoid unnecessary disturbance to the system user a False Alarm Rate of once per 100,000 hours is usually accepted.

b. GPS based system:

In the case of a GPS based system, the parameters used to express integrity requirements can be:

(1) Alarm Limit;
(2) Maximum Time to Alarm;
(3) Missed Detection Probability;
(4) False Alarm Rate.

The easiest values to determine are for the Alarm Limit and the Maximum Time to Alarm. Guidance on how to assess parameter values is provided hereafter:

(1) The Alarm Limit is determined as for the generic system.

(2) The Maximum Time to Alarm is related to safety margins and/or mission requirements. It can be less than one second when the integrity monitoring is managed by a GPS Receiver Autonomous Integrity Monitoring (RAIM).

(3) Missed Detection Probability is determined as for the generic system.

In the case of GPS, the Missed Detection Probability is calculated based on the hypothesis that the failure rate for the space and control segments is around 0.0001 per hour. As a consequence, for GPS based systems, the Missed Detection Probability has to be 0.001 in order to achieve an Integrity Risk of 10^{-7} per hour.

(5) For GPS based system, False Alarm Rate is usually fixed at about one every 100,000 hours in order to avoid unnecessary disturbance to the system user.

(6) In the document GUIDELINE FOR THE GPS RECEIVER APPLICATION MODULE (GRAM), the integrity requirement for Non-Precision Approach (NPA) navigation is:

(a) Alarm Limit: 556 m (0.3 nm);
(b) Missed Detection Probability: 0.001;
(c) Maximum allowable False Alarm Rate: 1/15000 h in PPS and 1/100000 h in SPS;
(d) Maximum Time to Alarm: 4 seconds;
(e) Integrity Risk: 10^{-7}.

The probability of missed detection is computed using the hypothesis that the failure rate for the GPS space and control segments is 0.0001.

The maximum allowable False Alarm Rate is computed assuming a fault-free error correlation time of 1 hour for authorised (PPS) operation.

NOTES :

(1) In the case of RAIM, the availability of the integrity monitoring function is directly linked to the Alarm Limit. To meet an availability of the integrity monitoring function of at least 95%, the Alarm Limit shall be around 100 m for the Precise Positioning Service (PPS) mode of operation.

(2) In usual RAIM algorithms, the false alarm rate is defined as the probability that the computed decision variable exceeds the fixed threshold for any given measurement. This definition is equivalent to the one in this STANAG if an alarm is generated as soon as the detection variable exceeds the threshold. If a satellite measurement is automatically excluded by the RAIM algorithm without alarm generation or if the algorithm waits for some consecutive values of the decision variable passing the threshold before generating an alarm, the false alarm definition used in RAIM is not equivalent to the one in this STANAG.

c. Generic maritime navigation system:

The following example is given for a navy integrated navigation system, but will in principle go for avionics and land navigation as well.

Figure 1 outlines the overall design for a navy navigation system, intended for large ships. The Navigation Computer (NAV-C) performs two tasks:

(1) Calculation of best estimation of the state vector (which includes position, velocity, set and drift) with its covariance matrix (from which the precision of the elements of the state vector can be derived);

(2) Integrity monitoring with Quality Control.

The main reason for installing two Inertial Navigation Systems (INS) on board a ship, is to maintain backup for the attitude and heading data for the various weapon systems. However, two INS combined with two GPS makes it possible to do some excellent integrity checks, because of the amount of redundancy.

In this example as much integrity functionality as possible is concentrated in the NAV-C. However, the GPS sensors can perform some additional integrity functions externally, e.g. by means of RAIM.

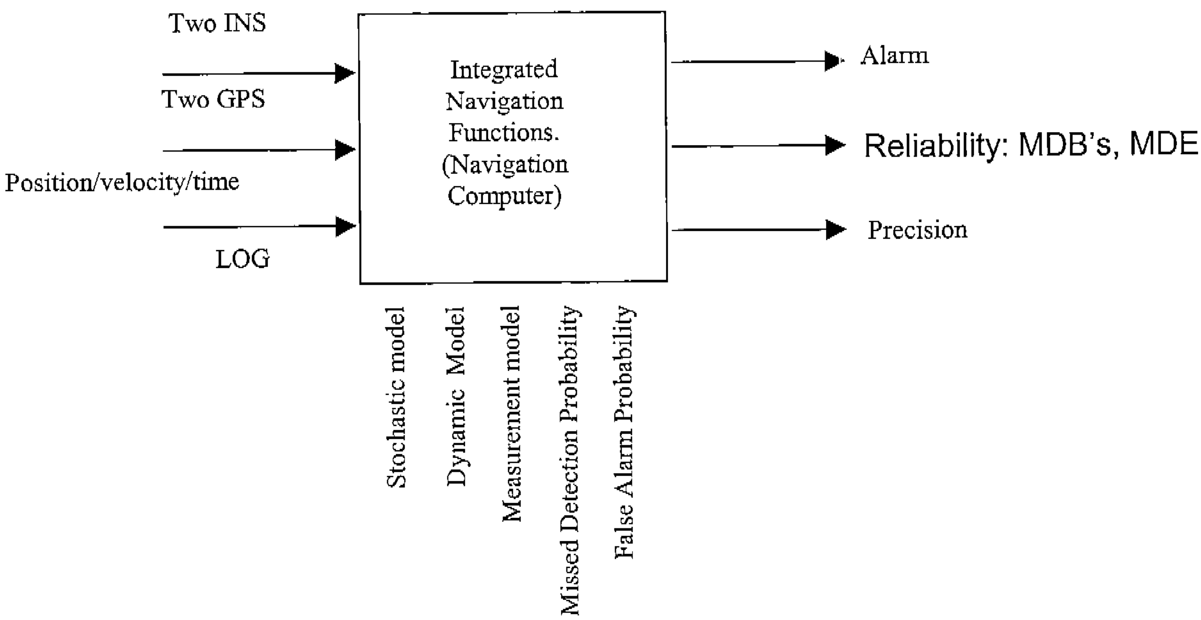

Figure 1. Simplified navigation system.

In the example the two INS are running in free inertial mode. This improves the integrity possibilities by allowing the NAV-C to detect (e.g. slowly drifting) accelerometer failure at an early state. The navigation computer calculates and compensates for the drift of the two INS. This task is normally done within the INS itself on the basis of GPS position input.

The NAV-C contains a stochastic model of each sensor on basis of its predicted precision, a measurement model that describes the relation between the measurements and the unknowns (position, velocity etc.) and a dynamic model, which describes the dynamics of the moving platform.

For the above-described system, the parameters used to express the integrity requirements are:

(1) Alarm
(2) MDB's and MDE
(3) Maximum time to alarm
(4) Missed Detection Probability
(5) False Alarm Rate

The NOTES in example 4.b are not applicable for this example, since definitions as alarm limit are chosen. The following descriptions are applicable for this case:

(1) By means of (sensor) redundancy a gross error can be detected and identified. The next step is to isolate or to compensate for it.

(2) The MDE is very much dependent on the number and the precision of the sensors used. Furthermore it is dependent on the chosen values of α and β. More accurate and precise sensors give the possibility to decrease the MDE.

(3) The maximum time to alarm is by some amount determined by the sensors, and their precision.

(4) The Missed Detection Probability has to be chosen. The United Kingdom's Offshore Operators Association (UKOOA) advises for typical marine applications a value of 20%.

(5) The False Alarm Rate has to be chosen. The UKOOA advises for typical marine applications a value of 1%.

BLANK PAGE BLANCHE