Original article
DOI: 10.21683/1729-2646-2017-17-2-41-47

A model of function-level fault tolerance of navigation signals provision processes in adverse conditions

Sergey M. Klimov, *4th Central Research and Design Institute of the Ministry of Defence of Russia, Korolyov, Russia*
Aleksey Yu. Polovnikov, *4th Central Research and Design Institute of the Ministry of Defence of Russia, Korolyov, Russia*
Aleksey P. Sergeev, *4th Central Research and Design Institute of the Ministry of Defence of Russia, Korolyov, Russia*


Sergey M. Klimov


Aleksey Yu. Polovnikov


Aleksey P. Sergeev

Abstract. *The aim of this article is to develop a model that would allow quantitatively evaluating the function-level fault tolerance of navigation signals provision processes in adverse reception conditions using consumer navigation equipment (CNE). The article also substantiates the relevance and importance of evaluation of the function-level fault tolerance of consumer navigation systems in those cases when the reception of the signals is affected by industrial interference, pseudo-satellites, rereflections from urban structures and terrain features. The function-level fault tolerance of the processes of navigation signals (of CNE) provision to consumers in adverse conditions is understood as their ability to fulfil their functions and retain the allowed parameter values under information technology interference within a given time period. The adverse conditions of provision of navigation data (signals) to consumers are understood as a set of undesirable events and statuses of reception and processing of navigation data with possible distortions. The article analyzes a standard certificate of vulnerabilities of navigation signal (by the example of distortion of pseudorange and pseudovelocity values distortion) that defines the input data for the analysis of CNE equipment fault tolerance. The model is based on the following approaches: the navigation signal parameters are pseudorange and pseudovelocity, system almanac data and ephemeris information; quantitative evaluation of function-level fault tolerance of the processes of navigation signals provision to users is based on the probability of no-failure of CNE in adverse conditions; function-level fault tolerance of the above processes is ensured by means of integrated use of functional, hardware, software and time redundancy; the hardware and software structure of the CNE fault tolerance facilities has the form of a three-element hot and cold standby system; the allowable level of function-level fault tolerance violation risk is defined according to the ALARP principle. It is shown that CNE fault tolerance and jamming resistance is based on the following: use of multisystem navigation receivers; navigation signal integrity supervision; spatial and frequency-time selection of signal; precorrelation processing of signal and interference mixture; postcorrelation signal processing; processing of radio-frequency and information parameters of the signal; cryptographic authentication; integration with external sources of navigation information and within a single signal processing system of a number of methods of interference countermeasures and pseudo-satellite navigation signals. The proposed model defines the CNE function-level fault tolerance as two variants of dynamic dependability models, in which the values of probability of no-failure are time-dependent: a hot standby system that includes three additional countermeasure modules and a cold standby system with a switch to three additional countermeasures modules. The model allows visualizing the processes of navigation signals provision to users in adverse conditions, quantitatively evaluating the probability of no-failure for hot and cold standby systems with three modules of information technology interference countermeasures, probability of recovery and CNE availability coefficient, as well as the allowable risk of CNE fault tolerance violation.*

Keywords: *navigation signals consumer, consumer navigation equipment, adverse conditions, function-level fault-tolerance, probability of no-failure.*

For citation: *Klimov SM, Polovnikov AYu, Sergeev AP. A model of function-level fault tolerance of navigation signals provision processes in adverse conditions. Dependability,2017;2: 41-47. DOI: 10.21683/1729-2646-2017-17-2-41-47*

Introduction

Currently, it is required to expand the application of services based on the GLONASS satellite radionavigation system (SRNS) both for national consumers and international application of Russian satellite navigation technology [1]. One of the key tasks of GLONASS development is to support the competitive performance of its guaranteed navigation field and further improve the system in terms of its consumer properties (most importantly, positioning accuracy).

The GOST R 52865-2009 standard defines the "satellite radionavigation system navigation field" as a set of radionavigation signals in the SRNS operating area that enables the measurement of navigation parameters and identification of the position and time of the consumer with the required level of availability, dependability and accuracy. Therefore, the navigation field is a set of radio signals at the input of the ground-based consumer equipment (CNE) that enables navigation and time definitions. A state-of-the-art CNE can be considered as a specialized computer system for collection, processing and output of navigation data to the consumer.

In the actual and complex conditions of GLONASS application (comparable to those of foreign space-based navigation systems) the integrity and availability of the received navigation data (signals) in CNE can be disrupted, which causes errors in coordinate and consumer movement speed definition (e.g. land, maritime and air transport).

Potential integrity and availability violations of received digital navigation signals are due to random manifestations of unintentional or intentional defects in the special software in the process of GLONASS CNE operation under the following adverse interference conditions:

- man-made interference,
- distorted navigation signals (data) from pseudo-satellites (e.g. transmitted by unmanned aerial vehicles [2]),
- distorted navigation signals rereflected from urban structures or distorted due to signal reception on the Earth's surface with challenging terrain (presence of multipath effect, e.g. in mountainous areas).

The manifestations of such defects in complex interference conditions are essentially information technology interference (ITI) against digital navigation data (frames) that are received and processed by the CNE hardware and software.

The set of undesirable events and states of reception and processing of navigation data with possible distortions will be understood as adverse conditions of processes of navigation data (signals) provision to consumers. This article does not consider the disruptions of navigation data caused by conventional errors of CNE positioning.

In practice, the mentioned adverse conditions cause not only stability problems, but in some cases blocking of processes and non-fulfilment of functions related to provision of navigation data to consumers and operation of systems that use coordinate and time information.

The objective cause of distortion of navigation data (frames) received by the consumer is the long distance (over 19000 km) between the visible GLONASS constellation and the CNE equipment. The coordinate and time information transmitted by the spacecraft in the navigation frame and the actual measurements on the consumer's side on the Earth's surface differ due to the Doppler effect of radio waves deviation in the course of their propagation.

The function-level fault tolerance of the processes of navigation signals (of CNE facilities) provision to consumers in adverse conditions will be understood as their ability to fulfil their functions and retain the allowed parameter values under information technology interference within a given time period.

In order to measure the function-level fault tolerance of the processes of navigation signals provision to customers, it is required to test the CNE architecture in adverse conditions of operation up to the occurrence of faults (failures), and then, based on the test results, perform the processing of statistical data and calculations.

Thus, the development of a model that would allow quantitatively evaluate the function-level fault tolerance of the processes of navigation signals provision to consumers in adverse conditions of man-made interference, presence of pseudo-satellites and signal rereflections is relevant and of practical interest.

Problem definition

The research is based on the following premises:

- the parameters of navigation signals are the pseudorange and pseudovelocity, as well as almanac data and ephemeris information of the navigation signal digital message [3];
- the quantitative evaluation of function-level fault tolerance of processes of navigation signals provision to customers is based on the probability of no-failure of CNE in adverse conditions;
- function-level fault tolerance of the above processes is ensured by multi-level redundancy (combination of functional, hardware, software and time redundancy) [4];
- the architecture of hardware and software facilities of CNE fault tolerance is seen as a three-element hot or cold standby system [5];
- the tolerable level of risk of CNE function-level fault-tolerance violation is defined according to the ALARP principle [4].

GLONASS onboard and CNE equipment are intended for the measurement of two initial navigation parameters, the distance between the satellite and the consumer s and this distance's change rate $\dot{s}$. Assertions about the distance s are made based on the signal propagation time from the satellite to the consumer, while assertions about the value $\dot{s}$ are made based on either the change of the signal s in time, or the Doppler effect [6].

As in the real conditions the satellite's and consumer's clocks are not synchronized, the used method of determining the distance and its change rate introduces errors caused

by independent errors of the satellite's and the consumer's clocks. For that reason the measurement results use the terms "pseudorange" and "pseudovelocity".

Based on the measured parameters s and $\dot{s}$, as well as the satellite coordinates and velocity data from the almanac and ephemeris information, the coordinates and velocity of the consumer can be calculated using Newton's iteration method involving the following mathematical expressions:

$$s_i = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} + \Delta s_i, \quad (1)$$

$$\dot{s}_i = ((x_i - x)(Vx_i - Vx) + (y_i - y)(Vy_i - Vy) + (z_i - z)(Vz_i - Vz)) / s_i + \Delta \dot{s}_i, \quad (2)$$

where x_i, y_i, z_i are the Greenwich orthogonal coordinates of the i^{th} navigation satellite, x, y, z are the Greenwich orthogonal coordinates of the consumer, Vx_i, Vy_i, Vz_i are the velocity vector components of the i^{th} navigation satellite, Vx, Vy, Vz are the velocity vector components of the consumer, Δs_i is the pseudorange measurement error, $\Delta \dot{s}_i$ is the pseudovelocity measurement error.

The processes of navigation signals provision to consumers are primarily implemented by the CNE hardware and software. In the simplest case, the analysis of the fault tolerance of the processes of navigation signals provision to consumers comes down to the CNE fault tolerance analysis.

The standard certificate of vulnerabilities of navigation signal (by the example of pseudorange and pseudovelocity values distortion) that defines the input data for the analysis of CNE fault tolerance is given in Table 1.

The CNE navigation data collection and processing hardware and software are a correlation receiver, of which the precorrelation pathway is coordinated with the useful signal bandwidth. The required CNE function-level fault tolerance in adverse conditions is to be achieved through multi-level redundancy (combination of functional, hardware, software and time redundancy) and the following methods of improving the CNE fault tolerance and jamming resistance:

- use of multisystem navigation receivers,
- navigation signal integrity supervision,
- spatial and frequency-time selection of signal,
- precorrelation processing of signal and interference mixture,
- postcorrelation signal processing,
- processing of radio-frequency parameters of the signal (e.g. signal strength control),
- processing of information parameters of the signal (e.g. code and phase measurements),
- cryptographic authentication,
- integration with external sources of navigation information,
- integration within a single signal processing system of a number of methods of interference countermeasures and pseudo-satellite navigation signals.

The diagram of the model of CNE function-level fault tolerance in adverse conditions is shown in Figure 1.

Figure 1 shows the standard states of the graph model of CNE function-level fault tolerance:

Table 1. Standard certificate of vulnerabilities of navigation signal (by the example of pseudorange and pseudovelocity values distortion)

Vulnerability description elements	Vulnerability description
1. Name of vulnerability	CNE vulnerability
2. Vulnerability identifier	NAP-2017-00003
3. Brief description of vulnerability	Vulnerability allows distortion of pseudorange and pseudovelocity
4. Vulnerability class	Software vulnerability
5. Name of vulnerable element	CNE computer module
6. Data communication protocol	Standard accuracy navigation radio signal
7. Type of defect	Stadiometric code defects
8. Location of occurrence (manifestation) of vulnerability	Vulnerability exists due to periodicity of pseudorandom stadiometric code
9. Date of vulnerability detection	10.02.2017
10. Author of information on detected vulnerability	Information security unit
11. Method (rule) of vulnerability detection	Execution of step-by-step instructions
12. Vulnerability hazard criteria	Exceeding of set values of accuracy characteristics
13. Hazard level of vulnerability	High
14. Possible vulnerability elimination measures	Introduction of functional, hardware, software and time redundancy in the CNE equipment

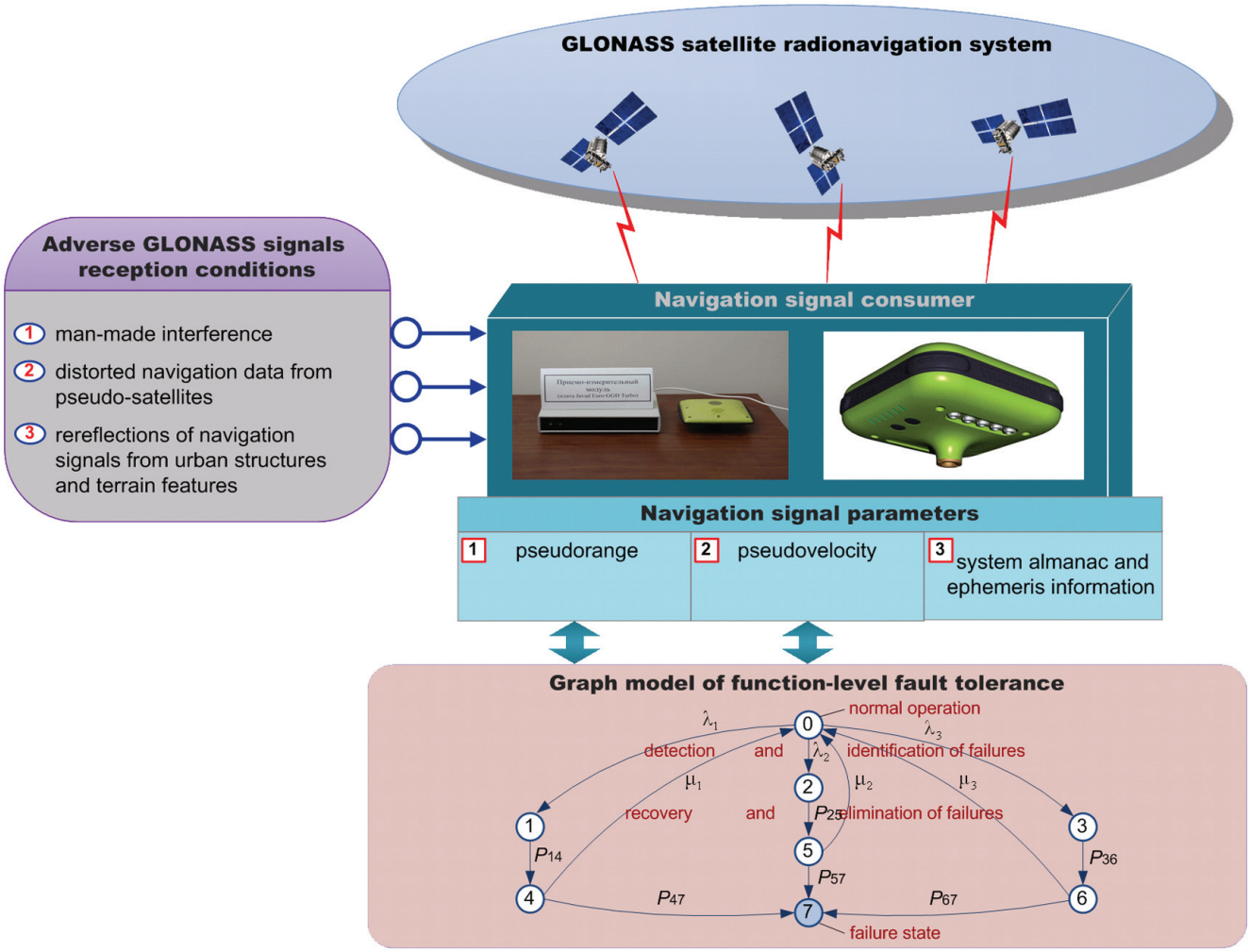

Figure 1. Diagram of the model of CNE function-level fault tolerance in adverse conditions

0 – CNE modules operate in the normal mode with no failures;

1 – failure (fault) of CNE due to man-made interference with the rate of λ_1;

2 – failure (fault) of CNE due to distorted navigation signals (data) from pseudo-satellites with the rate of λ_2;

3 – failure (fault) of CNE due to distorted navigation signals rereflected from urban structures or terrain features with the rate of λ_3;

4 – recovery and elimination of CNE failure (fault) by the man-made interference countermeasures module with the probability of p_{14};

5 – recovery and elimination of CNE failure (fault) by the pseudo-satellite navigation signals (data) countermeasures module with the probability of p_{25};

6 – recovery and elimination of CNE failure (fault) by the rereflected navigation signals (data) from urban structures and terrain features countermeasures module with the probability of p_{36};

7 – hazardous CNE failure due to non-operation of one of the above recovery and failure elimination modules (states 4 – 5) with the respective probabilities of p_{47}, p_{57} and p_{67}.

Expected mathematic correlations of CNE function-level fault tolerance model.

Let us consider the above model of CNE function-level fault tolerance as two variants of dynamic dependability models [5], in which the values of probability of no-failure are time-dependent:

First variant, a hot standby system that includes three additional countermeasure modules.

Second variant, a cold standby system with a switch to three additional countermeasures modules.

Both variants allow for cases when each of the countermeasures modules has an exponential failure law of CNE.

First variant. We interpret the model of CNE function-level fault-tolerance with the hot standby system with three additional countermeasures modules (relative to the general use CNE) that ensure equipment operability in the adverse conditions under investigation. In such hot standby system the three additional countermeasures modules are initially on, while system is able to operate even with a single module (in this case it is assumed the adverse conditions do not correlate with each other).

Then, assuming that there is no ITI in navigation signals, let us write the probability of no-failure of CNE (hot standby)

in adverse conditions for three additional countermeasures modules using [5] as:

$$P_{CNE}^{HSB}(t) = e^{-t\lambda 1} + e^{-t\lambda 2} + e^{-t\lambda 3} - e^{-t(\lambda 1+\lambda 2)} - \\ -e^{-t(\lambda 1+\lambda 3)} - e^{-t(\lambda 2+\lambda 3)} + e^{-t(\lambda 1+\lambda 2+\lambda 3)}, \quad (3)$$

where t is the time to failure of one of the CNE countermeasures modules.

Figure 2 shows the probability of no-failure of CNE (hot standby) in adverse conditions for three additional countermeasures modules under the following initial conditions: $\lambda_1 = 1{,}0\cdot10^{-8}$, $\lambda_2 = 1{,}0\cdot10^{-10}$, $\lambda_3 = 1{,}0\cdot10^{-6}$.

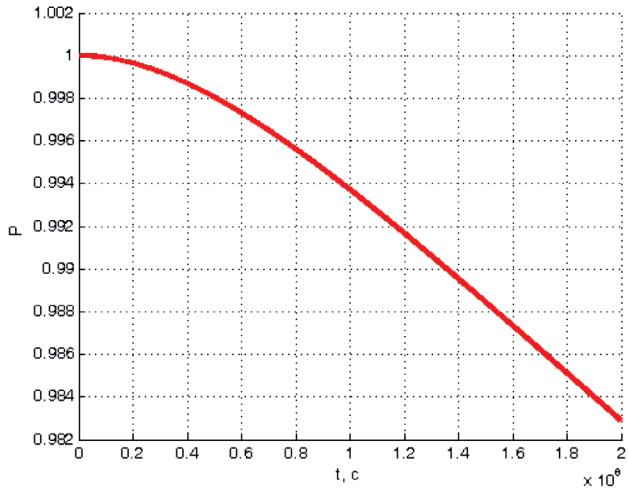

Figure 2. Probability of no-failure of CNE (hot standby) in adverse conditions for three additional countermeasures modules

Second variant. The model of CNE function-level fault-tolerance has the form of a cold standby system with three additional countermeasures modules (relative to the general use CNE). In such systems, at any time only one module is on and ensuring countermeasures against adverse conditions. If one of the modules fails under ITI, the next countermeasures module becomes active.

Assuming that for each countermeasures module the failure rate is constant and equals to λ, let us write the probability of no-failure of CNE (cold standby) in adverse conditions for three additional countermeasures modules using [5] as:

$$P_{CNE}^{CSB}(t) = e^{-t\lambda}\left(1+\frac{\lambda}{\lambda_{\Pi}}(1-e^{-t\lambda})\right)+ \\ +e^{-t\lambda}\left(\frac{\lambda}{\lambda_{\Pi}}\right)^2(1-e^{-t\lambda_{\Pi}}-\lambda_{\Pi}te^{-t\lambda_{\Pi}}), \quad (4)$$

where λ_{Π} is the failure rate of the CNE switch (set of hardware and software) that activates the countermeasures modules depending on the presence of adverse conditions.

Figure 3 shows the probability of no-failure of CNE (cold standby) in adverse conditions for three additional countermeasures modules under the following initial conditions: $\lambda = 1{,}0\cdot10^{-8}$, $\lambda_{\Pi 1} = 1{,}0\cdot10^{-7}$, $\lambda_{\Pi 2} = 1{,}0\cdot10^{-8}$, $\lambda_{\Pi 3} = 1{,}0\cdot10^{-2}$.

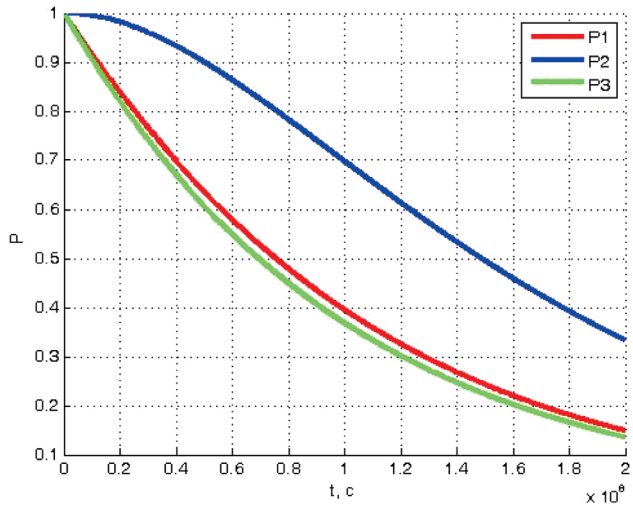

Figure 3. Probability of no-failure of CNE (cold standby) in adverse conditions for three additional countermeasures modules

In the simplest case, using [5], let us define the probability of CNE recovery in adverse conditions, assuming that the repair rate is constant and equals to μ, has an exponential distribution, as follows:

$$P_{CNE}^{REC}(t_R) = 1 - e^{-t_R\mu}, \quad (5)$$

where t_R is the CNE recovery time.

For the quantitative evaluation of the interdependent CNE failure and recovery processes in adverse conditions it is suggested to use the CNE availability coefficient that is defined as the probability of CNE performing the functions defined for the consumer and according to the specified parameters at a given moment in time and in adverse conditions. The following formula can be conveniently used for calculation of the CNE availability coefficient in adverse conditions:

$$P_{ACNE}(t_{NO}) = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda}e^{-(\mu+\lambda)t_{NO}}, \quad (6)$$

where t_{NO} is the CNE non-operability time.

Diagram and formula for evaluation of allowable risk of CNE function-level fault tolerance.

For the expert analytical evaluation of the CNE function-level fault tolerance in adverse conditions let us define the allowable risk level of its violation according to the ALARP principle [4], i.e. risk "as low as reasonably practicable", with the use of the diagram in Figure 4 and Table 2.

The ALARP area of violation of CNE function-level fault tolerance in adverse conditions corresponds to the navigation signals parameter values that are within their tolerances. The allowable value of risk of CNE function-level fault tolerance violation according to the ALARP principle (the upper part of the ALARP region) is only ensured if the navigation signal parameters are within the specified tolerances.

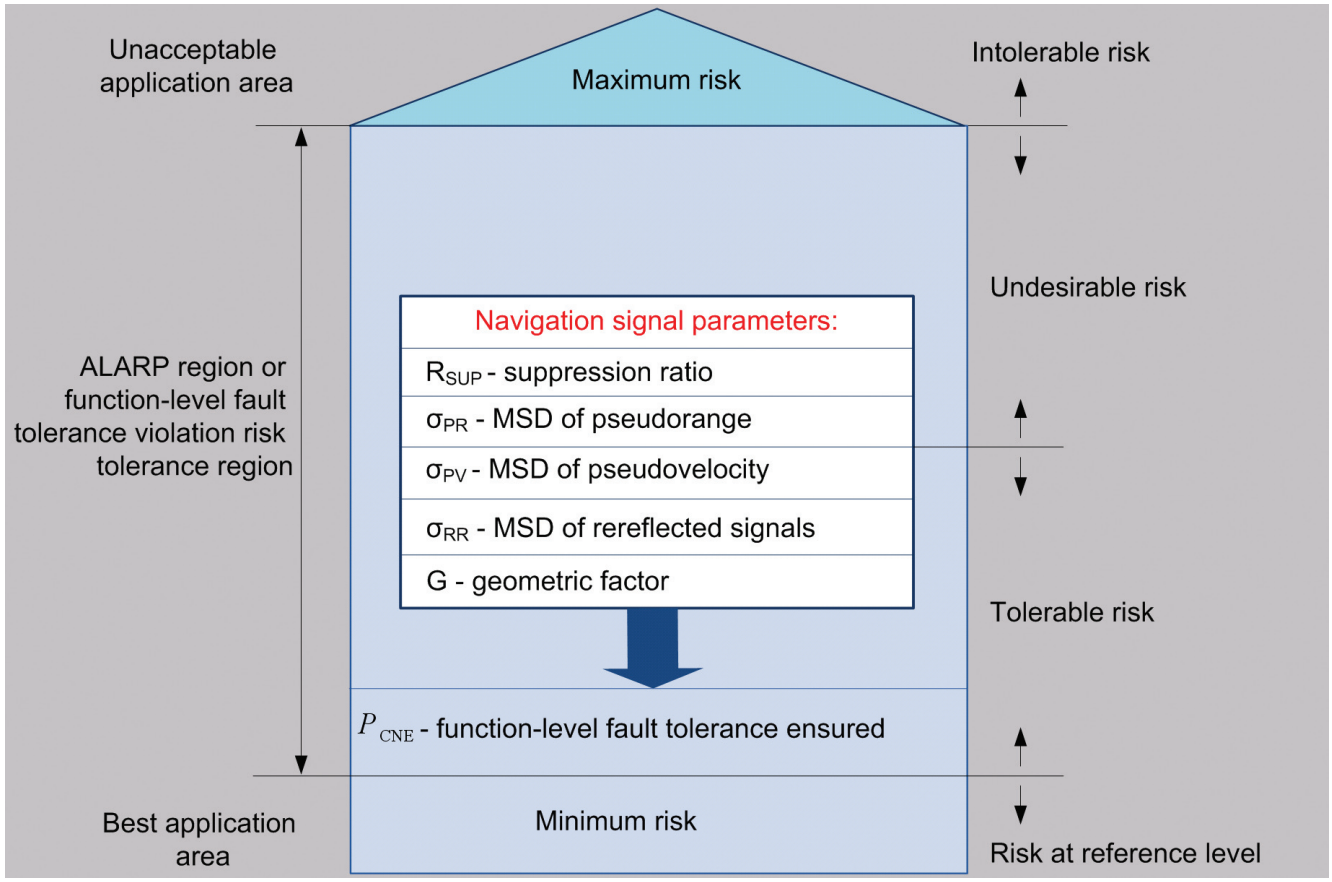

Figure 4. Diagram of allowable risk of CNE function-level fault tolerance level violation according to the ALARP principle

It is proposed to identify the risk of navigation signal parameter distortion in generic CNE hardware and software by means of monitoring the following parameter values:

- power of man-made interference, suppression ration not more than 30 dB,
- pseudorange of navigation signals, mean square deviation (MSD) of the pseudorange must not exceed 5 meters,
- navigation signal pseudovelocity, MSD must not exceed 0.01 m/s,
- multipath effect (navigation signal reflection from urban structures and terrain features), MSD of positioning not more than 10 meters, geometric factor not worse that 15 (minimization of the navigation signal rereflections accepted for processing).

According to Table 2, the CNE failure frequency (10^{-8} 1/h) and low risk level will correspond with the allowable value of the probability of no-failure $P_{CNE} \geq 0.8$ and minimal value of the harm of non-provision of quality navigation services to the consumer.

We deduce the value of allowable risk of CNE function-level fault tolerance level violation using the following formula:

$$R_{ALW} = \sum_{i=1}^{n} ((1 - P_{CNE,i})\gamma_j), \quad (7)$$

where $P_{CNE,i}$ is the probability of no-failure of CNE with the i^{th} CNE ITI countermeasures module, γ_j is the value of harm of the j^{th} level.

Conclusion

The article proposes a model that allows representing the processes of navigation signal provision to consumers in the form of a conventional state graph. The model includes mathematical expressions for quantitative evaluation of the probability of no-failure for hot and cold standby systems with three modules of information technology interference countermeasures, probability of recovery identification and

Table 2. Evaluation of allowable risk of CNE function-level fault-tolerance violation

Risk level	Frequency of failures	Evaluation of function-level fault tolerance level	Value of damage caused by CNE failure (points)
Low	10^{-8} 1/h	Tolerable $P_{CNE} \geq 0,8$	γ_L=1÷2
Medium	10^{-5} 1/h	Acceptable $0,6 \leq P_{CNE} \leq 0,7$	γ_M=3÷4
High	10^{-3} 1/h	Intolerable $0,5 \leq P_{CNE} \leq 0,6$	γ_H=5÷10

CNE availability coefficient, as well as the allowable risk of CNE fault tolerance violation.

References

1. Federal Target Program Support, Development and Use of GLONASS for the period between 2012 and 2020, <http://www.gost.ru>.

2. Boeing and QinetiQ working on a highly autonomous military UAV: the high-altitude drone is to operate without landing not less than five years with a 500-kg (1000 lbs) payload, <http://www.roscosmos.ru>.

3. Yatsenkov VS. Osnoivy sputnikovoy navigatsii. Sistemy GPS NAVSTAR i GLONASS [Introduction to satellite navigation. GPS NAVSTAR and GLONASS systems]. Moscow: Goriachaia linia-Telekom; 2005 [in Russian].

4. Shubinsky IB. Nadiozhnie otkazoustoychivie informatsionnie systemi. Metodi sinteza [Dependable failsafe information systems. Synthesis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2016 [in Russian].

5. Kapur K, Lamberson L. Reliability in engineering design. Moscow: Mir; 1980.

6. Babich OA. Obrabotka informatsii v navigatsionnykh kompleksakh [Information processing in navigation systems]. Moscow: Mashinostroenie; 1991 [in Russian].

About the authors

Sergey M. Klimov, Doctor of Engineering, Professor, Head of Division, 4th Central Research and Design Institute of the Ministry of Defense of Russia. 12 B. Komitetskaya Str., app. 105, 141092, Moscow Oblast, Korolyov, mkr. Yubileyny, Russia, phone: +7 (985) 928 13 55, e-mail: klimov.serg2012@yandex.ru

Aleksey Yu. Polovnikov, Candidate of Engineering, Associate Professor, Chief Researcher of Division , 4th Central Research and Design Institute of the Ministry of Defense of Russia. 9/18 Mayakovskogo Str., app. 70, 141090, Russia, Moscow Oblast, Korolyov, mkr. Yubileyny, phone: +7 (985) 119 24 65, e-mail: plv71@yandex.ru

Aleksey P. Sergeev, Senior Researcher, 4th Central Research and Design Institute of the Ministry of Defence of Russia. 27 Lenina Str., app. 159, 141070, Russia, Moscow Oblast, Korolyov, phone: +7 (926) 493 51 16, e-mail: lex_serg@mail.ru

Received on 28.03.2017