Methods of formalized quality assessment of intelligent transport systems

K Goloskokov¹, V Korotkov¹, V Gaskarov¹ and T Knysh¹

¹ Admiral Makarov State University of Maritime and Inland Shipping, 5/7, Dvinskaya St., St. Petersburg, 190031, Russia

E-mail: goloskokovkp@gumrf.ru

Abstract. The purpose of the paper is to identify the main problems of creating software systems with a given level of reliability for intelligent transport systems. Considering the importance of this approach and the gained experience, the paper discusses design solutions to ensure software reliability in the development process. The paper is based on domestic and foreign experience of software design for intelligent information systems, which include transport systems. The issues of achieving a given level of software reliability during the control process are considered taking into account the continuation of the development process. It also reflects efforts to model and evaluate the reliability of software systems by considering the most common types of software reliability assessment models during development, as well as to predict the reliability during maintenance. The emphasis is upon detecting and correcting software errors.

1. Introduction

It is necessary to know all sections of automated transport systems where errors may occur, as well as be able to distinguish the main ones among them. Processing must be designed to automatically detect any significant error that may occur in the system.

Error correction and detection is one of the main functions of the automated system.

2. Materials and Methods

Error detection methods. In information systems, which also include intelligent transport systems, errors are usually detected at three levels:

• at the system level, i.e. its appropriate operation;
• at the software level, i.e. development of programs or blocks thereof specifically designed to detect and correct errors;
• device level, i.e. when designing the corresponding device.

• Error detection at the system level. This is the main method of data check. It is formed when organizing the system and represents a set of measures that detect errors at all stages of system operation (from data collection to sending results).

• Error detection at the software level. This method is embedded in the development of intelligent system software. It is used when system methods do not provide the required level of confidence.

• At the software level, the following methods of information control are most common.

1. Change limits check. To do this, a standard checker [1–3] and a case-specific table of limit values of different attributes are used. For each attribute the program determines whether its value is
within the specified limits. If this condition is violated, the corresponding value of the attribute is marked with a symbol.

2. Consistency check. Specially designed programs check the fairness of conditions specific to the considered attributes. The detected deviations are analyzed in the described manner.

3. Symbol check. For this purpose, the description of each attribute specifies the class of symbols used to indicate it. The correctness of symbols is checked by standard mathematical software.

4. Totals control. All information arrays must have checksums. Specially designed routines that are part of separate procedures should, on the one hand, calculate checksum values in newly obtained arrays, and on the other hand, calculate the same values from the checksums of arrays used in processing. The results are then compared and the desired messages are issued in the event of a mismatch.

5. Data control. In order to monitor the data, the input documents must have totals lines obtained from a particular structure. The data is controlled in the same way as the totals. Characteristic attributes are controlled by retrieving the corresponding attributes in reference arrays or by means of module $R$. Data is controlled by special programs performed before the rest of information processing [4–8].

Error detection at the device level. Some errors such as computer system device failures, information loss, etc. are detected at the device level. Software and hardware methods are used for this.

Software methods are used to recognize errors with the help of the internal mathematical software of the device. The methods used here are the same as for error detection at the software level. Equipment duplication is often used to detect errors.

*Error correction methods.*

Error correction includes:

- data protection against destruction or damage;
- protection against loss of calculation results in case of failure of external devices, arithmetic devices or control devices;
- corrected data entry.

*Data protection against destruction and damage.* Typically, a destroyed array may be restored from previous versions. For each array, the number of historical data may be quite large. This type of protection is called the grandfather/father/son system.

Another way to protect data is to make copies of arrays (duplicates) used in case of their destruction. This method is typical for disks where it is extremely difficult to store the history of the array being updated. The contents of the disk are copied before each update. In other cases, the array of information recorded on the disc is copied at certain intervals. The changes made between copy times are saved and used when the array is restored.

Protection against loss of result is performed with the help of checkpoints and is applied for programs, the implementation of which requires a lot of machine time. As an example, let us consider the case when a problem occurred after a long work of the machine. If the system does not provide for special measures, then the entire calculation begins first. Therefore, the program provides for the so-called checkpoints. When the program reaches the checkpoint, the results obtained and all data to continue the program (memory area assigned to the program, contents of all registers, program control parameters) are automatically output to external media. After fixing the problem in the machine, the program continues the solution with the nearest checkpoint passed at that time.

There are three ways of organizing checkpoints:

- alignment along the input, i.e. formation of a mark at the beginning of the new input array or its part;
- alignment along the output, i.e. formation of a mark at the end of the output array or its part;
- time alignment when checkpoints are organized at certain time intervals.

*Evaluation of output accuracy.* The selected information protection system should be justified based on the following indicators:
• amount of machine time that will be wasted if there is no control procedure;
• values of losses due to error in input data under the proposed control system and without it;
• cost of developing and operating the error detection and correction system.

The error detection and correction process increases the cost of the data processing system by an average of 30%. Therefore, special attention should be paid to the correct selection of the information protection system [9–12].

3. Results
The task of selecting a rational information protection system is as follows: from the known set of options to increase the reliability of the output information we need to choose such a subset (security system) of it that would provide the minimum total losses on the one hand due to the costs of creating a security system, and on the other – losses in the information system caused by low reliability of the output information.

The intensity of error detection in the program \( \frac{dn}{d\tau} \) and the absolute number of eliminated errors are associated with the equation

\[
\frac{dn}{d\tau} + kn = kN_0;
\]

where \( k \) – coefficient.

Assuming that there are no errors detected at the beginning of debugging at \( \tau = 0 \), the solution to the equation is as follows:

\[
n = N_0 \left[ 1 - \exp(-k\tau) \right]
\]

The number of remaining errors in the program package \( n_0 = N_0 - n = N_0 \exp(-k\tau) \) is proportional to the detection intensity \( \frac{dn}{d\tau} \) to the accuracy of the coefficient \( k \).

Time to system failure \( T \) or time between failures, which is considered as the detectable distortion of programs, data or computational process, which disrupts serviceability, is equal to the value of inverse intensity of failures (errors) detection [13–16]:

\[
T = \frac{1}{\frac{dn}{d\tau}} = \frac{1}{kN_0} \exp(k\tau)
\]

If consider that before the start of testing, the set of programs contained \( N_0 \) errors and the time between failures \( T_0 \) corresponded to this, then the function of the time between failures dependent on the duration of checks may be presented as follows:

\[
T = T_0 \exp \left( \frac{\tau}{N_0 T_0} \right);
\]

If the moments of error detection \( t_i \) are known and one error is detected and reliably eliminated each time, then using the maximum likelihood method [17–21], an equation may be obtained to determine the value of the initial number of errors \( N_0 \):

\[
\frac{1}{n} \sum_{i=1}^{n} \frac{1}{N_0 - (i-1)} = \frac{n}{N_0 \sum_{i=1}^{n} t_i - \sum_{i=1}^{n} (i-1) t_i},
\]

as well as the expression for calculating the proportionality factor

\[
K = \frac{n}{N_0 \sum_{i=1}^{n} t_i - \sum_{i=1}^{n} (i-1) t_i}.
\]
As a result, it is possible to calculate the number of errors remaining in the program and the average time between failures $T_{cp} = 1/\lambda$, i.e. to obtain an estimate of time until the next error is detected.

In the process of debugging and testing programs, in order to increase the time between failures from $T_1$ to $T_2$, it is necessary to detect and eliminate $\Delta n$ errors. The value $\Delta n$ is determined by the ratio:

$$\Delta n = N_i T_0 \left[ \frac{1}{T_1} - \frac{1}{T_2} \right];$$

The expression for determining the time $\Delta \tau$ spent on debugging, which allows eliminating $\Delta n$ errors and accordingly increasing the time between failures from $T_1$ to $T_2$, is as follows:

$$\Delta \tau = \frac{N_i T_0}{K} \ln \left( \frac{T_2}{T_1} \right);$$

4. Conclusion

The information error protection system consists of a number of sections or operations used in data processing for timely detection and correction of errors in an intelligent transport system. These sections and operations are redundant, such since they are not directly due to the tasks solved in processing the information of the considered intelligent system. The obtained results allow developing the algorithm to select the system of information protection against errors in transport intelligent systems.

References

[1] Sokolov S S, Glebov N B, Nyrkov A P and Boriev Z V 2018 Formation of common legal framework for biometric data security based on contradictions in international legislation *IOP Conference Series: Earth and Environmental Science* 194(2)2

[2] Reshnyak V, Sokolov S, Nyrkov A and Budnik V 2018 Inland Waterway Environmental Safety *Journal of Physics: Conference Series* 1015(4)2

[3] Boriev Z, Sokolov S, Nyrkov A and Nekrasova A 2016 Mathematical and information maintenance of biometric systems *IOP Conference Series: Materials Science and Engineering* 124(1)2

[4] Nekrasova A, Boriev Z, Nyrkov A and Sokolov S 2016 Modeling and optimization of transmission and processing of data in an information computer network *IOP Conference Series: Materials Science and Engineering* 124(1)2

[5] Mamunts D, Sokolov S, Nyrkov A and Storchak T V 2016 The effect of dredger positioning accuracy on the environment. *Proceedings of the 2016 IEEE North West Russia Section Young Researchers in Electrical and Electronic Engineering Conference, EIConRusNW* pp 435–437

[6] Sokolov S S, Alimov O M, Golubeva M G, Burlov V G and Vikhrov N M. 2018 The automatting process of information security management *Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus* pp 124–127

[7] Reshnyak V I, Sokolov S S, Chernyi S G, Storchak T V and Tihomirov Y N 2017 System aspect course of creation of information and analytical system of environmental monitoring and control *IOP Conference Series: Earth and Environmental Science* 87(4)3

[8] Zhukov V, Gavrilov V, Sokolov S, Zhelezniak A and Bordiu A 2017 Control system of gas and dual fuel engines of generating units by way of accuracy increasing of load allocation *Proceedings of the 2017 IEEE Russia Section Young Researchers in Electrical and Electronic Engineering Conference, EIConRus* pp 1112–1115

[9] Kovalnogova N M, Sokolov S S, Chernyi S G, Shnurenko A V and Burlov V G 2016 Applying of E-learning and Distance learning technologies in electronic informational-educational
environment in modern university complex Proceedings of the 19th International Conference on Soft Computing and Measurements, SCM pp 446–448

[10] Nyrkov A, Sokolov S, Chernyi S, Chernyakov A and Karpina A 2016 Providing the integrity and availability in the process of data transfer in the electronic documents management systems of transport-logistical clusters 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM – Proceedings (Chelyabinsk)

[11] Mamunts D G, Sokolov S S and Nyrkov A P 2015 Using information technologies in dredging IOP Conference Series: Materials Science and Engineering 91(1)

[12] Zhukov V A, Sherban S A, Melnik O V, Sokolov S S and Kolesnichenko S V 2019 Improvement of methods and means of thermal control of ship power plants Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus pp 389–392

[13] Sokolov S, Glebov N, Novoselov R and Chernyi S 2018 Database problems of maritime transport industry on high load platform MATEC Web of Conferences 239

[14] Nyrkov A, Shurenko A, Sokolov S, Chernyi S and Korotkov V The effective optimization methods of port activity on the basis of algorithmic model International Journal of Electrical and Computer Engineering 7(6) 3578–3582

[15] Avdeyev B, Masyutkin E, Golikov S, Sokolov S and Gavrilov V 2017 Calculation of efficiency curve of magnetic hydrocyclone Proceedings of the 2017 IEEE Russia Section Young Researchers in Electrical and Electronic Engineering, ElConRus pp 1225–1228

[16] Zhilenkov A, Nyrkov A, Chernyi S and Sokolov S Simulation of in-sensor processes in the sensor – Object system type when scanning the elements of underwater communication lines with a probe beam International Review on Modelling and Simulations 10(5) 363–370

[17] Bukharmetov M, Nyrkov A, Sokolov S, Chernyi S, Kuznetsov V and Mamunts D 2017 Robust Method for Protecting Electronic Document on Waterway Transport with Steganographic Means by Embedding Digital Watermarks into Images 2017 Procedia Engineering 178 507–514

[18] Koroleva E, Sokolov S, Makashina I and Filatova E 2019 Information technologies as a way of port activity optimization in conditions of digital economy E3S Web of Conferences 138

[19] Koroleva E, Makashina I, Filatova E and Sokolov S Structural components of space as a component of logistic MATEC Web of Conferences

[20] Koroleva E A, Sokolov S S, Makashina I I and Filatova E V 2018 Freight Forwarding Space as a Component of Transport and Logistic Proceedings of the 2018 International Conference ‘Quality Management, Transport and Information Security, Information Technologies’, IT and QM and IS pp 112–116

[21] Goloskokov K, Korotkov V, Vasin A and Knysh T 2020 Features of Assessing the Quality of Functioning of Telecommunication Systems in Transport Proceedings of the XIII International Scientific Conference on Architecture and Construction, Lecture Notes in Civil Engineering Vol 130 (Singapore: Springer) Retrieved from: https://doi.org/10.1007/978-981-33-6208-6_10