SAFETY OF INFORMATION-MANAGEMENT SYSTEMS IN RAILWAY TRANSPORT

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

Prof., Dr. Technical Science Moiseenko V. I., Postgraduate. Kotov M. O.
Ukraine State University of Railway Transport – Kharkov, Ukraine
E-mail: mvi53@ukr.net, kotov.mykyta@gmail.com

Absract: *in the article is considered questions of the organization structure of the software of information-management systems in railway transport. A new approach based on matching software structure with functions and their level criticality by safety. Received results allow to implement the synthesis of structures of systems with regard to their purpose and the functions they perform.*
KEYWORDS: SYSTEMS STRUCTURE, SAFETY, SOFTWARE AND HARDWARE.

1. Introduction

Railway transport is one the most intensively developing sectors in the global economy. Modern train control systems is a difficult complex software and hardware. Besides the usual technological tasks assigned to them a very important function - providing traffic safety and continuity the transportation process. Most of the functions of information-management systems implemented at the software level. In connection with this question of improving the software of these systems are timely and relevant.

Problems of safety and reliability of the application software of railway automation has traditionally been considered from the standpoint of classical reliability theory, as evidenced by the work [1-3]. Usually authors in the process of synthesis of software and hardware structure not take into account the specifics of the technology of functioning of the control object. Often enough the software structure is tied to the structure of the hardware. Some few authors, try to link the structure of software and hardware complex with the singularity technology work of the control object, as that can be a railway station.

This work is a logical continuation of this direction. The objective is to formulate the basic principles of synthesis of software and hardware systems considering the specifics of the functions information and control system.

If we consider from this positions functions automated train control system on the station, in accordance with [4], it is possible to allocate:

-responsible functions, implementation of which ensures the functioning of the control system and its safety factor;

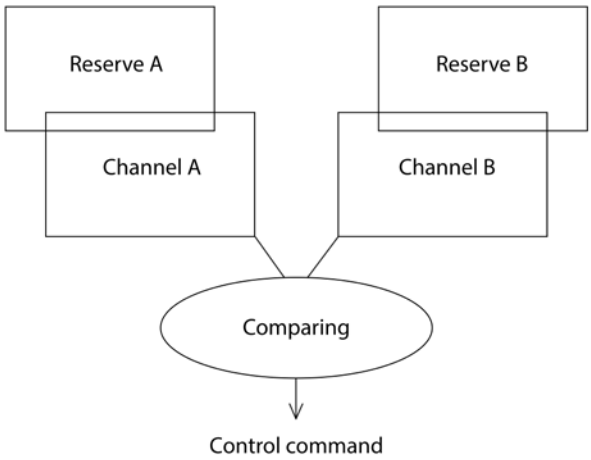
-functions related to ensuring of the system which are not critical to safety;

-service functions.

Regulatory documents of the EU and Ukraine (IEC 61508) sets different levels of risk dangerous events, as well as qualitative and quantitative indicators of the safety of functioning management systems.

2. Preconditions and means for resolving the problem

With this in mind, let us consider options for organization of software structure with classical two-channel reserve of station microprocessor control system, pic.1.

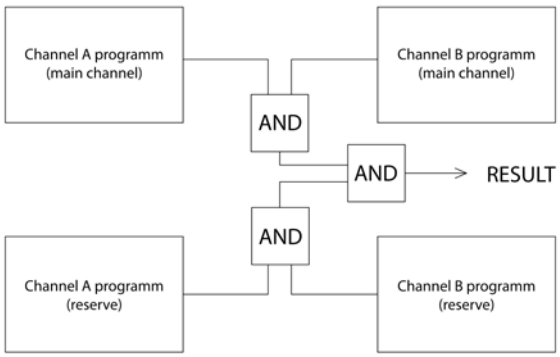


Pic.1. Block diagram of a hardware-software complex of the station information management system.

According to the scheme in picture 1, channels interact in scheme logical "AND", and reservation in each channel is carried on scheme "OR". Obviously, all the functions of control and management will be implemented by this logic.

After this we transform the scheme on picture 1, keeping in mind all the responsible functions, which are most critical to safety. In a case of failure, the system must go into the condition, so-called "the deffencive condition", wherein it's functioning is limited.

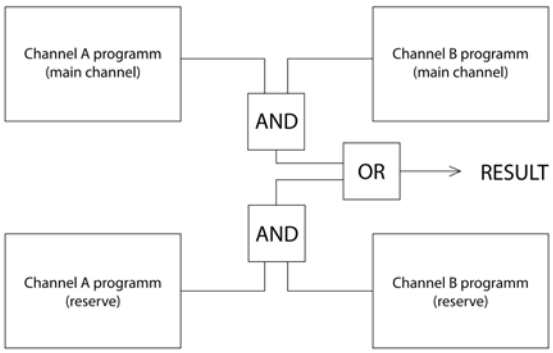
Basing on this limits, we have no need in reservation. And the main task consists find and to block mistake. For a software implementation of such functions, mostly fits the logical structure "AND"—"AND", pic.2.



Pic.2 The structural scheme of realisation of responsible functions.

The output signal can be created only with full identical work of A and B programms of both channels. A priori, such a structure loses in reliability, but can have good safety parameters. With the help of this structure, can be realized functions of object blocking, artificial opening, enabling of invitating light etc.

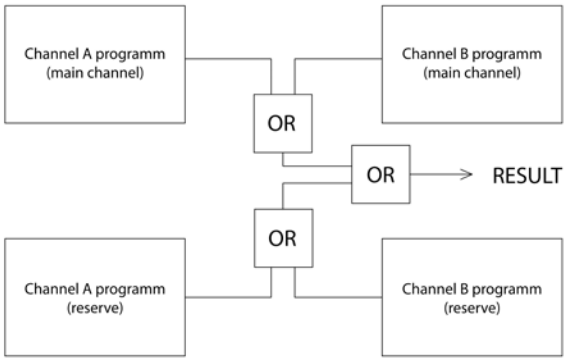
The structurally-logic scheme "AND"—"OR" can be used for realisation of functions, which are not so critial to safety, pic.3.



Pic.3 The structural scheme of realisation of management functions, which are not crirical to safety.

Such a structure is designed for the realisation of the main system commands, which are linked with the setting of the route, and also with locking and automatic unlocking. At the expense of the balance between the indicators of safety and reliability, it can provide an effective work of the hardware and software complex under the influence of destabilizing factors.

Failure operation serves as a main indicator of success for the service functions of information-management systems. According to this requirement, it's logical to suggest usage of operation "OR", pic.4.



Pic.4 The structural scheme of realisation service functions.

In this approach, some ambiguity is not excluded if one of the programs will crash. But it doesn't matter in two reasons. The first one, is that information is provided to the human operator. And the second one. It's not critical to the railway traffic safety.

3. The solution of the considered problem

The successfull work or the crashing of the system can be described with help of the combination of final events, which are united into the composite tree of all dangerous conditions of system. We can determine the parameters of probability for the all system for their further comparing.

The simultaneously pairwise coincidence of refusal in main and reserve channels A, A', B and B' of system software are the criterion of refusal at performing control functions for the scheme on picture 2. Let's mark by Ψ the parametre of condition of system which characterizing refusal, . then for the scheme in pic.2, it can be represented by a function of the form:

$$\Psi 1 = (A \,\&\, B) \,\&\, (A' \,\&\, B'). \quad (1)$$

In the same way for the structure, which is not so critical for safety on pic.3. :

$$\Psi 2 = (A \,\&\, B) \,\|\, (A' \,\&\, B'). \quad (2)$$

The structural function of refusal for service functions has a form of classical scheme "OR"

$$\Psi 3 = (A \,\|\, B) \,\|\, (A' \,\|\, B'). \quad (3)$$

According to this logic, the conditions of element or the whole system determine by auxiliary binary variable parametere of function of probability refusal component Yi [5]. Obviously, event occurs if Yi = 1, and conversely, doesn't occur, if Yi = 0. Accordingly, similarly for the systems of realization in general Z1, Z2, Z3.

A publication analysis [6-9] makes it possible to formulate a hypothesis about the independence of primary events, and to suggest the presence of exponential law distribution.The latter hypothesis is supported by the majority of researchers, working in this field [10-13]. A list of the main indicators of reliability and safety is set by normative documents, particularly in the evaluation of software according to ISO/IEC 9126, ISO/IEC 12207, GOST 28195-89. The issues of provision computational formulas required statistical data reflecting the reliably behavior of the system and with sufficient sample objects, is the main problem, faced by researchers.

We're going to use a maximum value for $Zo=9*10^{-9}$ 1/hour in flollowing discussions.

4. Results and Discussion

Taking into account the above the functions of probability of failure , for each of the proposed structures:

$$Z1 = Y1*Y2*Y3*Y4; \quad (4)$$

$$Z2 = 1-[1-Y1*Y2][1-Y3*Y4] = Y3*Y4+Y1*Y2-Y1*Y2*Y3*Y4; \quad (5)$$

$$Z3 = 1-[1-Y1][1-Y2][1-Y3][1-Y4] = Y4+Y3-Y3*Y4+Y2-Y2*Y4- - Y2*Y3+Y2*Y3*Y4+Y1-Y1*Y4-Y1*Y3+Y1*Y3*Y4-Y1*Y2+ +Y1*Y2*Y4+Y1*Y2*Y3-Y1*Y2*Y3*Y4. \quad (6)$$

where are Y1,Y2,Y3,Y4 – parameters characterizing of refusal component of the system A, B, A ', B', respectively.

Based on the fact that control system an arbitrary time t implements only a single function, and in the range [t; t+Δt] system may implement a row of basic functions. Then the function of refusal of the whole system is written like:

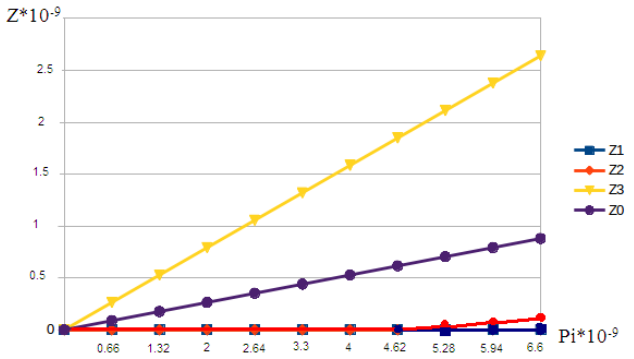
$$Zo = Z1 \,\|\, Z2 \,\|\, Z3. \quad (7)$$

We assume that the intensity of refusal of programs A, A', B and B' are the same, $\lambda 1 = \lambda 2 = \lambda 3 = \lambda 4$. This assumption may have a right to exist in connection with the setting task of comparison potential capabilities of different structures of the organization of the software.

To simplify further change of the last expression, considering previously adopted assumptions about the equality of the intensities of refusals components A,B,A',B', we make the change of variables Y1=Y2=Y3=Y4=X . Then in the final form the function of refusal of system can be represented by the equation:

$$Zo = 4X-4X^2-4X^3+11X^4-8X^5+8X^7-11X^8+4X^9+4X^{10}-4X^{11}+X^{12} \quad (8)$$

Figure 5 shows the probability of refusal Zo, Z1, Z2, Z3 from the refusal of individual component Pi.



Pic.5 The structural scheme of realisation of safety functions

Exterior view of implementation schedules Z1, Z2, Z3, and of whole system Zo confirms the prospects of the proposed approach.

5. Conclusion

The considered embodiments structure of hardware and software do not exhaust all the possible implementations. This is most likely just a basic configurations, icombining and extending them will allow to get considerable quantity of different modifications.The choice of a particular type is determined by the requirements for the overall system and for its individual functions.

Also it should be noted that to obtain the expected properties in reliability and safety it is advisable to allocate a hardware implementation of the programs A and B in the main and standby channels. Otherwise, malfunctions and failures on the general reasons may significantly to worse the expectation of developer.

6. Literature

1. РТМ 32 ЦШ 1115482.02-94. Безопасность ЖАТ. Методы расчета показателей безотказности и безопасности СЖАТ [Текст].
2. ГОСТ Р 51901.5-2005. Менеджмент риска. Руководство по применению методов анализа надежности [Текст].
3. Викторова, В. С. Анализ программного обеспечения моделирования надежности и безопасности систем [Текст] / В. С. Викторова, А. С. Степанянц // Надежность. – 2006. – No 4 (19). – С. 46-57.
4. ГОСТ Р 51901.14-2005 (МЭК 61078:1991). Менеджмент риска. Метод структурной схемы надежности [Текст].
5. ДСТУ 4178-2003 Комплексы технических средств систем управления и регулирования движением поездов. Функциональная безопасность и надежность.
6. MIL-HDBK-217F Military handbook. Reliability prediction of electronic equipment.
7. Надежность и эффективность в технике[Текст] : справ. в 10 т. Т. 3. Эффективность технических систем / под общ. ред. В. Ф. Уткина,Ю. В. Крючкова. – М. : Машиностроение, 1988.– 328 с.
8. Джон фон Нейман «Вероятностная логика и синтез надёжных организмов из ненадёжных компонентов».
9. Baun C. Cloud Computing. Web-Based Dynamic IT Services // C. Baun / Springer-Verlag, Berlin. - 2011. - 108 p..
10. René J. Chevance Server Architectures. Multiprocessors, Clusters, Parallel Systems, Web Servers, and Storage Solutions // J. René / Elsevier Digital Press USA. - 2005. - 709 p.
11. EN 50126 Европейский стандарт спецификация и доказательство надежности, эксплуатационной готовности, ремонтопригодности и безопасности (RAMS) для использования на железных дорогах.
12. Косолапов А.А. Исследование тенженций развития архитектуры информационных систем на сортировочных станциях.
13. Надежность технических систем и оценка риска. Автор: *Хенли* Э., *Кумамото* Х