Захист інформації

UDC 004.052

V.S. Kulynych, A.V. Kharybin

Research and Production Corporation Radiy, Kirovograd, Ukraine

FUNCTIONAL SAFETY ANALYSIS PROCEDURE FOR THE DESIGN STAGE OF THE SAFETY-RELATED INSTRUMENTATION AND CONTROL SYSTEMS' PROCESSING NODE ARCHITECTURE VARIANTS

Synthesis, analysis and selection procedure of architectural variants of the processing node as a part of the instrumentation and control system (I&CS) for safety-related applications is presented. Required levels of reliability and functional safety (FS) can be achieved in case of using this procedure at the design stage. I&CS processing node for safety-related applications is considered as an autonomous, unified computing and control node which consist of processing modules with ability to reconfiguration. The FS indexes assessment procedure, which takes into account the criticality degree of I&CS architectural elements and processed functions is specified.

Keywords: *functional safety, instrumentation and control system, architecture, processing node, design stage, criticality index, risk, harm.*

Introduction

Problem definition. It is known that failure of any safety function, which is implemented in and processed by the safety-related instrumentation and control systems, can lead to the acceptable risk overrunning and catastrophic consequences [1]. Therefore, nowadays huge attention is paid to the reliability and functional safety providing of the safety-related I&CS processes. This is presented by the large number of the international standards which define the FS requirements for the safety-related I&CS in different sectors - medicine [2], nuclear power plants [3], process industry sector [4], machinery [5] etc. In any particular application, the required safety support measures usually depend on application specific factors. International standards of the functional safety aspects for electric/ electronic/ programmable electronic safety-related systems specify only general approaches to the assessment of its reliability indexes, risk and functional safety levels.

Analysis of the latest publications. There are many works which are devoted to the assessment and assurance of functional safety or safety in general. For example, author in the article [6] suggested method of the FS index assessment for technical systems which permitted to calculate FS indexes by means of system statement graph. This method based on solving both Markov models and semi Markov models of the reliability and FS and used theoretical basis and definitions which were not comply with corresponding FS standard for I&CS [7]. Also in this work physical meaning of the introduced FS index doesn't comply with definition in standard [7]. The results of the FS assessment method, which is specified in [6], can't be used to provide system stability toward transitions to the dangerous states or to put the system from dangerous state into the safe state.

"Flexible" information-processing architecture is proposed in works [8, 9] for using to construct I&CS for safety-related application to provide FS. As described in these works this I&CS architecture bases on using processing node with ability to self-reconfiguration in case of operation failures or operation malfunction of the "active" unified processing modules (PMs).

Also in [10] author describes the approach to solving this scientific and technical problem related to the organization processing node (PN) in safety-related application (that is on-board processing systems) as well as there are listed the major issues associated with the processing node construction with the possibility of reconfiguration and resources reallocation depending on the PMs operability and PMs loading at runtime functions.

Taking into account modern approaches to computing, which are based on the cloud-computing principles, reconfiguration server functions can be distributed between all operable PMs which are consisted processing node. This specifies stricter requirements to the unified PMs performance and increases the reliability of such system with reconfiguration.

Therefore, there is necessity of the identification functional safety level assessment and assurance procedures of safety-related I&CS.

Taking into consideration described above **the aim of this article** is to describe the approach to the analysis of possible I&CS PN architecture variants

due to rigorous operation quality and FS requirements. It is one of the important tasks in the functional safety providing process at the design stage of the safety-related I&CS.

Initial characteristic set

It is appropriate to consider the procedure of synthesis and selection of the architectural and structural construction variants of I&CS processing node to achieve the required levels of reliability indexes and therefore FS indexes at the design stage. Nowadays I&CSs constructed in such way that each subsystem in its composition has own processing subsystem (PS) that performs safety functions only for this subsystem. This approach of I&CSs construction is traditional and widely used (for example, aircraft I&CSs).

In the article I&CS PN is considered as a set of unified PMs. PM unification means ability of any PM to perform not only assigned safety function for this PM but to perform any other I&CS PN function if it is reassigned for this PM in case of processing node reconfiguration because of operation failure of some other PMs. Unification of processing modules allows to reallocate computing resources within processing node for providing safety functions fulfillment.

Initial characteristic set (SV) to describe the synthesis and selection the most appropriate of architectural and structural construction (AS_{ij}) variants number of I&CS PN is:

$$SV = \left\{AS_{ij}, P_{NF}\right\},$$

where AS_{ij} – construction variants of I&CS PN/PS (i – indicates existing (i = 1) construction variants of I&CS PS or proposed (i = 2) construction variants of I&CS PN, j – parameter indicates the constructing technique of I&CS PN/PS);

P_{NF} – the probability of I&CS PN/PS non-failure operation.

The architectural and structural construction variants (AS_{ij}) of I&CS PN/PS is determined by following set:

$$AS_{ij} = \left\{DD, TR\right\},$$

where DD – basic digital device that is used as a processing device in I&CS PN/PS processing modules (microprocessor (MP) or field programmable gate array (FPGA));

TR – redundancy type (without redundancy (WR), continuous redundancy (CR), sliding redundancy (SR), group sliding redundancy (SR_G)).

Operability in the existing I&CS PS construction variants is provided by no-failure PS elements and by continuous redundancy without reconfiguration in failure case.

Using "flexible" information-processing architecture of I&CS PN is proposed to use in I&CS in addition to the using redundancy to increase level of reliability and functional safety [9].

This architecture contains control, diagnosis and reconfiguration means which are distributed on all unified PMs of I&CS PN.

It is proposed to consider following variants AS_{ij} of I&CS PN/PS:

1. Traditional (existing) I&CS PS construction variants:

– AS_{11} {MP, CR(D)} – I&CS processing subsystem with double continuous redundancy of PM based on microprocessor;

– AS_{12} {MP, CR(T)} – I&CS processing subsystem with triple continuous redundancy of PM based on microprocessor;

– AS_{13} {MP, CR(Q)} – I&CS processing subsystem with continuous quad-redundancy of PM based on microprocessor;

– AS_{14} {FPGA, CR(D)} – I&CS processing subsystem with double continuous redundancy of PM based on FPGA;

– AS_{15} {FPGA, CR(T)} – I&CS processing subsystem with triple continuous redundancy of PM based on FPGA;

– AS_{16} {FPGA, CR(Q)} – I&CS processing subsystem with continuous quad-redundancy of PM based on FPGA.

2. Proposed construction variants of I&CS PN according to the processing node construction principles [9]:

– AS_{21} {MP, SR} – I&CS processing node with sliding redundancy of PM based on microprocessor. I&CS processing node with SR is regarded in this article as a set of the N main PMs and NR redundant PMs (fig. 1);

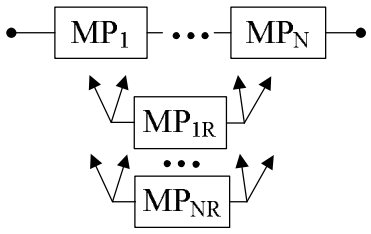

Fig. 1. I&CS PN with sliding redundancy of PMs based on microprocessor

– AS_{22} {MP, SR_G} – I&CS processing node with group sliding redundancy of PMs based on microprocessor. I&CS PN with SR_G is regarded in this article as two groups of the processing modules: the 1st group consists of the N main PMs and NR redundant PMs; the 2nd group consists of the N′ main PMs and NR′ redundant PMs (fig. 2);

– AS_{23} {FPGA, SR} – I&CS processing node with sliding redundancy of PMs based on FPGA (fig. 3);

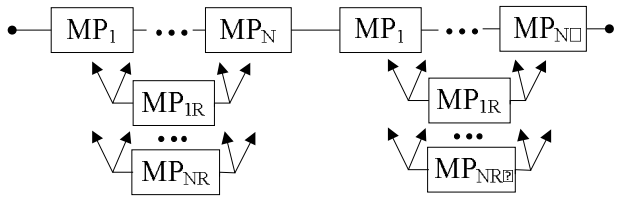

Fig. 2. I&CS PN with group sliding redundancy of PMs based on microprocessor

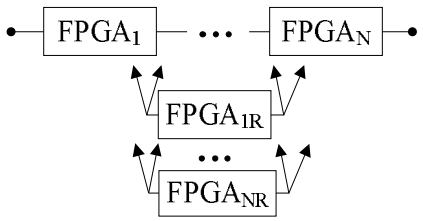

Fig. 3. I&CS PN with sliding redundancy of PMs based on FPGA

– AS_{24} {FPGA, SR_G} – I&CS PN with group sliding redundancy of PMs based on FPGA (fig. 4).

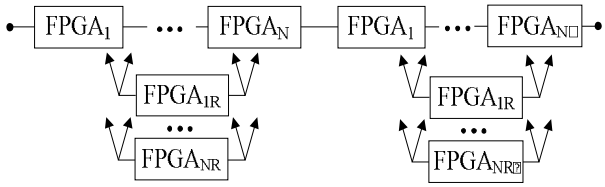

Fig. 4. I&CS PN with group sliding redundancy of PMs based on FPGA

Multicomponent FPGA-systems can be used for I&CS PN operation reliability improving.

These systems have flexible structure and allow not only to implement complex projects on a single chip and to perform multi-level verification during design stage of the FPGA electronic projects, but also allow (if necessary) the operational reconfiguration of internal algorithmic FPGA architecture during the operation of I&CS subsystems in which FPGA are used [11].

Architectural and structural variants analysis of the I&CS processing node construction

For analysis of the different AS_{ij} and further FS assessment it is specified indexes. These indexes can be used for comparison of different AS_{ij}.

Appropriate expressions for getting quantitative values of probability of non-failure I&CS PN/PS operation ($P_{NF\ ASij}$) for each AS_{ij} variant are following:

– for AS_{1j} variant:

$$P_{NFAS_{1j}} = 1-(1-P_{NF})^n,$$

where P_{NF} – the probability of the I&CS PS processing module non-failure operation. P_{NF} is defined by the following expression:

$$P_{NF} = e^{-\lambda_{PM}T},$$

where λ_{PM} – processing module failure rate;

T – time over which the probability of PM failure is determined;

n – number of the processing devices in I&CS PS for different TR (for CR(D) n = 2, for CR(T) n = 3, for CR(Q) n = 4).

– for AS_{21}, AS_{23} variant:

$$P_{NFAS_{21}} = P_{NFAS_{23}} = e^{N\lambda_{PM}} \sum_{i=0}^{NR} \frac{(N\lambda_{PM}t)^i}{i!},$$

where N – a number of the main PMs in I&CS PN;

λ_{PM} – I&CS PN processing module failure rate;

NR – a number of the redundant processing devices in I&CS PN;

– for AS_{22}, AS_{24} variant:

$$P_{NFAS_{22}} = P_{NFAS_{24}} = \left(e^{N\lambda_{PM}} \sum_{i=0}^{NR} \frac{(N\lambda_{PM}t)^i}{i!} \right) \times \left(e^{N'\lambda_{PM}} \sum_{i=0}^{NR'} \frac{(N'\lambda_{PM}t)^i}{i!} \right),$$

Expressions for $P_{NF\ ASij}$ are shown above with following limitations/assumptions:

– time distribution law to processing device failure – the exponential;

– all processing devices are identical and have the same reliability;

– majority means and reconfiguration means are built-in, that are part of unified processing modules;

– virtual recovery system immediately takes failing processing device for recovering after failure occurred;

– the main processing device functions instantly start running on the redundant processing device after the main processing device failure;

– switching from the main processing device on the redundant one is carried out instantly and unfailing.

The number of parallel similar PMs with MP or FPGA processing devices that are constituted I&CS PN/PS is defined by index d.

The index d depends on the redundancy type and defines as follows:

– $d = 2$ for AS_{11} and AS_{14} with redundancy type CR(D);

– $d = 3$ for AS_{12} and AS_{15} with redundancy type CR(T);

– $d = 4$ for AS_{13} and AS_{16} with redundancy type CR(Q);

– $d = N + NR$ for AS_{21} and AS_{23} with redundancy type SR;

– $d_1 = N + NR$; $d_2 = N' + NR'$ for AS_{22} and AS_{24} with redundancy type – SR_G.

Functional safety level depends on I&CS elements criticality and it should be accounted for FS assessment.

Processing modules criticality during critical tasks performance (z_{nm}, n – critical function index number, m – critical task index number) is defined by criticality index $v_N(z_{nm})$ for each of z_{nm}.

The index $v_N(z_{nm})$ depends on the redundancy type and defines as follows:

– $v_N(z_{nm}) = 0{,}5$ for AS_{11} and AS_{14} with redundancy type CR(D);

– $v_N(z_{nm}) = 0{,}33$ for AS_{12} and AS_{15} with redundancy type CR(T);

– $v_N(z_{nm}) = 0{,}25$ for AS_{13} and AS_{16} with redundancy type CR(Q);

– $v_N(z_{nm}) = \frac{1}{N + NR}$ for AS_{21} and AS_{23} with redundancy type SR;

– $v_N(z_{nm}) = \frac{1}{N + NR}$, $v_{N'}(z_{nm}) = \frac{1}{N' + NR'}$

for AS_{22} and AS_{24} with redundancy type SR_G.

Normalized index of PM criticality level v_N for n^{th} I&CS critical function f_n is specified as PM criticality multiplicity index. It is defined with following expression [9]:

$$v_N = \frac{m_{\Sigma N}}{m_{\Sigma N} + m_{\Sigma k}}, \qquad (1)$$

where $m_{\Sigma N}$ – absolute value of PM criticality through all critical tasks z_{nm} of I&CS critical function f_n;

$m_{\Sigma k}$ – total value of all elements criticality which are used during n^{th} critical function fulfillment.

Thus, it is possible to take into account PM criticality during critical functions realization for different I&CS PN/PS variants according to (1) and to select the most appropriate construction variant to assure I&CS PN/PS reliability at the design stage.

I&CS functional safety assessment

Functional safety (Fs) of I&C functional subsystem that performs one of the critical functions f_n is assessed according to the following expression:

$$Fs(f_n) = 1 - v_{\Sigma n} R_n, \qquad (2)$$

where $v_{\Sigma n}$ – specific total criticality of the n^{th} I&C subsystem critical function which is determined in accordance with the full set of I&C subsystem critical functions as on expression:

$$v_{\Sigma n} = \frac{m_{\Sigma n}}{\sum_{j=1}^{n} m_{\Sigma j}}, \qquad (3)$$

where $m_{\Sigma n}$ – criticality total value of all elements that are used in the n^{th} I&C subsystem critical function performance;

$m_{\Sigma j}$ – total criticality multiplicity index through all n critical functions (j = 1 ,…, n);

R_n – risk associated with critical function f_n:

$$R_n = P_{Fn} \cdot U_n, \qquad (4)$$

where P_{Fn} – the probability of the n^{th} critical function failure;

U_n – normalized in the range [0, 1] index of the probable harm that can take place during f_n operational failure.

Probability of the n^{th} critical function failure P_{Fn} can be defined using reliability block diagram methods. It is based on the direct state enumeration of the ways of exchange information and control signals.

This method allows taking into account all possible variants of I&C subsystem structural organization for complying with performing conditions of the critical functions.

The essence of this structural reliability estimation method is determination the average value of the failure probability of the connected block diagram elements, which are responsible for each critical function performance [12].

It is possible to take into account the reliability indexes of different architectural and structural variants of I&CS PN/PS construction during the iterative procedure of I&CS reliability and functional safety assessment at the design stage.

In general, to determine the critical functions failure probability it should be taken into account the following probabilistic components:

$$P_{Fn} = \left\{P_{FASij}, P_{FS}, P_{FA}, P_{FX}, P_{FY}\right\},$$

where $P_{FASij} = 1 - P_{NFASij}$ – the probability of the I&CS PN/PS processing modules failure;

P_{FS} – the probability of the I&CS sensors failure;

P_{FA} – the probability of the I&CS actuators failure;

P_{FX} – the probability of the I&CS signal transformation electronic blocks failure;

P_{FY} – the probability of I&CS signal transformation electronic/electromechanic control panel blocks failure.

Consequently, the most appropriate I&CS PN/PS construction variant using (2) - (4) (and as a result I&CS construction in general) can be selected to assure required FS level at the design stage.

Conclusion

To meet I&CS FS required level at the design stage it is necessary to achieve maximum effectiveness of the following actions:

1. Improving the reliability and continuity of information and control processes in I&CS by using different types of redundancy.

2. Application of new technology solutions (FPGA or microprocessor) for processing modules

which have the maximum values of the criticality multiplicity index due to results of FS assessment in order to increase the performance reliability of critical tasks and functions.

3. Using the proposed in this article analysis procedure of possible I&CS PN/PS construction variants and reliability and functional safety indexes it can be evidenced the applicability boundaries of the proposed architectural and structural construction variants to provide functional safety required level.

References

1. Functional safety of electrical / electronic / programmable electronic safety-related systems. Part 5: Examples of methods for determination of safety integrity levels: IEC 61508 - 5:2010, ed. 2.0. – [Publication data 2010-04-30]. – International Electrotechnical Commission, 2010. – 97 p.

2. Medical device software – Software life cycle processes: IEC 62304:2006, ed. 1.0. – [Publication data 2006-05-09]. – International Electrotechnical Commission, 2006. – 155 p.

3. Nuclear power plants – Instrumentation and control important to safety – General requirements for systems: IEC 61513:2011, ed. 2.0. – [Publication data 2011-08-25]. – International Electrotechnical Commission, 2011. – 205 p.

4. Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements: IEC 61511 - 1:2003, ed. 1.0. – [Publication data 2003-01-30]. – International Electrotechnical Commission, 2003. – 177 p.

5. Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems: IEC 62061:2012, ed. 1.1 Consol. with am.1. – [Publication data 2012-11-13]. – International Electrotechnical Commission, 2012. – 204 p.

6. Шубинский И.Б. Топологический полумарковский метод расчета стационарных показателей надежности и функциональной безопасности технических систем / И.Б. Шубинский, А.М. Замышляев // Ядерные информационно-измерительные технологии. – 2012. – № 2 (42) – С. 55-65.

7. Functional safety of electrical / electronic / programmable electronic safety-related systems. Part 4: Definitions and abbreviations: IEC 61508 - 4:2010, ed. 2.0. – [Publication data 2010-04-30]. – International Electrotechnical Commission, 2010. – 68 p.

8. Катаев О.В. Об одном подходе к построению отказоустойчивых бортовых многопроцессорных вычислительно-управляющих систем / О.В. Катаев // Искуственный интеллект. – 2008. – № 4. – С. 538-544.

9. Кулинич В.С. Методи та моделі оцінювання і забезпечення функціональної безпеки бортових інформаційно-керуючих систем літального апарату: автореф. дис. ... канд. техн. наук: спец. 05.13.06 «Інформаційні технології»/ В.С. Кулинич. – Х., 2013. – 20 с.

10. Павлов А.М. Принципы организации бортовых вычислительных систем перспективных летательных аппаратов [Електронний ресурс] / А.М. Павлов // Мир компьютерной автоматизации. – 2001. – 4(2001). – Режим доступу до ресурсу: http://www.mka.ru/?p=41177.

11. Федухин А.В. ПЛИС-системы как средство повышения помехоустойчивости / А.В. Федухин, А.А. Муха, А.А. Муха // Математичні машини і системи. – 2010. – №1. – С. 198-204.

12. Analysis techniques for dependability - Reliability block diagram and Boolean methods: IEC 61078:2006, ed 2.0. – [Publication data 2006-01-19]. – International Electrotechnical Commission, 2006. – 73 p.

Надійшла до редколегії 21.10.2014

Рецензент: д-р техн. наук, проф. Г.А. Кучук, Харківський університет Повітряних Сил імені Івана Кожедуба, Харків.

ПРОЦЕДУРА АНАЛІЗУ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ АРХІТЕКТУРНИХ ВАРІАНТІВ ОБЧИСЛЮВАЛЬНОЇ ПІДСИСТЕМИ ІНФОРМАЦІЙНО-КЕРУЮЧОЇ СИСТЕМИ, ПОВ'ЯЗАНОЇ ІЗ БЕЗПЕКОЮ НА ЕТАПІ ПРОЕКТУВАННЯ

В.С. Кулинич, О.В. Харибін

Приведена процедура синтезу, аналізу та вибору варіантів архітектурної та структурної побудови обчислювальної підсистеми як частини інформаційно-керуючої системи (ІКС), пов'язаної з безпекою. При використанні даної процедури можуть бути досягнуті необхідні рівні показників надійності та функціональної безпеки (ФБ) на етапі проектування. Обчислювальна підсистема ІКС для додатків пов'язаних з безпекою розглянута як єдине уніфіковане інформаційно-керуюче ядро, яке складається з обчислювальних модулів здатних до реконфігурації. Описана процедура оцінювання показника ФБ, який дозволить врахувати рівень критичності елементів та функцій ІКС.

***Ключові слова**: функціональна безпека, інформаційно-керуюча система, архітектура, обчислювальна підсистема, етап проектування, показник критичності, ризик, збиток.*

ПРОЦЕДУРА АНАЛИЗА ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ АРХИТЕКТУРНЫХ ВАРИАНТОВ ПОСТРОЕНИЯ ВЫЧИСЛИТЕЛЬНОЙ ПОДСИСТЕМЫ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ, СВЯЗАННОЙ С БЕЗОПАСНОСТЬЮ НА ЭТАПЕ ПРОЕКТИРОВАНИЯ

В.С. Кулинич, А.В. Харыбин

Приведена процедура синтеза, анализа и выбора вариантов архитектурного и структурного построения вычислительной подсистемы как части информационно-управляющей системы (ИУС) связанной с безопасностью. При использовании данной процедуры могут быть достигнуты требуемые уровни показателей надежности и функциональной безопасности (ФБ) на этапе проектирования. Вычислительная подсистема ИУС для приложений связанных с безопасностью рассматривается как единое унифицированное информационно-управляющее ядро, которое состоит из вычислительных модулей способных к реконфигурации. Описана процедура оценивания показателя, который позволит учесть степень критичности архитектурных элементов и функций ИУС.

***Ключевые слова**: функциональная безопасность, информационно-управляющая система, архитектура, вычислительная подсистема, этап проектирования, показатель критичности, риск, ущерб.*