UDC 681.324

V.V. SKLYAR

State Scientific Technical Center on Nuclear and Radiation Safety, Ukraine

A RISK-ORIENTED APPROACH TO ASSESSMENT AND ASSURANCE OF SAFETY OF CRITICAL INSTRUMENTATION AND CONTROL SYSTEMS

A solution of a task of assessment and assurance of safety of critical Instrumentation and Control systems (I&C) by risks analysis is considered. A common taxonomy of risks of critical I&C is formed. An approach to compared risks analysis for I&C used new information technologies is proposed.

risk analysis, new information technologies

1. Task setting and transactions review

The most essential property of technical critical systems is their safety. A safety is an object ability to achieve acceptable risks levels for people life and health, environment and economy [1-5].

From the above definition risk is one from the main categories of safety. Risk is potential possibility of break of operable conditions of a technical critical system and damage related with this event. For risks of Instrumentation and Control systems (I&C) influence of their failures to common safety of a technical critical system should be analysed. Risks damages lie in decreasing of safety level of technical critical systems.

The common scheme of safety assessment and assurance of critical I&C is presented in the fig. 1 [6]. Methods of risks analysis are the base of safety assessment.

A risk R(t) during time t related with some event is calculated as the product of probability of this event P(t) and adverse consequences D of this event:

$$R(t) = P(t) \cdot D . \qquad (1)$$

Thus risks values can be considered as safety indicators, a conception of risks analysis is identically with safety assessment and analysis.

Realisation of risks analysis is recommended by international standards [7-9] and approbated by long-term practice of I&C assessment in such critical branches as nuclear power engineering, chemical industry, aerospace technique, transport etc. At the same time risks analysis is the main constituent of safety assessment.

Methods of risks analysis are used for identification and assessment of potential damages with goal to develop recommendation for elimination or reducing risks probabilities and/or risks consequence till acceptable levels. The main methods of risks analysis are the following [10,11]:

– Fault Tree Analysis (FTA);

– Failure Modes, Effects and Criticality Analysis (FMECA);

– Hazards and Operability Analysis (HAZOP).

Application of new information technologies for development of modern I&C permits on the one hand greatly improve technical characteristics of such systems including their reliability and safety thanks to optimisation of a structure, increasing reliability of electronic elements, software quality and technologies of design and testing. On the other hand it is needed careful and complex analysis of risks which appear with new information technologies [12].

The known transactions focus the main attention to assurance of completeness of risks analysis which should cover all life cycle stages of I&C and of all hardware and software components of I&C [13-15]. But a task of I&C risks analysis at new information technologies consideration stays undecided. This task can be solved on the base of a deterministic approach.

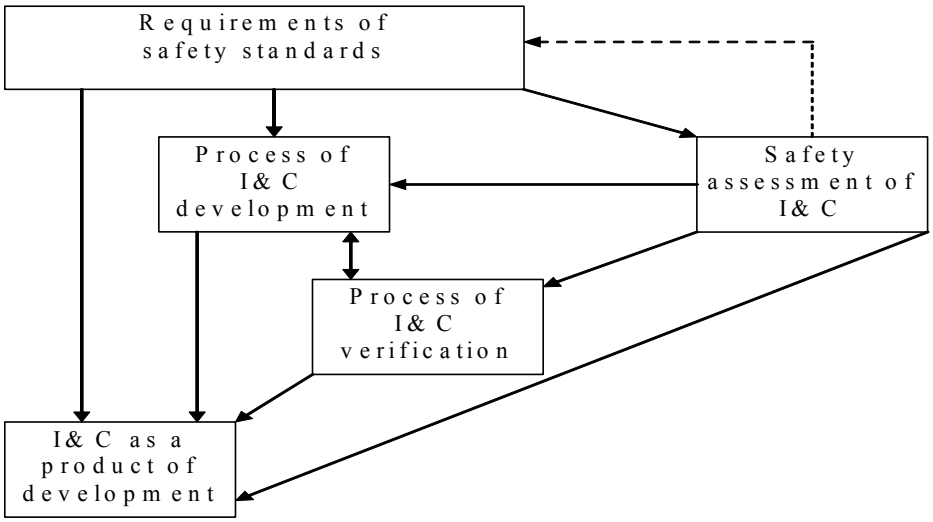

Fig. 1. The common scheme of safety assessment and assurance of critical I&C

The objective of this paper is development of such risk-oriented approach to assessment and assurance of safety of critical I&C, which permits to take into account and to assess new information technologies used for I&C creation.

2. Deterministic and probabilistic approaches to risks analysis

Deterministic and probabilistic approaches are used for safety assessment.

A deterministic approach consists in consideration of predetermined events (failures and accidents) which could occur. Such approach is used for example in nuclear power engineering as the conception of defence in depth of nuclear power plants [4,5]. In such conditions risks are considered without numerical value but as linguistic variable. The table 1 presents linguistic values of risks which depends from linguistic values of critically and frequency of events. The bold line rounds an area of risks which should be considered and analysed.

A probabilistic approach consists in definition of numerical values of probability of unacceptable events for every type of risks. For example nuclear and radiation safety standards establish for designed units of nuclear power plants probability of maximum accident radioactive injection equal to 10^{-7} 1/year for one reactor.

Table 1

An example of matrix for determining risks

Event frequency	Hazard Category			
	Catastrophic	Critical	Marginal	Negligible
Frequent	High	High	High	Medium
Probable	High	High	Medium	Low
Occasional	High	High	Medium	Low
Remote	High	Medium	Low	Low
Improbable	Medium	Low	Low	Low

3. Deterministic risks analysis for new information technologies

One from the main applications of deterministic risks analysis is safety standards development. Such standards contain set of safety requirements which in fact are directed at parry of some types of risks. In that way developers of I&C prevent possible unacceptable events by determinated actions for example by redundancy, by increasing of stability to external impacts etc.

The common approach to solution of a problem of application of new information technologies for safety critical I&C [12] is presented on the fig. 2.

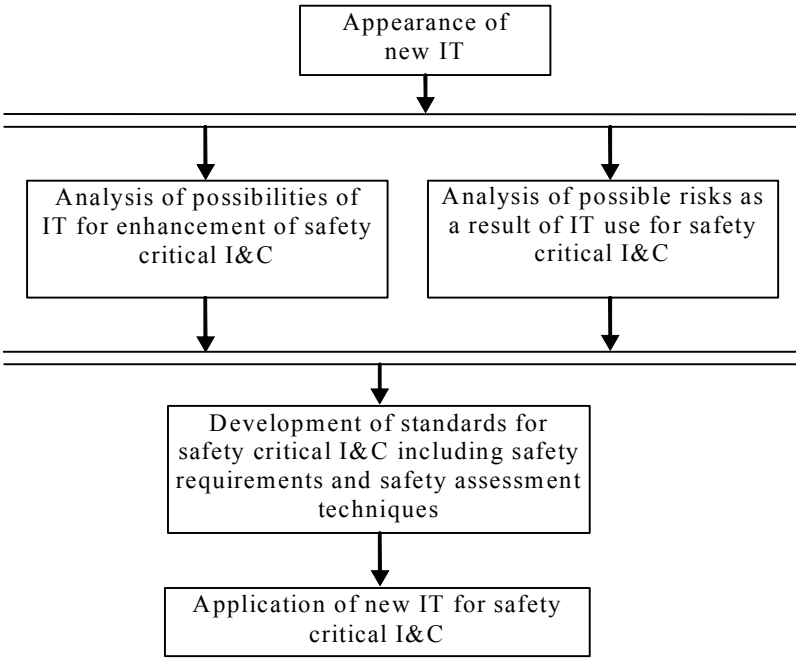

Fig. 2. Procedures of safety assessment and assurance of critical I&C developed on the base of new information technologies (IT)

New information technologies provide some possibilities for increasing of technical characteristics of safety critical I&C including properties related to safety and reliability. A back of technical progress is appearance of new risks which can abolish received advantages. Therefore before application of new information technologies complete analysis of appropriated risks should be fulfil. New safety requirements which regulate application of safety critical I&C for some critical branches can be developed as a result of such analysis. A required level of safety of critical I&C used new information technologies could be assured only in the case of realisation the above procedures.

4. A risks taxonomy for safety critical I&C

The common risks classification for man-caused objects includes the following:

– internal risks of I&C project including organisational, manufacturing and resource risks;

– external risks appeared during operation of I&C consisting of safety critical system including risks of external extreme impacts and risks of latent defects occurrence.

As a result of analysis the above common risks groups are concretised as the following two groups (see the fig. 3):

– risks related to products properties;

– risks related to realisation of life cycle processes.

The common taxonomy (classification scheme) of risks for safety critical I&C is given in the table 2. This taxonomy is the base for requirements formation of safety standards in area of safety critical I&C.

5. Comparative risks analysis for I&C used new information technologies

Software and hardware components of I&C have different properties and hence they generate different risks.

Therefore risks analysis should be performed as for I&C in whole as for software and hardware.

The common approach to safety assessment and assurance for modernised man-caused objects lies in reduction of summary risk for new safety critical system in comparison with summary risk for previous safety critical system [5, 8].

The above approach needs of two operation with risks: a comparison and an integration.

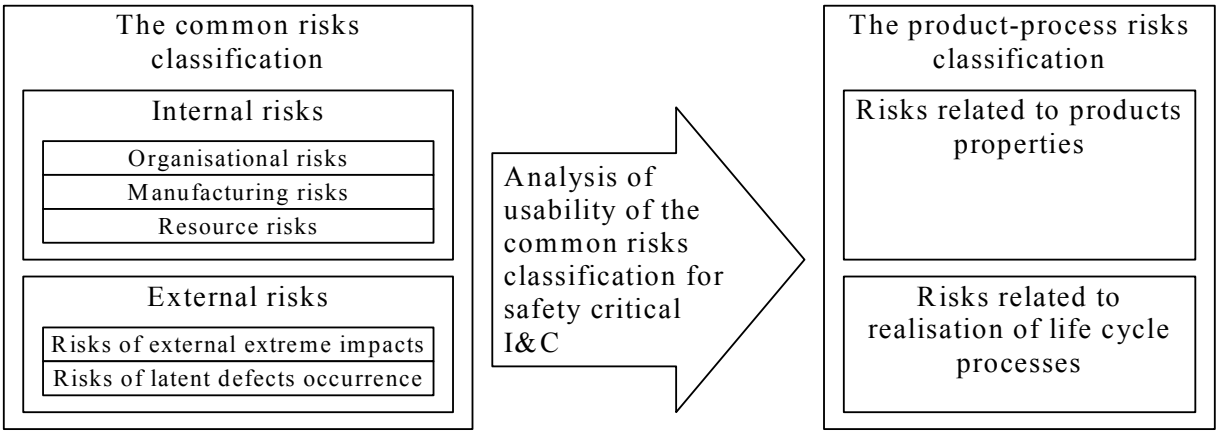

Fig. 3. A transition from the common risks classification to the product-process risks classification

Table 2

A risks taxonomy for safety critical I&C

Risks group	Risks type
Risks related to products properties	Risks of violation of requirements to functions
	Risks of violation of requirements to redundancy
	Risks of violation of requirements to independency of equipment
	Risks of violation of requirements to defence from common case failures
	Risks of violation of requirements to accuracy
	Risks of violation of requirements to time characteristics
	Risks of violation of requirements to reliability
	Risks of violation of requirements to man-machine interface
	Risks of violation of requirements to defence from faults of personnel
	Risks of violation of requirements to defence from input data distortion
	Risks of violation of requirements to defence from unauthorised access
	Risks of violation of requirements to defence from external impacts
	Risks of violation of requirements to defence from changing of parameters of power supply
	Risks of violation of requirements to defence from electromagnetic impacts
	Risks of violation of requirements to technical diagnostics
Risks related to realisation of life cycle processes	Risks of violation of requirements to development process
	Risks of violation of requirements to quality assurance process
	Risks of violation of requirements to verification and validation process
	Risks of violation of requirements to testing and acceptance process
	Risks of violation of requirements to operation process
	Risks of violation of requirements to pre-developed products

Comparative risks analysis for I&C used new information technologies includes the following sequence of operations:

1) development of model of risks related to safety critical I&C on the base of risks identification and classification taking into account national and international standards for appropriated safety critical area;

2) examination of risks related to application of new and previous (traditional) information technologies for safety critical I&C as well as of ways of decreasing and/or elimination of risks;

3) formation of conclusion of comparative risks analysis related to application of new and previous information technologies for safety critical I&C.

A formal description of operation with risks performed for comparative risks analysis is given below.

An initial model contains a set of risks $Risk = \{Risk_i\}$ which are identified in accordance with used taxonomy. This set can include several subsets. For the risks model given in the table 2 there are two disjointed subsets:

$Risk_{PROD} = \{Risk_{PROD\,i}\}$, $Risk_{PROC} = \{Risk_{PROC\,i}\}$.

An additional part of risks model included the subset $\Delta Risk = \{\Delta Risk_i\}$ is formed as a result of analysis of specific risks appeared through application of new information technologies.

During comparative analysis risks values for I&C used previous (traditional) information technologies are compared with risks values for I&C used new information technologies for every type of risks. The operation of risks comparison uses linguistic values of risks. Results of comparison is the one from the following three quantifiers: "MORE", "EQUAL", "LESS". Thus the operation of risks comparison has a view:

$$\begin{cases} VRisk_{NEWi} > VRisk_{OLDi} \Rightarrow Risk_{>} = Risk_{>i-1} \cup Risk_i; \\ VRisk_{NEWi} = VRisk_{OLDi} \Rightarrow Risk_{\Leftrightarrow} = Risk_{\Leftrightarrow i-1} \cup Risk_i; \\ VRisk_{NEWi} < VRisk_{OLDi} \Rightarrow Risk_{<} = Risk_{>i-1} \cup Risk_i , \end{cases} \quad (2)$$

where $VRisk_{NEW\,i}$ – a value for i^{th} risk in the case of application of new information technology;

$VRisk_{OLD\,i}$ – a value for i^{th} risk in the case of application of previous (old) information technology;

$Risk_{>} = \{Risk_{>\,i}\}$, $Risk_{\Leftrightarrow} = \{Risk_{\Leftrightarrow\,i}\}$, $Risk_{<} = \{Risk_{<\,i}\}$ – disjointed subsets of a risks model which include risks having values in the case of application of new information technology correspondingly more, equal and less than risks values in the case of application of previous information technology; before begin of risks analysis there is $Risk_{>} = Risk_{\Leftrightarrow} = Risk_{<} = \varnothing$; during comparative risks analysis elements are added to above subsets and in the end of risks analysis $Risk_{>} \cup Risk_{\Leftrightarrow} \cup Risk_{<} = Risk$.

It is needed to perform the operation of risks integration for making decision about a possibility of application of new information technology. Sometimes priority risks for which results of comparison are taken into account first of all can be given. Then in the case $VRisk_{NEWi} > VRisk_{OLDi}$ new information technology should be rejected.

In the common case for risks values integration it is needed to perform "weighing" of risks in respect to their influence to safety of critical I&C. The sum of weight factors is $\sum w_i = 1$. In the common case there is $w_i = 1 / card\ Risk$. Since numerical values of risks are not considered, risks integration can be performed with use only values of weight factors:

$$\Sigma VRisk_{>} = \sum_{Risk_{>}} w_i; \quad \Sigma VRisk_{<} = \sum_{Risk_{<}} w_i . \quad (3)$$

It should be performed comparison of integral risks values after their integration. If $\sum VRisk_{<} < \sum VRisk_{>}$, it means summary risk of operation of safety critical I&C will increase in the case of application of new information technology. In this case a decision about application of new information technology should be rejected. If $\sum VRisk_{<} > \sum VRisk_{>}$, it means summary risk of operation of safety critical I&C will decrease in the case of application of new information technology. In this case specific risks $\Delta Risk$ appeared with application of new information technology should be taken into account in risks model of I&C. Weight factors $\sum w_i = 1$ should be defined in the new base $i = 1,...card(Risk \cup \Delta Risk)$.

Risks integration is performed as

$$\Sigma \Delta VRisk = \sum_{\Delta Risk} w_i; \quad \Sigma VRisk_{<} = \sum_{Risk_{<}} w_i . \quad (4)$$

If $\sum \Delta VRisk > \sum VRisk_{<}$, it means summary risk of operation of safety critical I&C will increase in the case of application of new information technology. In this case a decision about application of new information technology should be rejected. If $\sum \Delta VRisk < \sum VRisk_{<}$, it means summary risk of operation of safety critical I&C will decrease in the case of application of new information technology. In this case application of new information technology is recommended for assurance of safety increasing of critical I&C.

6. Conclusions and the next steps

The proposed approach has been applied for comparative risks analysis of using of Fields Programmable Gates Arrays (FPGAs) and microprocessors for realisation of control functions of I&C important to safety of Nuclear Power Plants (NPPs). Performed risks analysis permitted to make a conclusion about possibility to use

FPGA in I&C important to NPPs safety. FPGAs permit to reduce most of I&C risks in comparison with I&C on the base of microprocessors. It concerns of risks related to the following requirements violations:

– to defence from common case failures;

– to time characteristics;

– to technical diagnostics;

– to realisation of all life cycle processes.

It is expediently to direct the next steps of research to development and detailing of risks model of I&C for different critical branches. One from the important aspects of such detailing is accounting of secondary risks appeared as a result of actions for decreasing and/or elimination of initial risks included to risks model.

References

1. Laprie J.-C. Dependability Handbook. LAAS Report n 98-346. – Toulouse: Laboratory for Dependability Engineering, 1998. – 365 p.

2. Lawrence J.D. Software Safety Hazard Analysis. NUREG/CR-6430. Livermore, CA, USA: Lawrence Livermore National Laboratory, 1995. – 80 p.

3. Leveson N. Safeware: System Safety and Computers.– Addison-Wesley, 1995.– 431 p.

4. Либман Ж. О ядерной безопасности. – Фонтене-о-Роз (Франция):, 1997. – 690 с.

5. Ястребенецкий М.А., Васильченко В.Н., Виноградская С.В. и др. Безопасность атомных станций: информационные и управляющие системы. – К.: Техника, 2004.– 472 с.

6. Скляр В.В. Оценка и обеспечение безопасности информационно-управляющих систем критического использования: элементы методологии и формальные модели // Авиационно-космическая техника и технология. – 2005. – № 6 (22). – С. 84-93.

7. Steininger U., Karff H. Risk and cost optimization of the safeguarding of DB's Railwork // Proceeding of the 10th European Conference of Safety and Reliability.– Munich (Germany).– 1999.– P. 1593-1596.

8. Лола І.О., Севбо О.Є. Впровадження ризик-орієнтованих підходів у регулюючу діяльність в Україні // Ядерна та радіаційна безпека. – 2002. – Спеціальний випуск присвячений 10-й річниці програми TACIS. – С. 45-48.

9. Згуровский М.З. и др. Информационный подход к анализу и управлению проектными рисками // Проблемы управления и информатики. – 2000.– № 4. – С. 148-156.

10. Печерица А.В. Пути получения достоверной информации по надежности для оценок риска // Ядерная и радиационная безопасность. – 2004. – Т. 7. – № 2. – С. 42-46.

11. Грачева М.В. Анализ проектных рисков. – М.: ЗАО Финстатинформ, 1999. – 216 с.

12. Харченко В.С., Ястребенецкий М.А., Скляр В.В. Новые информационные технологии и безопасность информационно-управляющих систем АЭС // Ядерная и радиационная безопасность. – 2003. – Т. 6. – № 2.– С. 19-28.

13. Радаев Н.Н. Повышение точности прогноза вероятности катастроф за счет ущерба неоднородных статистических данных по ущербу // Автоматика и телемеханика. – 2000. – № 3. – С. 183-189.

14. Харченко В.С., Байда Н.К. Скляр В.В. Надежность и безопасность сложных проектов и технологии снижения рисков // Системи обробки інформації. – Х.: НАНУ, ПАНМ, ХВУ. – 2001. – Вип. 2 (12). – С. 182-188.

15. Харченко В.С., Скляр В.В., Тарасюк О.М. Анализ рисков аварий для ракетно-космической техники: эволюция причин и тенденций // Радіоелектронні і комп'ютерні системи. – Х.: НАКУ «ХАІ». – 2003. – Вип. 3. – С. 135-149.

Надійшла до редакції 31.01.2006

Рецензент: д-р техн. наук, проф. В.С. Харченко, Національний аерокосмічний університет ім. М.Є. Жуковського "ХАІ", Харків.