ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
UDC/UDK 658.562.4.011.3

TECHNICAL PRODUCT RISK ASSESSMENT INTEGRATION INTO THE ENTERPRISE RISK MANAGEMENT

Mirko Djapic, Ljubomir Lukic, Predrag Popovic

Subject review

In the nineties of the previous century, the European Union achieved, through introducing the New and Global Approach to technical harmonization and standardization, a significant improvement in the approach to conformity assessment of products, by integrating the requirements for technical products safety into the process of its designing. This was achieved by preventive analysing and quantifying of risk levels in the design process with the objective of determining the scope of the needed safety systems. On the other hand, we have witnessed a rapid development and implementation of holistic approaches to risks management in enterprises, unified in the modern business practice by the name of Enterprise Risk Management (ERM). Going along that line, the paper presents the basis of the EU New and Global Approach and gives an approach to integrating New Approach Directives risk assessment into the holistic approach of risks management in organization, such as ERM.

Keywords: *Enterprise Risk Management, EU New and Global Approach, ISO 31000*

Integriranje ocjene rizika tehničkih proizvoda u upravljanje rizicima u poduzeću

Pregledni članak

Europska Unija je početkom devedesetih godina prošlog stoljeća, kroz uvođenje Novog i Globalnog pristupa tehničkoj harmonizaciji i standardizaciji, ostvarila značajno unapređenje u postupku ocjenjivanja usuglašenosti proizvoda na taj način što je zahtjeve za sigurnost tehničkih proizvoda integrirala u proces projektiranja. To je postignuto tako što se u procesu projektiranja preventivno analiziraju i kvantificiraju nivoi rizika u cilju određivanja opsega potrebnih sustava sigurnosti. S druge strane, svjedoci smo ubrzanog razvoja i uvođenja cjelovitih pristupa upravljanja rizicima u poduzeću koji je u suvremenoj poslovnoj praksi objedinjen nazivom Upravljanje rizicima poduzeća (ERM – Enterprise Risk Menagment). Slijedeći to, u radu se preko osnova Novog i Globalnog pristupa Europske Unije daje pristup za integraciju ocjene rizika u smjernicama Novog pristupa u cjeloviti pristup upravljanju rizicima u poduzeću kakav je ERM suglasno standardu ISO 31000:2009.

Ključne riječi: *ISO 31000, Novi i Globalni pristup EU, upravljanje rizicima poduzeća*

1 Introductions

European Union through introducing the New Approach to technical harmonization and standardization has achieved a breakthrough in the product safety by integrating its safety requirements into the product development process [1, 2, 3]. In the directives for technical products, essential health and safety requirements have been set, that each technical product has to satisfy prior to placing it on the market. These requirements are defined in a general form and the way of their implementation is given in the harmonized standards. In this way, designers and suppliers of technical products have got clear instructions regarding the way to accomplish the conformity of these products to the directives' requirements and the way of integrating safety requirements into the phase of developing these products. In this way, fundamental change has been achieved in preventing possible occurrence of accidents. The decision regarding the level of safety measures is based on previously conducted risk assessment.

Risk assessment is the methodology through which risk levels are quantified with the objective of determining the scope of required safety measures [4]. Management of risk is a continuous process and should span all of the product development and realization phases [5, 6].

On the other hand, contemporary business practice proves how important risk analysis and assessment is for running a business successfully. The importance of individual risks for an organization is determined by numerous factors, both internal ones depending on the organization itself and external factors set forth by the environment in which the organization operates. Experience in the business practice in the last fifteen years has shown that the risk management concept has been in the phase of significant changes. This is substantiated by the fact that business associations, international, regional and national standardization bodies have created several models, standards and operation frameworks with the basic objective of defining what it is and how it is to be implemented. That is how the slogan Enterprise Risk Management – ERM originated to denote a comprehensive (holistic) approach to treating all risks in an organization [7, 8, 9, 10, 11, 12].

Analyses of major ERM models that have so far been developed and successfully implemented in the world go beyond the scope and objectives of this paper. Therefore, the paper only partially presents the ERM model defined in the international standard ISO 31000:2009 [13]. This has been done in order to show that it is possible to integrate the risk assessment required in the EU New Approach Directives (NAD) into a holistic risk management model of an enterprise, which is the basic objective of the paper. In order to fulfil this objective, the text to follow presents: (1) EU New Approach basics and the concept of conformity assessment in New Approach directives (the Global Approach), (3) the concept of international standardization in the risk management field. At the end, the model is given of integration of the risk assessment given in the NAD into the Enterprise Risk Management (ERM) model.

2 European Union New and Global Approach

Free circulation of goods, services, people and money are the cornerstone of the single market. The objective is as follows: *Removal of all technical barriers from the EU*

*internal market, which have resulted from **national** technical regulations, applying of national standards and the established procedures for products testing, controlling and certification* [14].

The mechanisms in the form of New and Global approach enable accomplishing of this goal (Fig. 1). The approaches are based on:

- preventing new barriers to trade
- mutual recognition and
- technical harmonization.

On the other hand, there are different ways or procedures to placing products on the European Union market. In these procedures, the manufacturers, i.e. suppliers, use various techniques which very often also involve engaging independent third parties in product conformity assessment. Fig. 2 offers the global depiction of the algorithm applied with "**mandatory**" (require CE mark) and "**voluntary**" product certification.

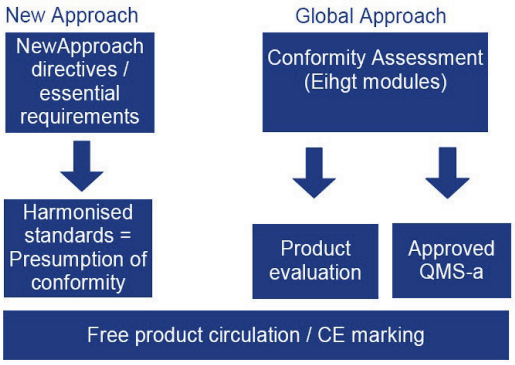

Figure 1 New and Global Approach

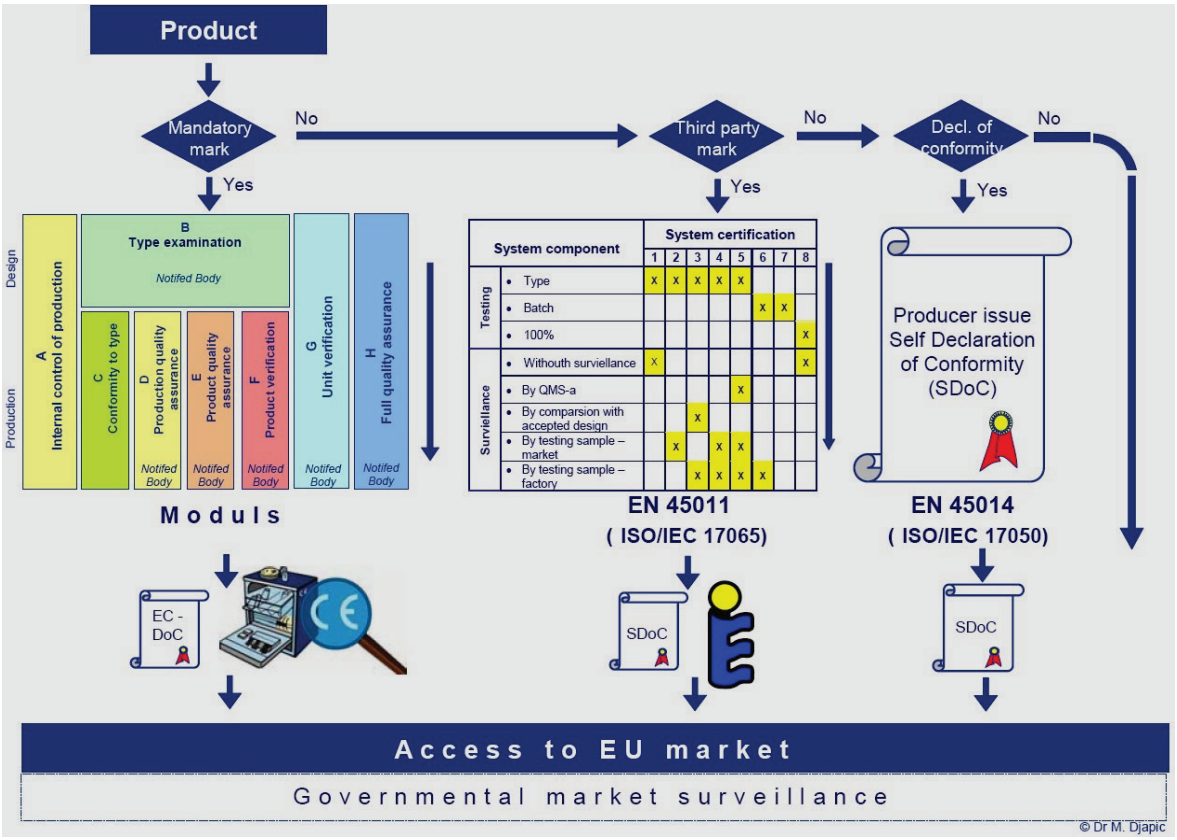

Figure 2 European approach to product conformity assessment [2, 4]

The first response requested from the manufacturer or his authorized representative is to the question whether the products have been covered by the New Approach technical legislation or not. If it falls within technical legislation, i.e. is covered by the New Approach directives, the conformity assessment procedures are defined in the European Union Council's Decision on introducing the Conformity Assessment Modules (Global Approach (Fig. 2). Many of the modules out of the total eight of them, require the manufacturers to involve, in their conformity assessment procedure, an independent third party, i.e. notified bodies. Engagement of these bodies is mainly requested in the conformity assessment procedures related to highly risky products, from the point of view of hazards for human health and environment safety. It is therefore very important that these bodies perform their function with previously proven high levels of competence, integrity and professional attitude.

The other response imposed to manufacturers is to the question whether, if a product does not fall under the New Approach technical legislation, the product certification is required, out of marketing or other reasons, or not.

The ISO book "Certification and Related Activities" [15] renders eight systems for product certification through a third party (Fig. 2). In essence, the product certification systems should cover at least two activities: (1) the acceptance of the product based on testing of the product and/or the production process and (2) the surveillance of the continuing ability of the manufacturer to produce a conforming product.

3 The Concept of the Enterprise Risk Management

All organizations, regardless of their field of activity and size, are faced, in realizing their objectives, with some form of risk. The objectives may vary and may be related to a strategic initiative, operative realization of a project, product, service and the similar. They are reflected through environment protection, social safety and security outcomes, commercial, financial and economic measures, such as in social, cultural, political and regulatory influences.

The Enterprise Risk Management – ERM is one of the most popular and at the same time very often insufficiently understood concept in the contemporary business practice. It is a discipline which has had rapid development and which has been viewed in multiple ways, starting from the point of view regarding what it encompasses to how it is implemented.

The concept is not overly complex nor is it cost demanding, but it can bring benefits and new values to organizations. If we define a problem correctly and share our findings with others, we can reduce the surprises which, unfortunately, often cannot be eliminated. However, they can be kept under control.

In the beginning, the risk management focused only on the negative side of risk, i.e. on protecting from hazards, while the modern practice has brought about a holistic view, treating with equal importance both positive and negative risk facets (upsides and downsides). The above risk is related to an ingoing event, the consequences of which increase the organization's objectives realization likelihood, or have a positive effect on the interested parties. The below stated risks, on the other hand, are related to those events and their consequences that are threatening or have a negative effect on realizing the objectives and on the interested parties.

Today, risk management incites reviewing of all the factors, whether positive or negative ones, potentially affecting realization of the organization's objectives. Management of opportunities and threats represents a key portion of the organization's strategic planning process.

The basic assumption of a successful risk management in an enterprise starts from the assumption that it has to bring about additional values to the organization, i.e. in other words, the costs of developing and implementing this process, i.e. system, have to be lower than the benefits it is passing on. These benefits are reflected on the one hand in reducing the potential threats effects and consequences on realizing the organization's objectives, creating on the other hand the conditions for these possible benefits to exert more pronounced influence over these objectives themselves.

In literature, this discipline is named by the following titles [7]: Total Risk Management (TRM), Integrated Risk Management (IMR), Holistic Risk Management or Enterprise Risk Management (ERM)

Regardless of which of these "buzz words" names is used, it is the risk management relating to the issue of how to organize and how to carry out identification, analysis and controlling from the managerial level of "opportunities" and "threats" that organizations face in realizing their objectives. How to relate to opportunities and threats that endanger the organizational objectives depends on how well the organization's management and employees understand the risks and the way of managing them.

3.1 Standardization in the risk management field

Enterprise Risk Management (ERM) is a discipline present in all organizations, either private owned, public, non-profit and profit ones, at all levels of hierarchy, i.e. in all circumstances. That is one of the basic reasons that more than fifteen years ago, the need was articulated for a form of standard so as to ensure agreement of all interested parties regarding [7]:

- Terminology related to this concept
- Infrastructure, organizational structure and the processes it is implemented through
- Risk management objectives.

At the start of defining the previously stated items, it is important to designate the facts in the text below.

There are organizations in the world today, such as bodies, associations, alliances, etc. which have developed and published various forms of standards and/or "frameworks" in the field of risk management. On the other side, there is no uniform comprehension of the word "standard" with all these protagonists. Apart from the international, regional and national organizations for standards developing (such as ISO, IEC, CEN, CENELC or, for example, the national standardization body for example DIN, BS, HZN, etc.), other protagonists use the term standard and/or framework. The closest synonym for a framework could be a **general instruction**. However, the understanding of the concept of standard and framework differs from region to region. In the United States of America, for example, the Committee of Sponsoring Organizations of the Treadway Commission, COSO has developed **ERM Integrated framework** [16], while in Europe, for instance, the Federation of European Risk Management Associations (FERMA) uses the **Risk Management Standards** developed by three bodies from Great Britain (Risk Management Institute, Managers' Association of Risks and Insurance and the National Forum for Risk Management in Public Sector) [7].

Thus, as stated by Erben in [8], the terms standard and framework represent the same thing for some, as they are used to describe a set of rules for solving an actual problem or to fulfil some concrete requirements.

The readers should not be confused by this, as generally speaking, it is more or less the same things, i.e. defining (industrial standardization) the management process named "Enterprise Risk Management – ERM". The purpose of these frameworks and/or standards is to serve as a general instruction primarily for the organization's management on their onset of developing and implementing this management process.

Presenting the standards, i.e. frameworks presented in the world today surpasses the objectives of this paper. Therefore, we are going to focus further only on standardization in the field of risk conducted by the International Organization for Standardization and some of the most significant national standardization bodies (Tab. 1).

Significant efforts in the risk defining were exerted by the international organizations for standards ISO/IEC [13, 17] as well as by some national ones, first and fore-

most the Australia & New Zealand standardization organizations (AS/NZS 4360:2004) [18].

Thus, the "AS/NZS 4360 Risk Management Standard" defines the risk as the probability of something that may happen affecting the previously defined objectives. Risk is measured as the ratio of consequences and probabilities of some events' occurrence. This definition was, for many years, the leading one when explaining what risk management is and what it serves for. It is still topical as it can be found in many standards such as the standards serving as guidelines for conducting the risk analysis and assessment in the EU New Approach directives, such as, for instance, ISO 14121:2007 standard.

Table 1 The most influential international and national standards developed by the standards developing bodies

Publisher	Standards	Publisher	Standards
ISO	**ISO 31000:2009,** Risk management -- Principles and guidelines	CSA (Canada)	**CSA Q 850: 1997**, Risk Management Guidelines for Decision Makers
ISO/IEC	**ISO/IEC 73:2009**, Risk management -- Vocabulary	JSA (Japan) (withdraw)	**JIS Q 2001:2001**, Guidelines for development and implementation of risk management system
	ISO/IEC 51:1999, Safety aspects -- Guidelines for their inclusion in standards	AS/NZS (Australia / New Zealand)	**AS/NZS 4360:2004**, Risk Management
	ISO/IEC 31010:2009, Risk management -- Risk assessment techniques	BSI (Great Britain)	**BS 25999-2:2007**, Business continuity management. Specification
ISO	**ISO 14121-1:2007**, Safety of machinery — Risk assessment — Part 1:Principles		**BS 31100:2011**, Risk management. Code of practice and guidance for the implementation of BS ISO 31000
	ISO/TR 14121-2:2007, Safety of machinery -- Risk assessment -- Part 2: Practical guidance and examples of methods		**BS 6079-3:2000**, Project management. Guide to the management of business related project risk
	ISO 14971:2007, Medical devices -- Application of risk management to medical devices	ON (Austria)	**ONR 49000:2010**, Risk Management for Organizations and Systems - Terms and basics - Implementation of ISO 31000
ISO/IEC	**ISO/IEC 27005:2011**, Information technology -- Security techniques -- Information security risk management		**ONR 49001:2010**, Risk Management for Organizations and Systems - Risk Management - Implementation of ISO 31000
ISO	**ISO 14798:2009**, Lifts (elevators), escalators and moving walks -- Risk assessment and reduction methodology		**ONR 49002-1:2010**, Risk Management for Organizations and Systems - Part 1: Guidelines for embedding the risk management in the management system - Implementation of ISO 31000
	ISO 17776:2000, Petroleum and natural gas industries -- Offshore production installations -- Guidelines on tools and techniques for hazard identification and risk assessment		**ONR 49002-2:2010**, Risk Management for Organizations and Systems - Part 2: Guideline for methodologies in risk assessment - Implementation of ISO 31000
EN	**EN 1127-1:2011,** Explosive atmospheres. Explosion prevention and protection. Basic concepts and methodology		**ONR 49002-3:2010**, Risk Management for Organizations and Systems - Part 3: Guidelines for emergency, crisis and business continuity management - Implementation of ISO 31000
	EN 13463-1:2009, Non-electrical equipment for use in potentially explosive atmospheres. Basic method and requirements		**ONR 49003:2010**, Risk Management for Organizations and Systems - Requirements for the qualification of the Risk Manager - Implementation of ISO 31000

Standard ISO 31000:2009 [13] on risk management and ISO/IEC 73:2009 [17] guidelines for defining terms in the risk field, define risk as the **effect of uncertainty on acquiring organization's objectives**. It is the effect of a deviation from the expected outcome of an event, situation, etc., that can be in either positive or negative direction.

Risk is often expressed as a combination of consequences of an event and the probability of its occurrence. Probability is defined as a chance for something to happen, no matter whether it has been defined, measured or determined, either objectively or subjectively, or whether it has been described in quantified or qualified manner by using general mathematical terms, such as event probability (expressed in the 0-1 interval) or an event occurrence frequency in the given period of time. The uncertainty is observed as a state of lack of information and in some cases as a state of partial lack of information related to the knowledge and understanding of certain events, their consequences on the organization's objectives or corresponding likelihood.

Out of these definitions, the conclusions that follow can be drawn [19, 20]:

- Risk is related to achieving objectives.
- ISO/IEC organizations use the uncertainty as the basic pillar in defining risk, and not the probability as it was formerly defined by the standard AS/NZS 4360:1995.

Today, papers can be traced in literature highlighting some shortcomings of the risk being defined in this way by the ISO/IEC organizations. Readers are directed, for example, to [19], etc. This is understandable, as the concept of risk is related to all fields of human activities and it is very difficult to find and define something that would be satisfactory to all. However, the authors of this paper consider this definition to be the best, most general definition that is acceptable for practitioners in most of the fields of human activities. This is additionally corroborated by the contemporary mathematical tools which enable mathematical modelling of uncertainty, such as the tools developed on the basis of fuzzy sets, Bayes' nets or valuation nets, developed on the basis of the Dempster–Shafer theory of belief function. Also it is important to mention that the IEC - International Electrotechnical Commission has developed standard related to the techniques that can be used in risk management. This is the standard IEC 31010:2009 [21], where there are some of the methods of modelling the uncertainty.

The above definition of risk (ISO/IEC 73:2009) relates this concept to effects of uncertainty on an organization's objectives and on their realization. The objectives may relate to various aspects within the organization, such as: finances, health protection and safety, environment protection, etc., or they can be related to different levels in an organization, such as strategic, overall organizational objectives, a program, project, product or process objectives.

If we go back to the issue of EU technical legislation, i.e. to the requirements from the New Approach directives, we can state the facts that follow. The objectives that are the subject of the analyses are related to products safety and to project of product design and development by the manufacturer. The objectives in general form are defined in the New Approach directives, i.e. in adequate standards for products, if such standards exist.

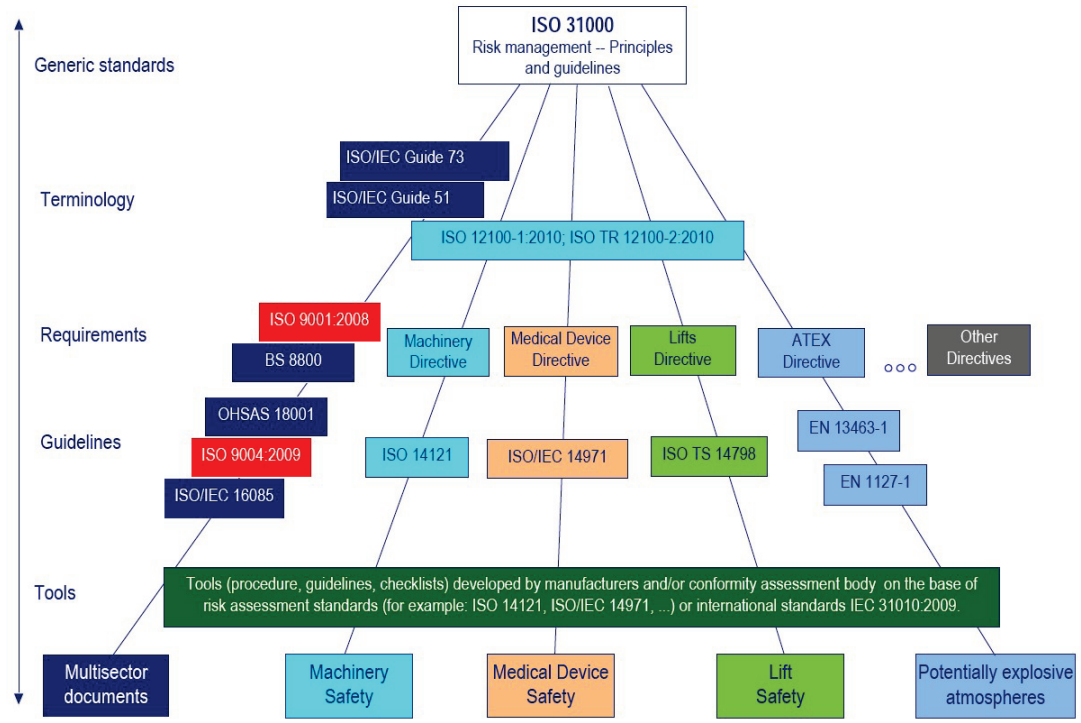

Figure 3 Hierarchy structure of standards in the risk management field, of importance in implementing the EU technical legislation (Adjusted on the basis of [22])

The concept of standardization in the field of risk, implemented by the International Organization for Standardization ISO and European standards bodies (CEN and CENELEC) has got the hierarchical structure of standards, as depicted in Figure 3. The concept starts from the fact that successful implementation of risk management in any organization requires a standards structure which sets up from general standards and through the standards defining terminology to standards in which risk analysis and assessment requirements are set for individual business processes and/or functions, and further on to standards in which there are guidelines directing about how to execute these analyses and assessments, and finally, there are structures defining the tools to be used in the risk analyses and assessments. Fig. 3 depicts complete hierarchy structure of international and regional standards in the field of risk management, which are of importance for implementing the New Approach directives.

At the highest generic level, there is the standard ISO 31000:2009 [13] which provides for general instructions and principles for developing and implementing risk management in any organization. In the following level, there are the standards and guidelines incorporating the vocabularies of terms. These are ISO/IEC Guide 73:2009 [17] and ISO/IEC Guide 51:1999 [23] standards.

ISO/IEC 73:2009 provides a basic vocabulary of the definitions of generic terms related to risk management. It aims to encourage a mutual and consistent understanding, a coherent approach to the description of activities related to risk management, and use of risk management terminology in the processes and frameworks dealing with the management of risk.

This group of standards defining the terms might also be extended by standard ISO 12100-1:2010 [24], expressing the basic overall methodology to be followed when designing machinery and when producing safety standards for machinery, together with the basic terminology related to the philosophy underlying this work. Although the purpose of this standard is to advance the machinery designing process, it can be successfully used in designing other technical products, such as lifts, medical devices, etc.

The requirements for technical products safety are given in the New Approach directives. They are defined in a general form so that they cannot become obsolete so quickly. From the risk point of view, the requirements defined in such a manner represent the risk management objectives in the process of product development related to the safety of the products.

In the course of product development, designers have a dilemma of how to determine if a product is safe or not, i.e. how to execute the risk analysis and assessment and how to improve the design solution on the basis of this. It is difficult to determine in practice the safety of a non-

standardized product if there is no adequate reference with respect to which it can be done. In some sectors, it is not justifiable nor is it practical or economically viable to standardize all product types, as new types are constantly being developed, and most often the unique ones (as in some of the fields of the machinery sector). In addition, development of new products in some fields is so accelerated that some of the products go ahead of standardization. In some sectors, it is not even possible to implement standardization due to various circumstances.

In response to this problem, the European Commission has initiated with CEN the development of generic harmonized standards enabling the systematic approach and providing the guidelines for: (1) identification of hazards; (2) risk assessment due to these dangers, and (3) assessment of acceptability of the selected safety measures.

Thus, a set of generic standards ensued for assessing risks in the New Approach directives, such as:

- ISO 14121-1:2007 for machines products [25]
- EN ISO 14971: 2002 for medical products [26].
- ISO TR 14798:2006 for lifts [27]
- EN 1127-1:2007 [28] and EN 13463-1:2009 [29], for the area of explosion prevention, etc.

From the standpoint of product safety, these standards serve as guidelines on how to conduct the risk analysis and assessment. Thus, as it is depicted in Figure 5, they have got a dual role. On the one hand, they serve as the tool (guidelines) used by designers and engineers in analysing and assessing the level of safety of design solution in the course of product development process, while on the other hand they are also the tool for the organization's staff and/or conformity assessment body in assessment whether a product satisfies the requirements of directives and/or harmonized standards, i.e. whether they possess satisfactory levels of safety.

At the lowest level of the standards structure hierarchy, there are the tools developed as independent standards, such as, for example, ISO/IEC 31010:2009 [21] which provides a large number of techniques that can be applied in risk assessment. In addition to the standards serving as tools, organizations very often also develop specific tools in which the risk assessment methodology given in some of the standards, such as for instance ISO 14121:2007, is adjusted to products and business practice present in that particular organization. These tools are presented in the form of various procedures, instructions or, most often, in the form of checklists.

3.2 Standard ISO 31000:2009

Standard ISO 31000:2009 was published on November 15th, 2009, together with standard ISO/IEC Guide 73. It can be applied in a portion of, or in the whole organization, regardless of whether it is a private, public or state-owned organization, association or a group of individuals.

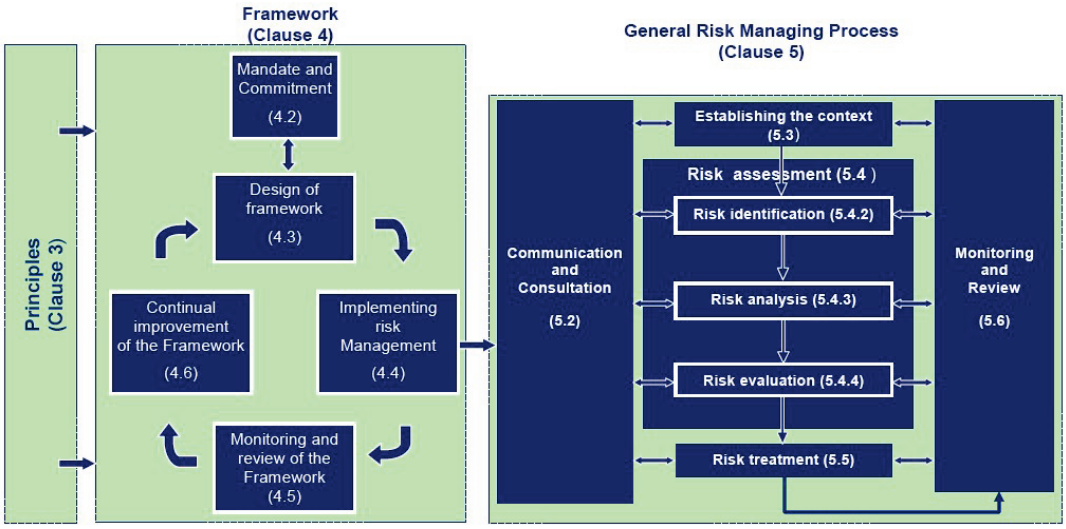

Figure 4 Relationships between the risk management principles, framework and process (ISO 31000:2009)

This international standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

The generic approach described in this international standard provides the principles and guidelines for managing any type of risk, whatever its nature, whether having positive or negative consequences in a systematic, transparent and credible manner and within any scope and context [30]. It suggests risk management principles, frameworks, processes and activities that should be followed to help organizations better meet their goals and objectives. The basic clauses of this standard define the following (Fig. 4):

- risk management principles (Clause 3),
- risk management infrastructure, by defining the framework (Clause 4) and
- general process for managing risks (Clause 5)

In order for risk management to be effective, the organization has to integrate the risk management principles into its business practice. ISO 31000 (Clause 3) contains 11 key principles, implementation of which enables risk management positioning as one of fundamental processes on which the organization's success depends. These principles offer the basis for defining and implementing the ERM program according to the specific needs of any organization.

In the Clauses 4 of the standard ISO 31000, the risk management framework is presented. This clause de-

scribes the necessary components of the framework for managing risk and the way in which they interrelate in an iterative manner, as shown in Fig. 4 (Framework). This framework is not intended to prescribe a management system, but rather to assist the organization to integrate risk management into its overall management system. Therefore, organizations should adapt the components of the framework to their specific needs.

The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organization at all levels. The "Plan, Do, Check, Act" cycle of continuous improvement is used as the basis for a risk management framework and associated risk management processes. Organizations adopting this approach will design, implement, monitor and review their risk management framework and take remedial action where necessary. A company's ERM should be continuously improved, typically on an annual basis.

The framework assists in managing risks effectively through the application of the risk management process (see Clause 5 ISO 31000:2009) at varying levels and within specific contexts of the organization. There may be thousands of such processes found in an organization. As an example of the processes for managing risk are those for risk assessment in the New Approach directives.

The framework ensures that information about risk derived from these processes is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels (ISO 31000).

The risk management process should be (ISO 31000):

- an integral part of management,
- embedded in the culture and practices, and
- tailored to the business processes of the organization.

A model of the process for managing risk is shown in Fig. 4 (General Risk Management Process). It comprises the activities described in the points 5.2 to 5.6.

Although this International Standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed [31; 9].

While other ISO standards can be used for certification, ISO 31000 is non-certifiable but it does provide guidance on best practices.

3.3 Technical product risk assessment integration into the ERM according to the ISO 31000:2009

Standard ISO 31000:2009 defines one of possible risk management models in the enterprise (ERM). The model has got several significant advantages with respect to other models, according to Kevin Knight [31], who was one of the driving forces behind these standards:

"ISO 31000:2009 is clearly different from existing guidelines on the management of risk in that the emphasis is shifted from something happening – the event – to the effect of uncertainty on objectives. Every organization has objectives – strategic, tactical and operational – to achieve and, in order to achieve these objectives, it must manage any uncertainty that will have an effect on their achievement.

ISO 31000:2009 sets out principles, a framework and a process for the management of risk applicable to any type of organization in public or private sector. It does not mandate a "one size fits all" approach, but rather emphasizes the fact that the management of risk must be tailored to the specific needs and structure of the particular organization."

Standards structure of the ERM mode as defined in standard ISO 31000:2009, is based on the following facts (Fig. 5):

- The organization's management is responsible for risk management framework development, implementation and continual improvement. This implies development and maintenance of an adequate organizational structure with clearly defined authorizations and responsibilities of key protagonists. The implemented risk management framework, as well as other management systems, has to be the subject of continual evaluations (most often once a year) on the basis of which necessary improvements are defined;
- The framework structure is given in Clause 4 of the standard. It has to be integrated into the existing organization's management system structure (QMS – ISO 9001, EMS – ISO 14001, ISMS – ISO 27001 etc.), i.e. into the structure of the integrated management system;
- The risk management principles given in standard ISO 31000:2009 have to be embedded into the organization's integrated management system, i.e. into the structure of the risk management framework;
- Structure of the general processes model for managing risk is given in the standard (Clause 5). These processes, of which there may be thousands at all the organizational levels and functions, are integrated into the ERM framework structure through its implementation (Clause 4.4).
- All managers and employees who take decisions have to be made familiar with the general and/or specific processes for risks management and with the way in which to include the analysis results and risk assessment into the procedure of taking decisions, regardless of whether the decisions are taken at the strategic, tactical or operative levels.

If we return to the risk assessment required by implementation of the New Approach directives on actual technical products, the following conclusions can be made. Risk assessment in such cases is, on the one hand the constituent part of the development process and on the other hand the constituent part of product conformity assessment conducted by the organization itself and/or the body for conformity assessment. The model of a possible integration of this risk assessment in the New Approach Directives into the ERM structure is given in Fig. 5.

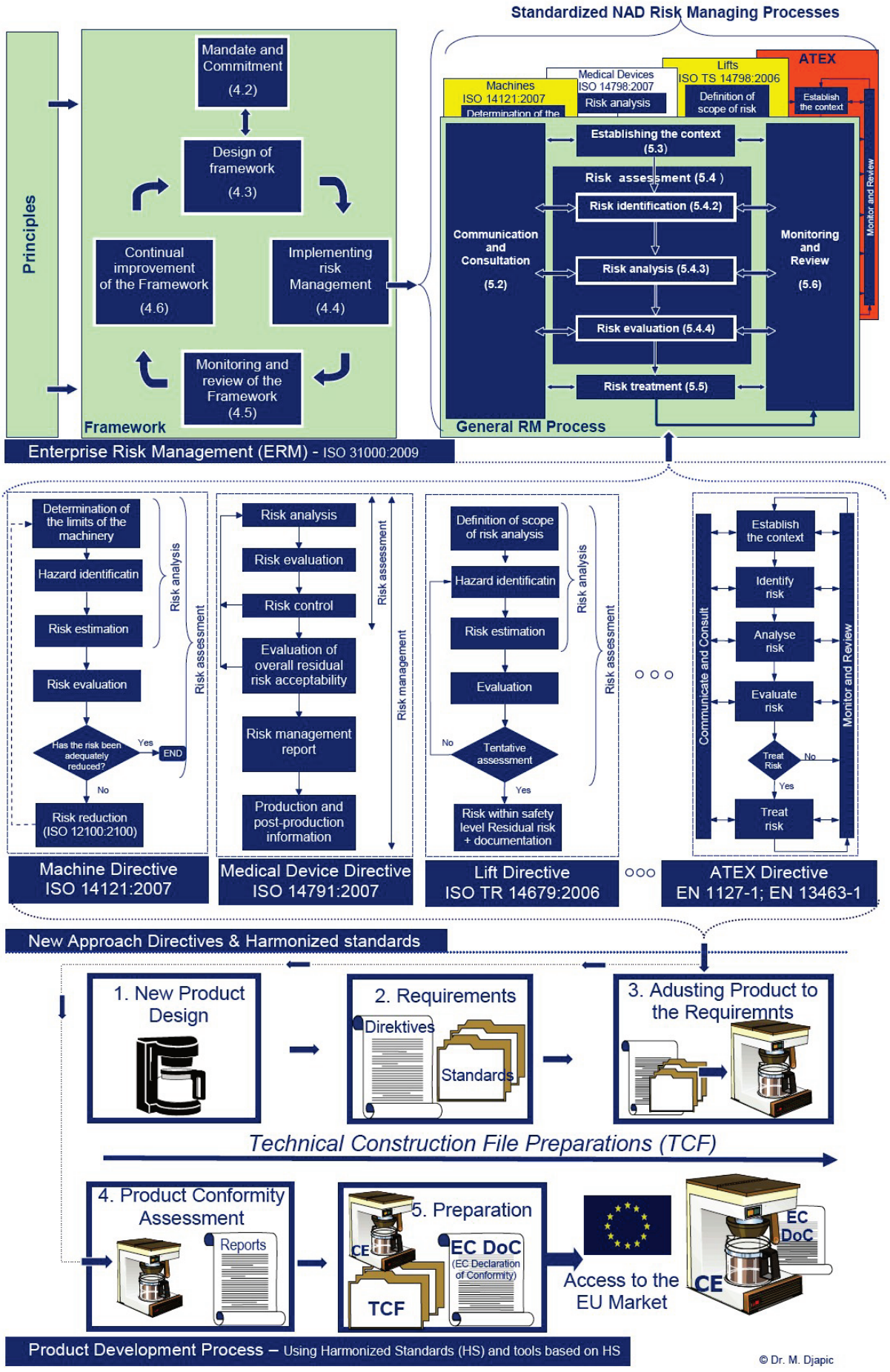

Figure 5 Integrating risk assessment in New Approach directives into ERM model, according to standard ISO 31000:2009

Several important facts can be observed from Fig. 5:

- The organizations wishing to improve the procedure of bringing decisions at all the hierarchy levels and all functions, have to implement some of the ERM models. One of these models is given in the international standard ISO 31000:2009.
- Risk assessment of technical products is the constituent part of their design and development process. It is conducted according to the requirements of directives, i.e. of harmonized standards developed and published for that purpose. Thus, the risk assessment of machinery products is done according to standard ISO 14121:2007, and that of medical devices according to standard ISO 14798:2007, etc. This risk assessment is integrated into the ERM framework through its implementation, as depicted in Figure 5. If there is no adequate harmonized standard according to which to perform the risk assessment for certain technical products, there remains available to the designers the general structure of the process for managing risks given in standard ISO 31000:2009 (Clause 5).
- At the operational level, in the course of product conformity assessment, as shown in Figure 5, various tools are used in the form of checklists in which the risk assessment methodology, given in harmonized standards, is adjusted to the actual products in question. Each conformity assessment body develops these tools according to its own needs.

It is important to point out that one of intended purposes of standard ISO 31000:2009 is to harmonize risk management processes in the current and future standards. It is to offer the joint approach to the standards treating specific risks and/or sectors and not to replace those standards. This means that this standard, although developed in 2009, does not replace the standards for specific risks and/or sectors that were developed earlier, such as for example ISO 14121:2007, but it only has to serve as the leading idea in harmonizing these standards on occasions of future revisions. This only points out to the fact that development of the risk management standards has not developed in logical sequence, i.e. the general generic ERM standard and terminology standard were not developed first, and then followed by standards for specific risks, but the business practice has imposed that just the standards treating risks in specific fields were developed first. It is certain that future development of the standardization system in this field will establish a harmonized standards structure, as shown in Fig. 3.

4 Conclusion

European Union has accomplished, through introducing New Approach to technical harmonization and standardization, a breakthrough in the field of technical products safety and in assessing their conformity, in such a manner that it integrated products safety requirements into the process of products design and development. This is achieved by quantifying risk levels, in the course of the designing process, with the aim of determining the scope of the required safety systems, where the safety requirements are preventively considered during the designing process. In that respect, the European Commission has given a task to CEN to develop generic standards to serve as guidelines and to alleviate technical products' risk assessment in the phase of assessing their conformity.

On the other hand, contemporary business practice has imposed the request for quality improvement in the process of taking decisions, which inevitably brought about the request to analyze and assess the risks for each business objective of the organization. This resulted in the occurrence of several standards/frameworks in which the models of a holistic (integrated) risk management in enterprises have been presented. A new "buzz words" - Enterprise Risk management (ERM) has emerged, which encompassed all of that.

Standard ISO 31000:2009 *Risk management - Principles and guidelines*, defines one of the ERM models. Pursuant to this standard, the ERM model is based on (1) eleven risk management principles, (2) framework within which the P-D-C-A cycle is integrated, and (3) the general process for managing risk. The risk management framework is the management system that defines and describes how risk management will be embedded and executed at all levels of the organization. An effective framework is critical to the success of ERM in whatever business. Framework does not exist separate from other organization's management systems, but its integration into the existing management systems structure is requested. In connection with the implementation of the framework (item D from the PDCA cycle), the standard proposed a general process structure for managing risk in enterprises. There may be thousands of such processes, depending on the organization's size and line of activity.

The processes of risk assessment required by the New Approach Directives refer to a group of these processes. Since risk assessment in these processes is defined in the harmonized standards which appeared prior to the ERM model (ISO 31000:2009), the paper gives a model on how they are integrated into the holistic approach of the enterprise risk management (ERM). In many of the New Approach directives there are no harmonized standards for risk assessment, so that manufacturers in such cases can use the general model of risk management processes given in Clause 5 of the ISO 31000:2009 standard.

5 References

[1] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC Official Journal of the European Union L 154/24/2006

[2] Djapic, M.; Lukic, Lj.; Ivanovic, S. Machine Safety Requirement Integration in the Process Designing – Risk Assessment in the Machinery Directive. // Journal of IMK-14 Research and Development, Institute IMK 14. October, Krusevac, Vol. XV, No. (30-31), 1-2(2009), pp. 43-58, ISSN 0354-6829.

[3] Guide to the Implementation of Directives Based on the New Approach and Global Approach, by the European Commission (Blue Guide), November, 2011, http://ec.europa.eu/enterprise/policies/single-market-goods/documents/blue-guide/

[4] Djapic, M.; Zeljkovic, V.; Vojinovic, M. Machine Tools Harmonization with EU Technical Legalizations Requirements. // International Journal for Quality Research. 2, 3(2008), pp. 171-177.

[5] Baron, P.; Dzubakova, I.; Mikita, J. Parallel approaches in the pre-manufacturing phase-process of technical preparation of manufacture and risk assessment of technical systems. // Tehnicki vjesnik-Technical Gazette. 17, 3(2010), pp. 377-381.
[6] Ceric, A.; Marcic, D.; Ivandic, K. A Risk-assessment Methodology in Tunneling. // Tehnicki vjesnik-Technical Gazette. 18, 4(2011), pp. 529-536.
[7] AIRMIC, Alarm, IRIM, A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000, The Public Risk Management Association, London, UK, 2010.
[8] Erben, E. B. Risk Management Standards – role, benefits & applicability – 2nd European Risk Conference, Università Bocconi, September 11th & 12th, 2008.
[9] Leitch, M. ISO 31000:2009 – The New International Standard on Risk Management. // Risk Analysis. 30, 6(2010), pp. 887-892.
[10] Purdy, G. How to bring your ERM Framework in line with ISO 31000, LexisNexis 5th Annual Risk Management Conference, Sydney, Australia, 2008.
[11] Purdy, G. ISO 31000:2009 – Setting a New Standard for Risk Management. // Risk Analysis. 30, 6(2010), pp. 881-886.
[12] Shortrees, J. Enterprise risk management and ISO 31000. // The Journal of Policy Engagement. 2, 3(2010), pp. 8-10.
[13] ISO 31000:2009 Risk management -- Principles and guidelines, International Organization for Standardization, www.iso.org
[14] Lindholm, G. General principles of the New Approach legislation, Workshop of the Pressure Equipment Directive, Directorate General for Enterprise European Commission, Riga, 27-28. November 2003.
[15] International Organization for Standardization, Certification and related Activities, 1992.
[16] Moeller, R. R., COSO Enterprise Risk Management, Understanding the New Integrated ERM Framework, John Wiley & Sons Inc., Hobaken, New Jersy, 2007, ISBN 978-0-0471-74115-2.
[17] ISO/IEC Guide 73 Risk Management - Vocabulary - Guidelines for use in standards, International Organization for Standardization, www.iso.org
[18] Standards Australia & Standards New Zealand Committee OB/7 on Risk Management, Risk management, AS/NZS 4360:2004, www.saiglobal.com
[19] Aven, T. Perspectives on risk in a decision-making context – Review and discussion. // Safety Science. 47, (2009), pp. 798-806.
[20] Aven, T. A holistic framework for conceptualizing and describing risk. // In Kolowrocki, K., Soszynska, J. & Zio, E. (eds.) Proceedings SSARS 2010. // Journal of Polish Safety and Reliability Association. 1, (2010), pp. 7-14.
[21] IEC 31010:2009, Risk management – Risk assessment techniques, International Electrotechnical Commission, www.iec.org
[22] CEN/BT WG 160, Implementation of Risk Assessment in European Standardization, Annex 3, 2005
[23] ISO/IEC Guide 51:1999 Safety aspects – Guidelines for their inclusion in standards. International Organization for Standardization, www.iso.org
[24] ISO 12100-1:2010 Safety of machinery – Basic concepts, general principles for design, Part 1: Basic terminology, methodology, International Organization for Standardization, www.iso.org
[25] ISO 14121-1:2007 – Safety of machinery – Risk assessment – Part 1: Principles, International Organization for Standardization, www.iso.org
[26] ISO 14971:2007 - Medical devices -- Application of risk management to medical devices, International Organization for Standardization, www.iso.org
[27] ISO TR 14798:2006 Lifts (elevators), escalators and moving walks -- Risk assessment and reduction methodology, International Organization for Standardization, www.iso.org
[28] ISO EN 1127-1 2007 Explosive atmospheres - explosive prevention and protection basic concepts and methodology, International Organization for Standardization, www.iso.org
[29] BS EN 13463-1:2009, Non-electrical, equipment for use in potentially explosive atmospheres, Part 1: Basic method and requirements, British Standard, www.bsi.org
[30] Knight, K. Future ISO 31000 standard on risk management, ISO Management Systems, July-August, 2007, pp. 8-11.
[31] Knight, K. ISO 31000 and the Icelandic volcano crisis, International Organization for Standardization, http://www.iso.org/iso/iso-focus-plus_index/isofocusplus_online-bonus-articles/isofocusplus_bonus_iso31000-icelandic-volcano-crisis.htm (September 2011)

Authors' addresses

Dr. Mirko Djapic
University of Kragujevac
Faculty of Mechanical Engineering Kraljevo
Dositejeva 19, 36000 Kraljevo, Serbia
E-mail: mdjapic@yahoo.com; djapic.m@mfkv.kg.ac.rs

Dr. Ljubomir Lukic
University of Kragujevac,
Faculty of Mechanical Engineering Kraljevo,
Dositejeva 19, 36000 Kraljevo,
Serbia
E-mail: ljubomir.lukic@abs.rs; lukic.lj@mfkv.kg.ac.rs

Dr. Predrag Popovic
Institute Vinca,
BIRO-Biro for certification
Mike Alasa 12-14, Vinca, Belgrade
Serbia
E-mail: biro@vinca.bg.ac.rs