R&E-SOURCE http://journal.ph-noe.ac.at
Open Online Journal for Research and Education
Special Issue #4, December 2015, ISSN: 2313-1640

The Safety Analysis for the Safety-Critical Processes

Veronika Stoffová[*], *Milan Štrbo*[†]

Abstract

Ensuring a safety of technology process is very important. Therefore it is necessary to include the safety analysis into the developing process of automatic control system and also to curricula at technology universities and high schools. The aim of the article is to propose a methodology for implementing a model-driven safety analysis of dynamical technology systems. The safety analysis is performed in the process of control system development, especially aiming at safety-critical processes of system operation. The methodology was divided into a few steps. The individual steps of the methodology are carried out in a hierarchical sequence. The roles of individual methodology steps are detailed in the paper. The principle of safety-critical process monitoring based on models is also described in the presented article.

Die Sicherheitsanalyse für die sicherheitskritischen Prozesse

Gewährleistung der Sicherheit von Technologie-Prozess ist sehr wichtig. Deshalb ist es notwendig, die Sicherheitsanalyse in den Entwicklungsprozess der automatischen Steuerung miteinzubeziehen und dies auch in der Lehre an Technischen Universitäten und Hochschulen zu integrieren. Ziel des Artikels ist es, eine Methodik zur Realisierung einer modellgetriebenen Sicherheitsanalyse von dynamischen technischen Systemen vorzustellen. Die Sicherheitsanalyse wird im Prozess der Steuerung der Systementwicklung durchgeführt, insbesondere mit dem Ziel, sicherheitskritische Prozesse des Systembetriebs aufzudecken. Die Methode wurde in mehrere Schritte unterteilt. Die einzelnen Schritte der Methode sind in einer hierarchischen Reihenfolge. Diese Schritte sind in dem Beitrag beschrieben. Das Prinzip der sicherheitskritischen Prozessüberwachung, basierend auf Modellen, wird auch im Artikel beschrieben.

Keywords:	*Schlüsselwörter:*
safety analysis, dynamic systems, technology control process safety-critical processes	Sicherheitsanalyse, Dynamische Systeme, Technologie Steuerungsprozess, Sicherheitskritischen Prozessen

1 Introduction

The automation of continuous-discrete technical processes greatly depend on the implementation functions of control and regulation. What more, it also depends on automatic control according to the operating rules. The engineering-technical applications are deployed to the monitor process which are often mathematical models, in order to obtain an accurate description of the technical equipment. However, especially for complex

[*] Trnava University in Trnava, Faculty of Education, Department of Mathematics and Informatics, Priemyselná 4, 917 01 Trnava, Slovakia
E-mail: NikaStoffova@seznam.cz

[†] Trnava University in Trnava, Faculty of Education, Department of Mathematics and Informatics, Priemyselná 4, 917 01 Trnava, Slovakia
E-mail: milan.strbo@truni.sk

dynamic systems, the construction of a mathematical model for the control is associated with many difficulties. The main problem is that the parameters of the model are unknown and therefore for the analytical procedures must be used an estimate of state respectively an estimate of parameters. On the basis of these problems are also taken into account qualitative procedures for complex systems. The qualitative models may not be accurately reflect internal physical connections, in models are include only those situations when something "does". The qualitative model distinguishes these situations and allows the characterization of complex systems. The disadvantage of qualitative models is mainly the fact that the dynamic properties cannot be at all or only very inaccurately described. However, this is a necessary condition for the control of dynamic properties of the system. For this reason, we propose to use for safety analysis of the complex dynamic systems the combination of both forms of the model, therefore the qualitative models for assessing the complexity of systems and quantitative (mathematical) models for description of the dynamics (Manz, 2004) (Štrbo, 2013).

2 The proposal of the safety analysis

The overall proposal of the course of the safety analysis is shown in the figure 1. The proposal The of methodology is illustrated using ordinary UML state diagram consisting of a sequence of six successive steps. After the execution of each step of the analysis is performed verifying of achievements. If weaknesses in the proposed models are revealed during the verification, safety analysis process continues to the point: „Removing and reducing risk“, and then return to the point: „Modelling a safety-critical process". The full content of the tasks for various steps of the safety analysis is described in this article later.

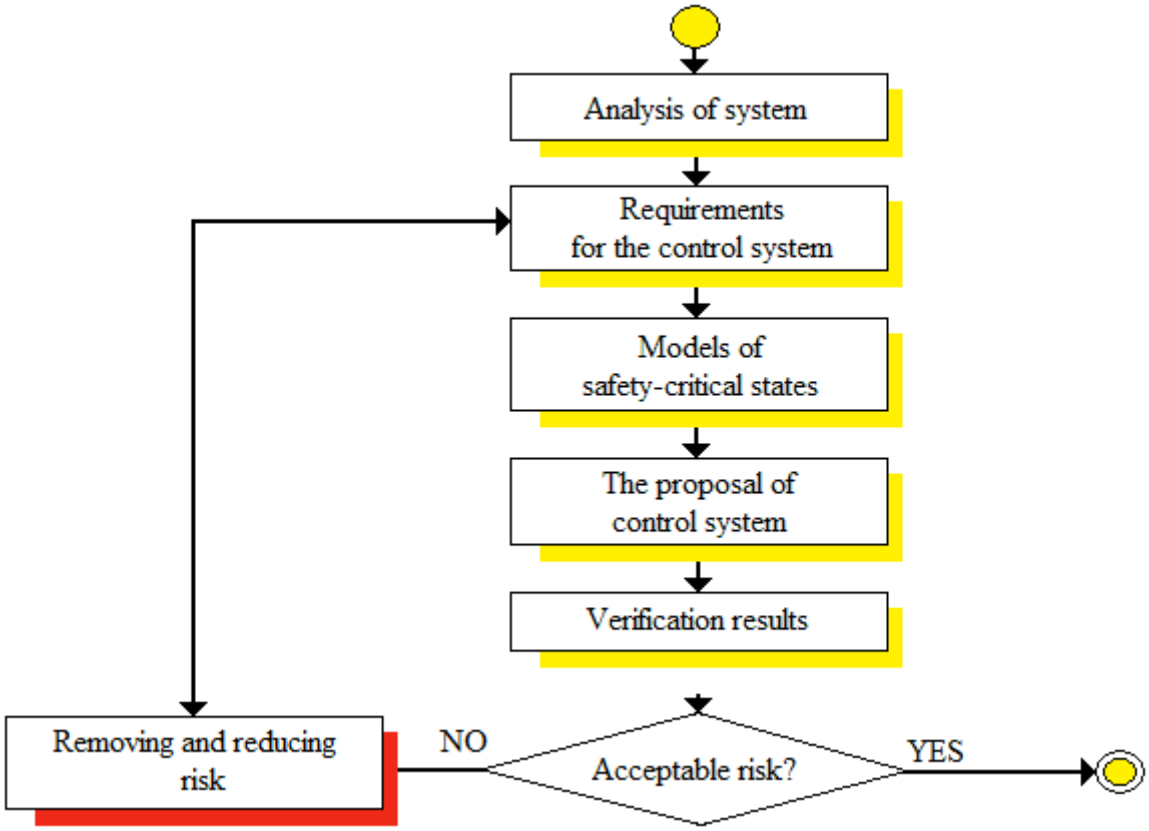

Fig. 1: The proposal of process for safety analysis

3 Processes of safety analyses

3.1 Analysis of system

The content of this step is to analyze the dynamic system with a focus on the implementation of the safety analysis. It means to become familiar with the system and its features and identify all possible states of the system during operation. It is necessary to analyze the actual terms and basic operating parameters respectively conditions. It is closely related to the analysis of limitations in individual states, analysis of deficiencies, analysis of risks and all available resources of the system. The selection and analysis of the operating states, which are safety-critical for a system, are very important steps of analyses. To define whether these states are deterministic or stochastic is also important. For the critical states is necessary to done the select of resources information. These will provide information to the operating personnel about the process of these states. It is also necessary to define the inputs for individual states, mutual relations between states and the characteristic of states on the output.

3.2 Requirements for the control system

The aim of this step is to establish requirements for the safety analysis respectively requirements for control process in terms of origin, course and evaluation of critical situations (faults). This can be understood as the determination of the individual requirements for hardware and software of the control system for safety-critical situations that we get an analysis of conditions obtained in step one. Each process has some set of the states. In this step, we will work only with safety-critical states. By detailed analysis of these states we obtain the requirements for measurement, control functions during the states or requirements of the actuators controllers. We must take into account all the relevant standards and the implementation safety-critical states to criteria of the SIL (Safety Integrity Level). The content of this step is also the selection and analysis methods of observation of the processes (estimate of the states). For determination of the methods and processes for safety analysis in deterministic states the Luenberger´s observer and in stochastic Kalman´s observer (filter) are suitable. It is necessary to the mention the Top-Down method, which allows us to decompose a system from a global perspective to the individual subprocesses (Štrbo at al., 2014).

3.3 The models of safety-critical states

In this step, we will describe the critical states of the system through models. The aim is to develop qualitative and quantitative models within the general description of the system. For the development of qualitative models of the individual processes we use fuzzy logic, possibly we can to use description through causal networks. Quantitatively, mathematical models we develop by using differential and difference equations. The structure of these models we can orient into UML (Unified Modelling Language) diagrams. It is also necessary to carry out the synthesis of these models, evaluate their effectiveness and make the validation of these models. To verify the accuracy of models, need to be verified it by simulation.

3.4 The proposal of the control system

The result of this step will be conceptual design of the structures system for safety analysis (control of process) of the dynamic process. It is important to evaluate all possible solutions, opportunities and strategies in terms of fulfilment expectations and in the terms of achieving the specific goals. We carry out the design and analysis of our solutions. In conclusion, we select the final solution which we have selected on the basis of certain criteria on system and we get a real design of hardware and software of control system.

3.5 The verification results

The obtaining of the solution will be verified by simulation. We compare the results obtained with the system requirements. We establish the criteria for validation and verification of the proposed solutions. Then we

perform validation and verification solutions based on these criteria. Finally we evaluate the results obtained for long-term and for short term and also evaluate the effect of the proposed solutions with respect to future possibilities. If the validation process finds deficiencies in the proposed solutions, so the process of safety analysis returns to the step "Requirements for the control system".

3.6 Removing and reducing risk

After a risk analysis was made is necessary to design proper mechanisms to removal and reduce risk. This way remove a hazard completely or help us reduce the intensity of the hazard to an acceptable level. The type of protective equipment must be safe for operation of safety-critical systems as well as for employees and the surrounding environment. When we have the recommended protective equipment, workers must be trained and they must familiar manner of their use. It is important that additional safety measures proposed in this step was sufficient. The mechanism for the removal respectively reduction of risk is illustrated in Fig. 2

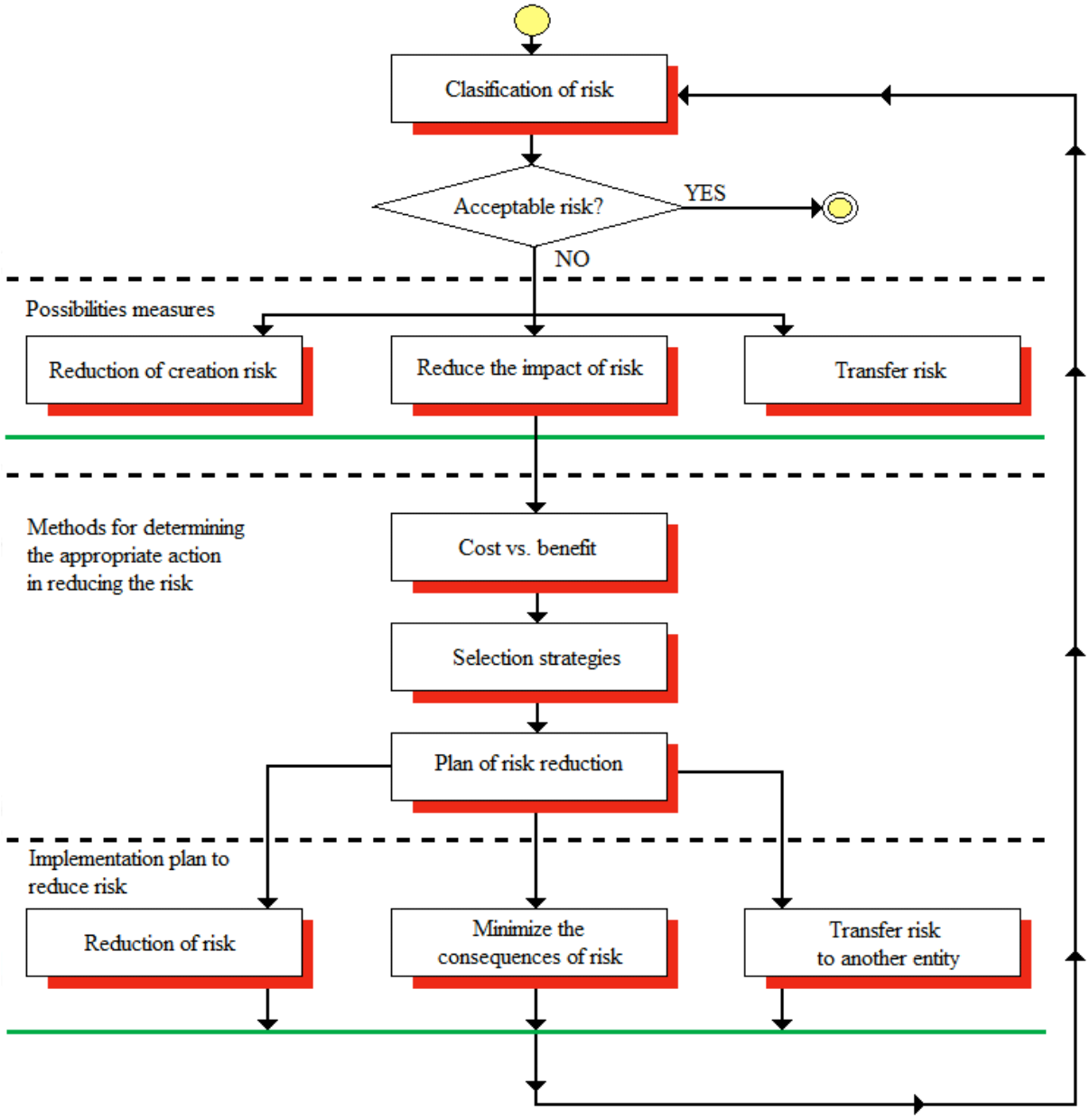

Fig. 2: The proposal of procedure on risk elimination

4 Developing a model for on-line monitoring of processes

The question of using a combination of qualitative and quantitative modelling of controlled processes for safety analysis of complex systems is appropriate. SQMD is a method for modelling dynamic systems and it uses currently a combination of these two forms of modelling. The method uses a hybrid model for monitoring and detecting of real-time. The hybrid model includes qualitative and dynamic elements, and combines the advantages of both methods. Thus we can imagine on-line monitoring and diagnostics to detect and locate faults in complex dynamic systems. The main advantage of the safety analysis by method SQMD is easy modelling of complex dynamic systems.

In order to develop a suitable method for monitoring of dynamical technology systems following objectives must be taken into account:

1 - modelling dynamical systems,

2 - observing dynamical systems,

3 - analysing errors of dynamical systems.

Errors and failures of hardware components, software errors or defects caused by construction disregarding operating conditions may lead to a dangerous situation in the operation of technical processes. The role of an appropriate process model is to provide quantitatively or qualitatively measurable parameters in relation to the characteristics of the system in order to detect deviations in the process in real-time. Models to be deployed in the monitoring process do not often comply with a simple description of the reality. Besides describing the desired operation mode, for monitoring, it is necessary to additionally identify all possible faults in the real process enabling them to be taken into account for the model. In this way, models for the desired operation states and corresponding models for failure operation states are created. Models for the required operation states are deployed in monitoring and subsequently they are compared with the real values. If the value of the models does not match the reality, it is considered to be an error. In this case, type and location of the error is determined by models of error operation modes. Considering all the possible errors in the model is therefore an important task of designing models (Fröhlich, 1996).

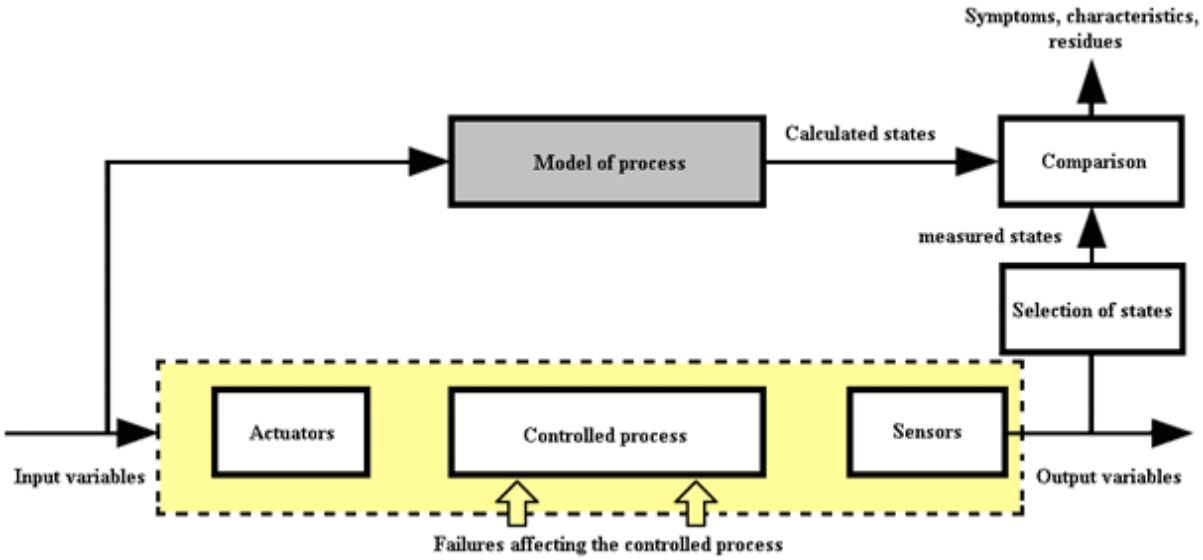

Fig. 3 Principle of control based on the model of the real process

Figure 3 demonstrates monitoring based on the model. Model of the process is conducted on-line, i.e. to the parallel controlled process. According to the input data the behaviour of the real process can be determined using output values (measured state). The measured behaviour is affected by the parallel assigned model with the same input data. The determined (calculated) states are compared with the measured outcomes and from

this comparison symptoms, characteristics or residues important for error detecting are derived (Lauber, Göhner, 1999), (Štrbo, 2013)..

5 Conclusion

The aim of this article was the proposal of the safety analysis in context of the risks in the process of development of the control systems for the complex dynamic technology systems. The proposal of the process is shown by activity UML diagrams. Furthermore, we have reported a detailed description of the tasks for each step of the safety analysis. The process of the safety analysis begins with familiarizing yourself with the system on which is carried out the analysis. Then it goes through the requirements on the system, modelling of the individual states to the overall design of the control system for the system. In conclusion of our proposal does not lack verification of the results obtained.

References

[1] Fröhlich, P. (1996). Überwachung verfahrenstechnischer Prozesse unter Verwendung eines qualitativen Modellierungsverfahrens, Institut für Automatisierungs- und Softwaretechnik (IAS), Universität Stuttgart, Dissertation, Universität Stuttgart.

[2] Lauber, P. Göhner (1999). Prozessautomatisierung 1, Band 1, 3. Auflage, Berlin Heidelberg, Springer-Verlag

[3] Manz, S. (2004). „Entwicklung hybrider Komponentenmodelle zur Prozessüberwachung komplexer dynamischer Systeme“, January 2014, Forschungsbericht Institut für Automatisierungs- und Softwaretechnik, Universität Stuttgart

[4] Štrbo, M. (2013): *Komplexná modelovo-orientovaná bezpečnostná analýza rizík v procese návrhu informačných systémov pre bezpečnostne-kritické procesy.* [PhD theses] - Slovenská technická univerzita v Bratislave. Materiálovotechnologická fakulta so sídlom v Trnave; Ústav aplikovanej informatiky, automatizácie a matematiky, Trnava: MTF STU, 2013, 137s.

[5] Štrbo, M. - Tanuska P. - Gese, A. Hagara, I. - Smolarik, L. (2014). Safety Analysis for Complex Dynamic Systems, Faculty of Materials Science and Technology, Slovak University of Technology in Bratislava