Safety Analysis for the Complex Dynamic Technology Systems and Removing of the Risks

Milan Strbo, Pavol Tanuska, Augustin Gese
Faculty of Materials Science and Technology
Slovak University of Technology in Bratislava Paulínska 16, 91724 Trnava, Slovakia
{milan.strbo, pavol.tanuska}@stuba.sk

Abstract. *The aim of this article is the proposal of the safety analysis for complex dynamic technology systems in process of the development of control system for safety-critical processes. The method of safety analysis depends on safety-critical states of system which are system are controlled by models. In our article we propose to use the method SQMD for modeling these states. Method SQMD combines qualitative and quantitative methods for modeling states and takes advantages of both methods.*

The proposal of safety analysis is shown by activity diagram. The article also includes the proposal of the removing and reducing risks.

Keywords. safety analysis, qualitative and quantitative models, method SQMD

1 Introduction

The automation of continuous-discrete technical processes greatly dependeds 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 dynamic technology systems, the construction of a mathematical models 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 dynamic systems. The qualitative models may not be accurately reflect internal physical connections, in these models are include only those situations when something "does". The qualitative model distinguishes these situations and allows the characterization of complex dynamic systems. The disadvantage of qualitative models is mainly the fact that the dynamic properties can not 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 quantitative (mathematical) models for description of the dynamics and qualitative models for assessing the complexity of systems. [1]

2 The control of processes and development of models

The question of using a combination of quantitative and qualitative modeling of controlled processes for safety analysis of complex dynamic systems is appropriate. SQMD is a method for modeling complex dynamic systems and it uses currently a combination of these two forms of modeling. The method uses a hybrid model for detecting and monitoring 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 dynamic systems. The main advantage of the safety analysis by method SQMD is easy modeling of complex dynamic technology systems. [5]

The control of complex dynamic technology systems takes into account these objectives:

1 - modeling of the complex dynamic technology system,
2 - observation of the complex dynamic technology system,
3 - error analysis of the complex dynamic technology system.

The errors and failures of the hardware components, software errors or errors in the proposal that have not been taken into account for the operating conditions may cause a dangerous situations in the operation of technical processes. The role of an appropriate model of process is to provide a qualitative or quantitative measurable parameters in relation to the properties of the system and from these we can in real-time detect deviations during the process. [2]

The models which should be deployed in controlling process often do not meet the requirements of a simple description of reality. With respect to the control process except for the description of the desired mode of the operation, it is necessary to identify all possible faults in the real process. In this way arise except models for the desired operating conditions also appropriate models for degraded modes of the operation. When checking are deployed the models for desired state, and these are compared these with the course of reality. As soon as a discrepancy is found between the model and reality, it is considered as an error. In this case, models of error operating modes determine the type and location of the error. An important task for the elaboration of the models is therefore taking into account all the possible errors in the model. [2]

In figure 1 is shown the principle of control loaded at the model. The process model is carried out on-line, i.e. parallel to the controlled process. Based on the input data is impossible to determine the behavior of the real process using output values (measured situation). This measured behavior is determined in parallel model with an associated of the same input data. The determined (calculated) situation are compared with measured and from this comparison are derived symptoms, characteristics or residues which are important to the detect errors. [3]

The tasks of the process control:

- examination of the current state from measured process signals and indication of the state for the operating personnel,
- examination of the failed subsystems caused by deviations from the regular operation and from these derived stimuli for actions performed by operating staff,
- output of the alarm messages for immediate outages,
- automatic protection of technical devices at hazardous or emergency situations,
- early detection of the emerging faults and outages. [4]

3 The proposal of the safety analysis

The overall proposal of the safety analysis for complex dynamic technology systems is shown in the figure 2. This process is divided into five steps. Concrete steps are *Analysis of system*, *Requirements for the control system*, *Models of safety-critical states*, *The proposal of the control system* and *Verification results*.

After the execution of each step of the analysis is performed verifying of achievements. The contents of the tasks for various steps of the safety analysis is described later in this article.

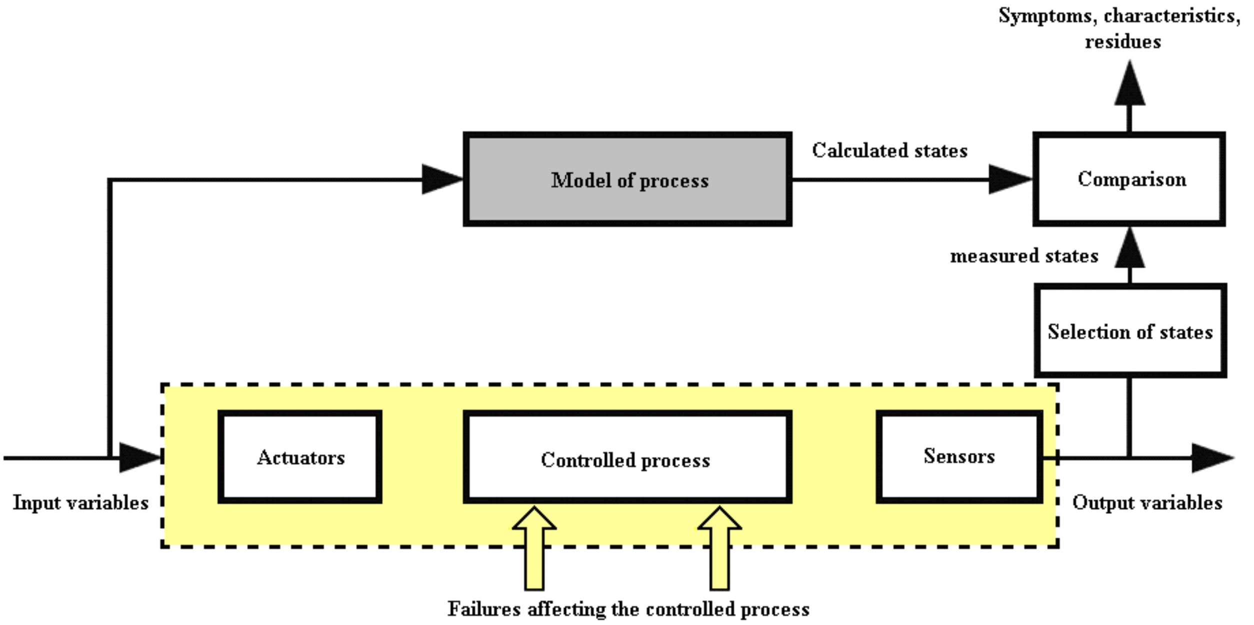

figure 1. The principle of control based on the model of the real process

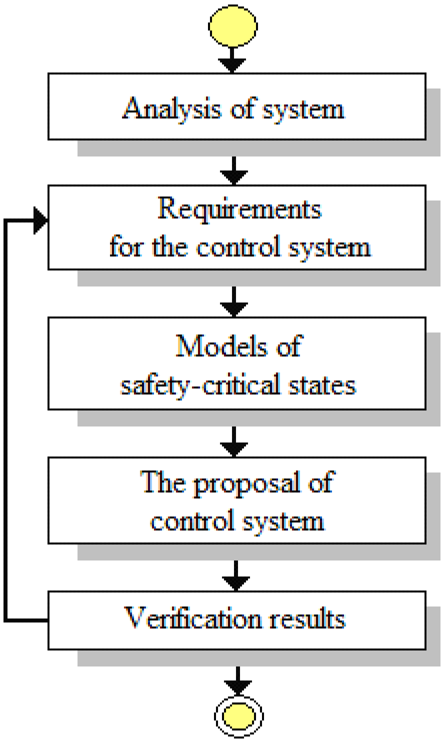
Analysis of system
Requirements for the control system
Models of safety-critical states
The proposal of control system
Verification results

figure 2. The proposal of safety analysis

4 The process of safety analysis

4.1 Analysis of system

The content of this step is to analyze the complex 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 conditions respectively parameters. 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, and determine whether these states are stochastic or deterministic. 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.

4.2 Requirements for the control system

The result 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 software and hardware 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). The use of the Kalman´s observer (filter) for stochastic states and the Luenberger´s observer for deterministic states. The determination of the processes and methods for safety analysis. 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.

4.3 The models of safety-critical states

In this step, we will describe the safety-critical states of the system through models. The aim is to develop quantitative and qualitative 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 will develop by using difference and differential equations.

The structure of these models we can orient into UML 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.

4.4 The proposal of the control system

The aim of this step is conceptual proposal of the structures system for safety analysis (control of process) of the complex dynamic technology system. It is important to evaluate all possible solutions, opportunities and strategies in terms of fulfillment expectations and in the terms of achieving the specific goals. We carry out the analysis and proposal 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 proposal of software and hardware for control system.

4.5 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 verification and validation of the proposed solutions.

Then we perform verification and validation solutions based on these criteria. Finally we evaluate the results obtained for short term and for long-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".

When we have the recommended protective equipments, workers must be trained and they must familiar manner of their use. Workers must be informed of the residual risks associated with the operation of the plant. It is important that additional safety measures proposed in this step was sufficient. The mechanisms for the reduction respectively removal of risk is shown in figure 3. [6]

5 The proposal of the reducing and removing of risks

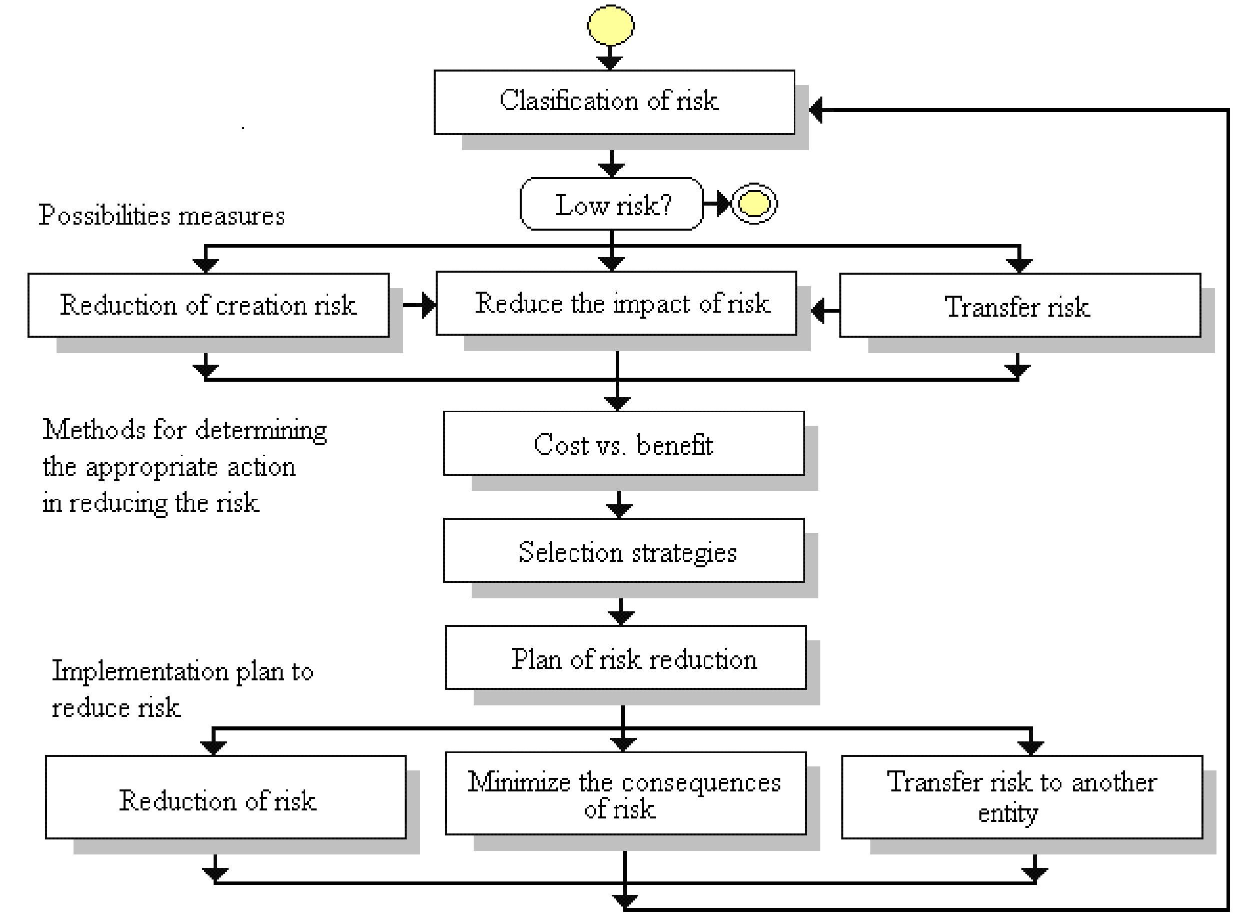
Clasification of risk
Low risk?
Possibilities measures
Reduction of creation risk
Reduce the impact of risk
Transfer risk
Methods for determining the appropriate action in reducing the risk
Cost vs. benefit
Selection strategies
Plan of risk reduction
Implementation plan to reduce risk
Reduction of risk
Minimize the consequences of risk
Transfer risk to another entity

figure 3. The proposal of procedure of risk elimination

After a safety analysis was made is necessary to proposal proper mechanisms to reduce and removal risks. These mechanisms remove a hazard completely or help us reduce the intensity of the hazards to acceptable values. We must achieve in order to eliminate all of hazards. The type of protective equipment must be safe for operation of safety-critical system as well as for employees and the surrounding environment. Safe work practices must be consistent with people's abilities. Information about the use of equipment must be sufficiently clear.

6 Conclusion

The content of article is the proposal of the safety analysis in context of the risks in the process of development of the control systems for the complex dynamic systems.

The proposal of the process is shown by activity diagrams in UML (Unified Modeling Language). 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, modeling of the individual states to the overall proposal of the control system for the system. In conclusion of our proposal does not lack verification of the results obtained. In conclusion of the article we proposed mechanisms for reducing and removing of risks.

References

[1] S. Manz, Entwicklung hybrider Komponentenmodelle zur Prozessüberwachung komplexer dynamischer Systeme“, Forschungsbericht Institut für Automatisierungs- und Softwaretechnik, Universität Stuttgart, Germany, 2004

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

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

[4] R. Lauber, P. Göhner: Prozessautomatisierung 2, Band 2, 1. Auflage, Berlin Heidelberg, Springer-Verlag, 1999

[5] L. Huraj, H. Reiser, VO Intersection Trust in Ad hoc Grid Environments. In: Fifth International Conference on Networking and Services (ICNS 2009), Valencia, Spain, IEEE Computer Society, April 2009

[6] M. Strbo, P. Tanuska, A. Gese, The proposal of preliminary hazard analysis for safety-critical control systems. In Infokommunikacionnyje technologii v nauke, proizvodstve i obrazovanii: 5. meždunarodnaja naučno-techničeskaja konferencija, Kislovodsk, Stavropoľ, 2 - 6 maja 2012. s. 162—167

[7] P. Schreiber, O. Moravcik, P. Tanuska, P. Vazan, R. Vrabel, M. Bartunek, P. Husar, Safety Distance by Simulation and Collision Avoidance on a Road´s Danger Zones, In Vol. 10 : 2012 International Conference on Affective Computing and Intelligent Interaction (ICACII 2012). Taipei, Taiwan, February 27-28, 2012. s. 326--331.

[8] A. Libosvarova, P. Schreiber, Fault tree analysis optimized by genetic algorithms, In International Doctoral Seminar 2013, Proceedings of the 8th International Doctoral Seminar (IDS 2013), Dubrovnik, 13 - 15 May 2013.

Európska únia
Európsky fond regionálneho rozvoja

This publication is the result of implementation of the project: “Increase of Power Safety of the Slovak Republic” (ITMS: 26220220077) supported by the Research & Development Operational Programme funded by the ERDF.

Operačný program VÝSKUM a VÝVOJ