RESEARCH PAPERS
FACULTY OF MATERIALS SCIENCE AND TECHNOLOGY IN TRNAVA
SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA

2013 Special Number

THE PROPOSAL OF THE PROCESS OF SAFETY ANALYSIS FOR COMPLEX DYNAMIC TECHNOLOGY SYSTEMS

Milan ŠTRBO, Pavol TANUŠKA, Augustín GESE

ABSTRACT

The aim of this article is the proposal of process of the safety analysis for complex dynamic systems in process of the proposal of control system for safety-critical processes. The method of safety analysis depends on various safety-critical states of system which are system are controlled by models. We propose to use the method SQMD for modeling these states. This method combines qualitative and quantitative methods of modeling states and takes advantage of both methods. The model of the proposal is shown in the diagram. The article includes detailed description of the tasks for each step of analysis.

KEY WORDS

complex dynamic system, qualitative model, quantitative model

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 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 quality 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 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

Milan ŠTRBO, Pavol TANUŠKA, Augustín GESE - Institute of Applied Informatics, Automation and Mathematics, Faculty of Materials Science and Technology, Slovak University of Technology in Bratislava, Paulínska 16, 917 24 Trnava, Slovakia, milan.strbo@stuba.sk, pavol.tanuska@stuba.sk, gese@stuba.sk

qualitative models for assessing the complexity of systems and quantitative (mathematical) models for description of the dynamics (Manz 2004).

THE DEVELOPMENT OF MODEL AND CONTROL OF PROCESSES

The question of using a combination of qualitative and quantitative modeling of controlled processes for safety analysis of complex systems is appropriate. SQMD is a method for modeling dynamic systems and it uses currently a combination of these two forms of modeling. 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 modeling of complex dynamic systems.

The control of complex dynamic systems takes into account these objectives:
1 - Modeling,
2 - Observation,
3 - Error analysis.

The errors and failures of the hardware components, software errors or errors in the design 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 quantitative or qualitative measurable parameters in relation to the properties of the system and from these we can in real-time detect deviations during the process (Fröh 1996).

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 (Fröh 1996).

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 (Laub 1999 b).

Figure 1 shows 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 (Laub 1999 a).

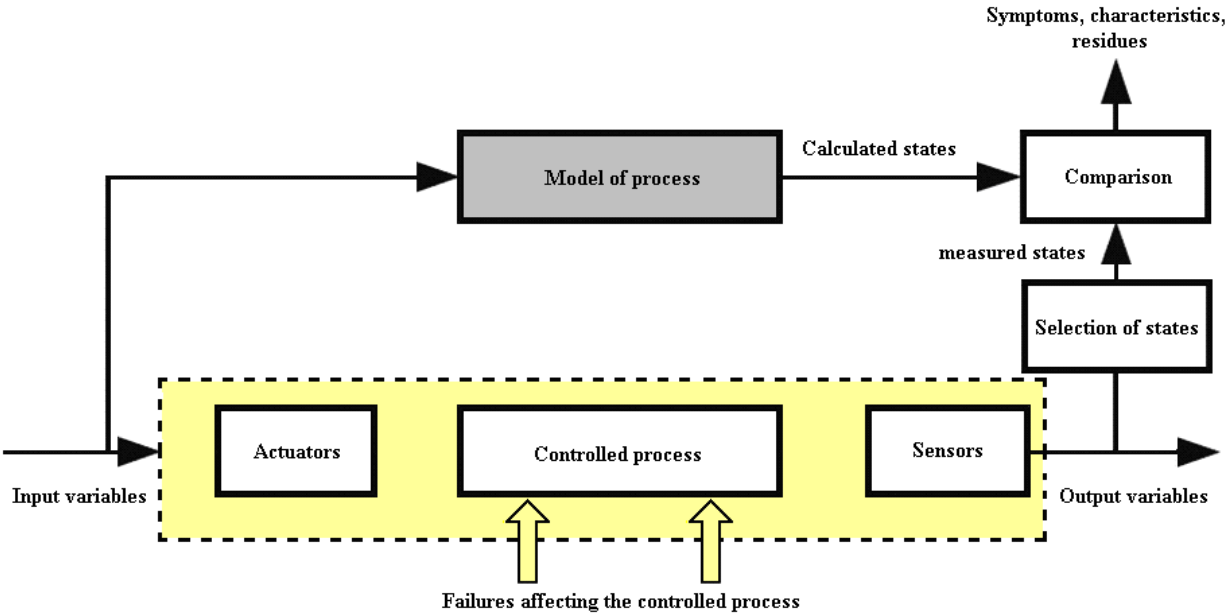

Fig. 1 *Principle of control based on the model of the real process. (Laub 1999 a)*

THE PROPOSAL

The overall proposal of the course of the safety analysis is shown in the figure 2. This process was divided into five steps. After the execution of each step of the analysis is performed verifying of achievements. The full contents of the tasks for various steps of the safety analysis is described later in this article.

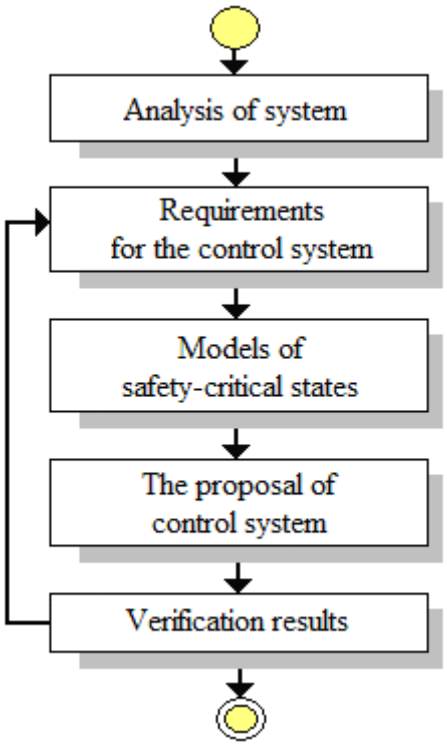

Fig. 2 *The proposal of process for safety analysis*

PROCESS OF SAFETY ANALYSIS

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, and determine whether these states are deterministic or stochastic. 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.

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). The Use of the Luenberger´s observer for deterministic states and Kalman´s observer (filter) for stochastic states, the determination of the methods and processes 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.

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 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. 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 fulfillment 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.

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".

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 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 design of the control system for the system. In conclusion of our proposal does not lack verification of the results obtained.

REFERENCES

1. Susanne MANZ. 2004. *Entwicklung hybrider Komponentenmodelle zur Prozessüberwachung komplexer dynamischer Systeme*. Stuttgart: Forschungsbericht Institut für Automatisierungs- und Softwaretechnik, Universität Stuttgart.
2. Susanne MANZ. 2004. *Entwicklung hybrider Komponentenmodelle zur Prozessüberwachung komplexer dynamischer Systeme*. Stuttgart: Forschungsbericht Institut für Automatisierungs und Softwaretechnik, Universität Stuttgart.
3. P. FRÖHLICH. 1999. *Überwachung verfahrenstechnischer Prozesse unter Verwendung eines qualitativen Modellierungsverfahrens*. Stuttgart: Institut für Automatisierungs- und Softwaretechnik (IAS). Dissertation. Stuttgart: Universität Stuttgart.
4. LAUBER, P. GÖHNER. 1999. Prozessautomatisierung 1. Band 1, 3. Auflage. Berlin: Heidelberg, Springer-Verlag.
5. R. LAUBER, P. GÖHNER. 1999. Prozessautomatisierung 2, Band 2, 1. Auflage. Berlin Heidelberg: Springer-Verlag.

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