© Wydawnictwo UR 2016 „Edukacja – Technika – Informatyka" nr 1/15/2016
ISSN 2080-9069 www.eti.rzeszow.pl
ISSN 2450-9221 online DOI: 10.15584/eti.2016.1.26

ŠTRBO MILAN[1], STOFFOVÁ VERONIKA[2]

The proposal of complex safety analysis for development of dynamical systems

[1] Ing., PhD., Department of Mathematics and Informatics, Faculty of Education, Trnava University in Trnava, Slovak Republik
[2] Prof. Ing., CSc., Department of Mathematics and Informatics, Faculty of Education, Trnava University in Trnava, Slovak Republik

Abstract

The aim of the article is to propose a complex methodology for implementing a safety analysis of dynamical 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 sevenbasic steps. The individual steps of the methodology are carried out in a hierarchical sequence. The step "Preliminary Hazard Analysis" consists of the PHI and PHA methods. Further, roles of individual methodology steps are detailed. In the second part of the article, the principle of safety-critical process monitoring based on models is.

Key words: safety analysis, dynamic systems, safety-critical systems described.

Introduction

Safety and care for the physical and mental health of a person is the highest priority in every society. Information security, internet and computer security, privacy and identity of the individuals are an important tasks of each organization [Pšenáková, Szabó 2014; Pšenáková et al. 2012; Pšenáková 2012]. Equally important are the safety and care about human health, their property and the environment in the design and development of control systems. Operation of safety-critical systems for his surroundings is a danger. Intensity of damage can be really huge. Based on this knowledge is emphasized in the design of control systems and especially for the analysis of potential risks. The preliminary hazard analysis is a design tool that helps developers to identify and address risk in the early stages of developing such a system. The safety is a concept that seems to be very obvious, but the sequence of steps that has to be done for its implementation into system is very difficult. In this article we drafted a preliminary risk analysis.

Besides control and regulation functions, automatic monitoring according to operating rules is of great importance in continuous-discrete technology process

automation. Mathematical models are often deployed for process monitoring in engineering and technology applications in order to obtain as accurate description of the technical device as possible. However, especially for dynamical technology systems, creating a mathematical model applicable to system monitoring is associated with many difficulties. As not all the parameters of the model are known, in analytical procedures, it is necessary to use estimations for these states or parameters. On the basis of these issues, qualitative procedures are also taken into account for monitoring dynamical systems. The qualitative models do not require exact reflecting of inner physical dependencies, the models include only those situations where there occur changes. Qualitative model is able to distinguish these states, thus enabling describing dynamical systems attributes. The fact that the dynamic characteristics can be described only very inaccurately or they are impossible to be described at all is the main disadvantage of qualitative models. Though, this is a necessary demand for monitoring dynamic elements of the system. Therefore, the possibility of using a combination of both model forms for safety analysis of dynamical systems is to be researched. Qualitative models for assessing the complexity and quantitative mathematical models are applied to describe the dynamics [Štrbo at al. 2014].

1. Proposal of safety analysis methodology

Figure 1 presentsa methodology for modelling safety-critical processes, specifically for modelling dynamical technology systems. The methodology is illustrated using ordinary UML state diagram consisting of a sequence of six successive steps. The final step of the methodology is verification of proposed models with the purpose of monitoring safety-critical processes. If weaknesses in the proposed models are revealed during the verification, safety analysis process returns to the step modelling safety-critical process.

1.1. The proposal of the preliminary hazard analysis

The preliminary analysis consists of methods PHI and PHA. Task of PHI is to identify all possible risks during operation of system. Task of PHA is to analyse these risks. The proposal of the Preliminary hazard analysis is shown in the figure 2.

1.1.1 PHI – Preliminary Hazard Identification

At the beginning is carried out PHI. The aim of the PHI is to identify all potential hazards that should be done in the proposal of every subsystem nested to test, if this system is truly safety-relevant. All of the risks and potential events have to be identified. Therefore is really important to consider all parts of the system, safety systems, modes of operation and maintenance. So PHI tries to answer the question: „what dangers and accidents may have influence on this system“. In the process of identifying risks is needed to be thoroughly familiar

with the system, which we want to analyse. It is necessary to know on what system depends (inputs), what activities are being done by the system (feature) and what services is the system providing (outputs). In order to identify all hazards and events, it is often necessary to divide the system into a manageable parts (process units), individual activities and to the group "who and what all" are exposed to risk. The output of method PHI is a list of risks, which contains all of the possible risks associated with the operation of the control system. This list will be used in the next phase of the preliminary analysis, where will be analysed the individual risks of this list.

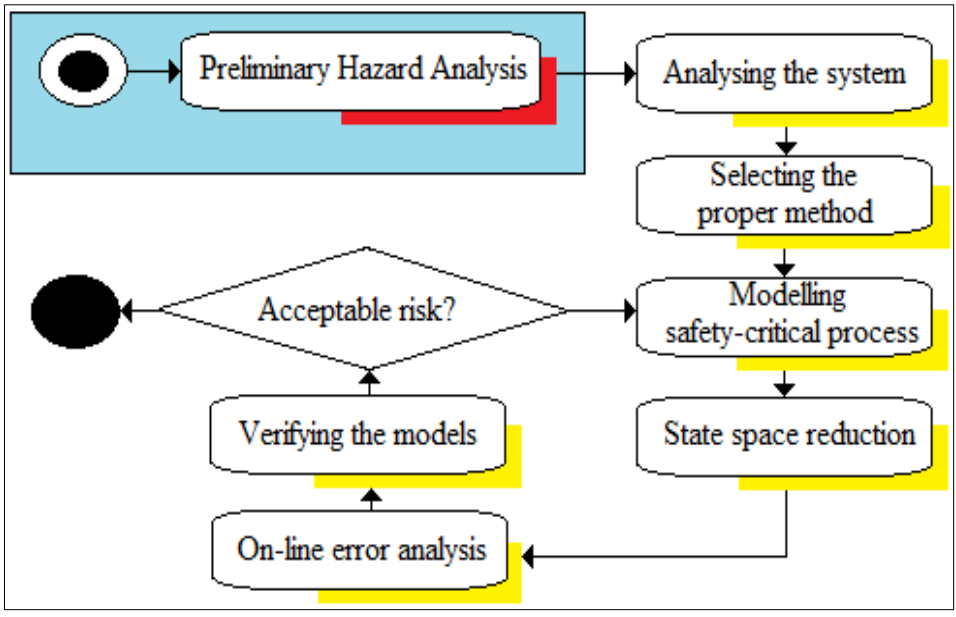

Figure 1. Proposal of a methodology for modelling dynamical systems

1.1.2. PHA – Preliminary Hazard Analysis

It is an inductive method, which is applied in all periods of system service and points on danger and dangerous events, which can cause an accident. The PHA is based on results of PHI and is used in more detailed analysis of identified hazards. Furthermore we will examine the risk related to functional requirements of the system in order to assign safety inserts to individual functions. Except that, is by now possible to develope various alternatives of system design, with respecting identified hazards. The merit of PHA is to identify all potential hazards and events that may lead into insurance, to evaluate observed events related to their severity, and not the least is necessary to determine required hazard of control and following activities.

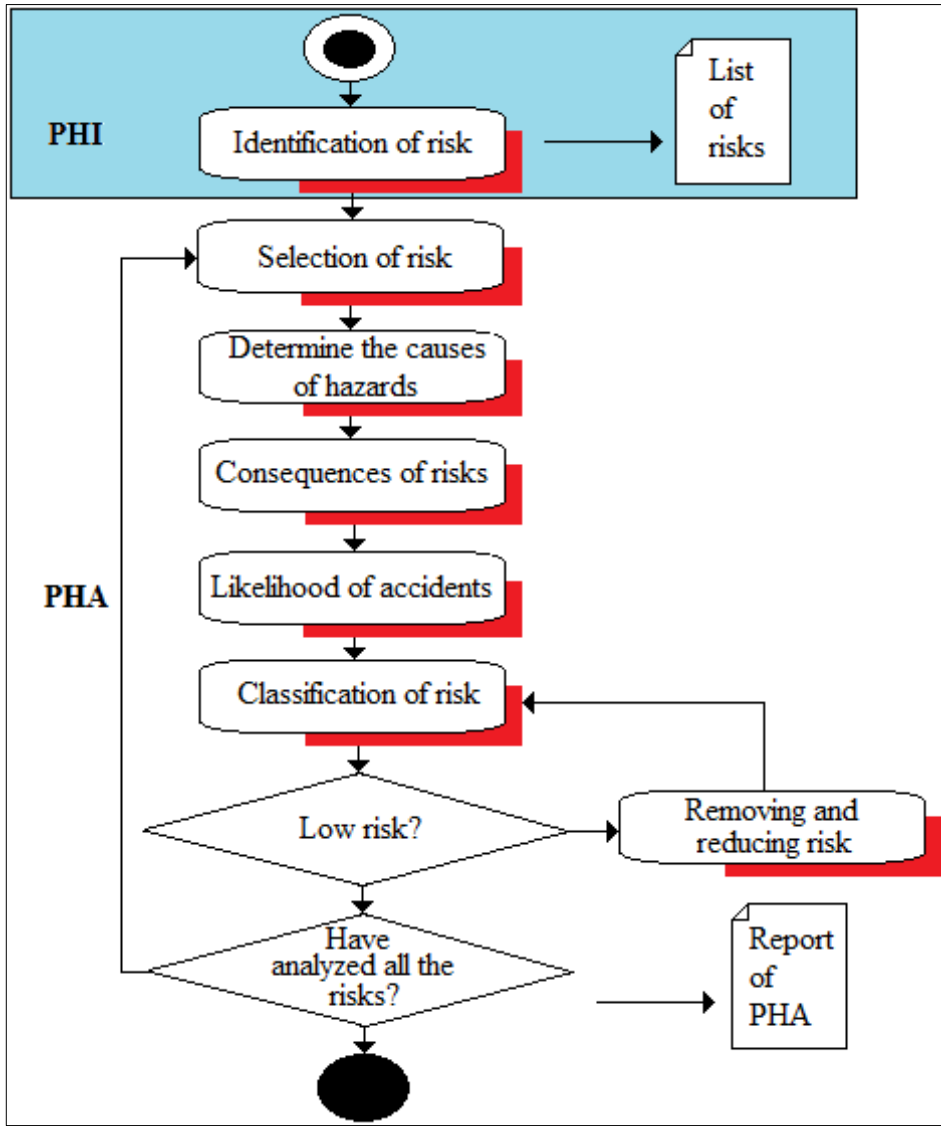

Figure 2. Process of preliminary analysis

1.2. Analysis of dynamical technology system

The content of this step is to analyse 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 analyse the actual terms and basic operating parameters respectively conditions. It is closely related to the analysis of limitations in indi-

vidual 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.

1.3. Selection of the appropriate method for modelling safety-critical processes

A detailed system analysis is able to provide all the information necessary for the safety analysis. Based on this system analysis, selecting the appropriate method for creating models required for automated monitoring of dynamical system operation is much easier. We propose to use the SQMD method for developing models for safety-critical processes of dynamical systems.

The SQMD method is used for the safety analysis of dynamical systems. It is based on quantitative and qualitative modelling methods. It implements hybrid models for real time monitoring and detecting. The hybrid model includes qualitative and dynamic elements and combines advantages of both methods. On-line monitoring and diagnostics with the aim of detecting and locating faults in dynamical technology systems are to be understood in this way. The main advantage of the safety analysis applying the SQMD method is the simplicity of dynamical system modelling. The method includes two important aspects. On the one hand, there are the existing mathematical models which are combined with qualitative models in order to model and simulate dynamical systems. On the other hand, analysing the states becomes an interesting part of the process, as it enables on-line evaluation requiring less processing power.

1.4. Modelling safety – critical processes of dynamical systems

In this step, it is important to correctly describe the safety – critical processes of a specific system using the models. The purpose is to develop qualitative and quantitative models within the range of the general system description. We applied the fuzzy logic to create qualitative models of individual processes. Alternatively, Petri nets can be used for causal network or purely discrete processes. Quantitative (mathematical) models can be constructed using differential and difference equations, since dynamical technology systems are to be described. Deducing from another examples, almost every correct mathematical formula can be used as a mathematical model. Carrying out the synthesis of models, assessing their effectiveness and inspecting their validity are also necessary procedures. For automated control of dynamical systems, we propose to use hybrid

models consisting of qualitative and quantitative (mathematical) models. The correctness of these models is to be evaluated in the final step of the methodology – verification.

1.5. State space reduction

The focus of the overall concept is the on-line state space reduction, allowing monitoring dynamical systems. After constructing the individual models for automated monitoring of safety-critical system processes, the state space needs to be reduced. The combinatorial explosion removal is the most important reason for this reduction. The aim is to determine the reduced qualitative state space for time interval specified in advance. It contains all the possible states of the system for a defined time interval. These states can bee valuated in the following point of the methodology, in the on-line failure analysis.

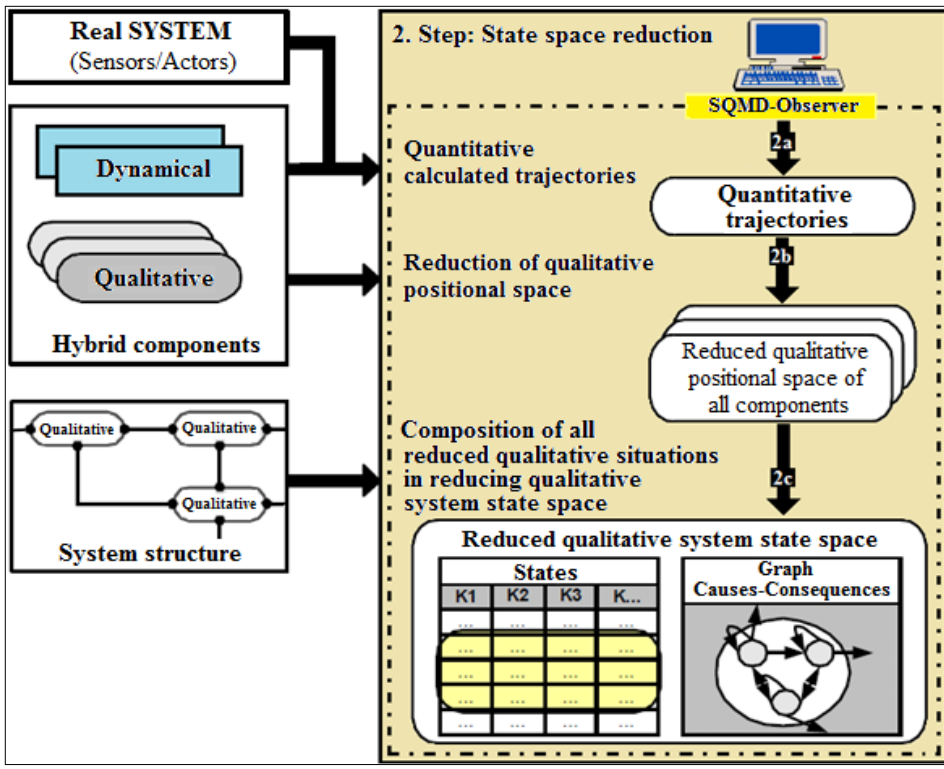

Figure 3. Concept of State space reduction [Manz 1999]

The state space reduction is periodically carried out by SQMD observer illustrated in figure 2 in three consequent sub-steps 2a, 2band2c. The following sub-steps include specifically the following activities [Manz 2004]:

– Determination of quantitative trajectories (2a),
– State space reduction on the level of components (2b),
– Composition of the components(2c).

The advantage of reducing the state space at the component level is the removal of combinatorial explosion. Analysis and evaluation are not carried out in the whole state space, but are performed only for the time period corresponding to the relevant part of the space. Directe valuation of data from the technical process at the component level represents another advantage. This means that the qualitative parameters are replaced with the exact values of the measured data obtained from sensors and actuators. The accuracy of the model is increased in this way [Manz 2004].

1.6. On-line error analysis

In this step of the methodology, analysis of the qualitative state space reduced in the previous step is to be performed. Accordingly, the damage prognosis is evaluated. The purpose of the error recognition is the analysis of quantitative and qualitative relations within the time interval enabling to carry out the decision of erratic system behaviour according to the analysis. The concept of on-line analysis is shown in figure 3. As shown in the figure, the concept of on-line analysis can be divided into two partial steps

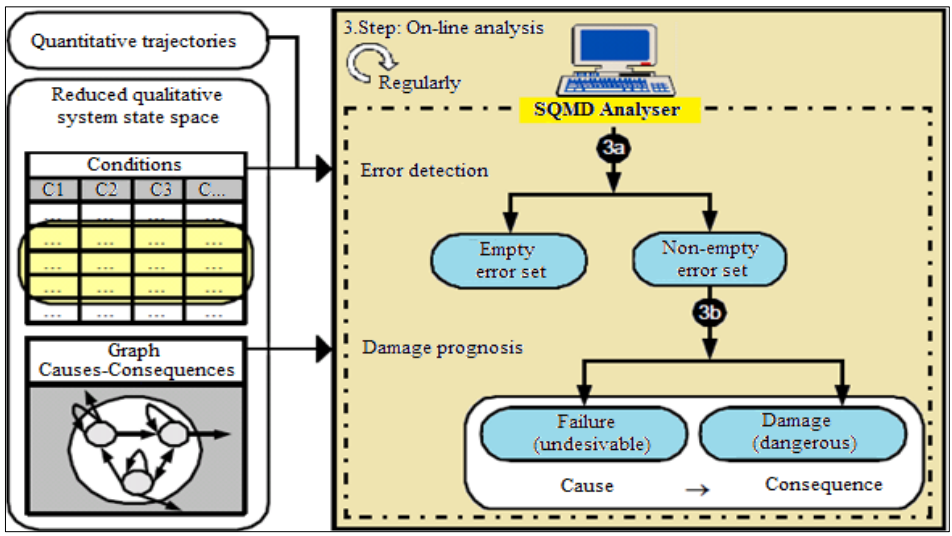

Figure 4. Concept of on-line analysis [Manz 1999]

"Recognising (detecting) errors – Step 3a" and "Damage prognosis – Step 3b". These steps are supplemented by calculations carried out by analyser. The purpose of the error recognition is the analysis of quantitative and qualitative

relations within the time interval enabling to carry out the decision of erratic system behaviour according to the analysis. The damage prognosis does not primarily serve to diagnose, but to recognise the potential harm caused by undesirable proceeding.

1.7. Verification of the proposed model for safety-critical processes

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 point "modelling safety-critical processes of dynamical systems".

2. Developing a model of on-line monitoring 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. 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 [Štrbo, Tanuška 2012; Štrbo et al. 2014].

Conclusion

In this paper, a methodology for implementing the model-driven safety analysis for dynamical technology systems is presented. The proposal of the process includes seven steps and it is shown by states diagrams in UML (Unified Modelling 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, 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.

Literature

Fröhlich P. (1996), *Überwachung verfahrenstechnischer Prozesse unter Verwendung eines qualitativen Modellierungsverfahrens*, Stuttgart.

Manz S. (2004), *On-line monitoring and diagnosis based on hybrid component models*, Stuttgart.

Pšenáková I. (2012), *Bezpečne na internete*, "Media4u Magazine: čtrvtletní časopis pro podporu vzdělávání" Roč. 9, č. X2.

Pšenáková I. et al. (2012), *Course Content of Computer Security*, [w:] ICETA 2012: IEEE 10th International Conference on Emerging eLearning Technologies and Applications, Slovakia, Košice.

Pšenáková I., Szabó T. (2014), *Niektoré aspekty potreby kurzu počítačovej bezpečnosti pre neprofesionálov*, [w:] *Science for education – education for science*, Nitra.

Štrbo M., Tanuška P. (2012), *The process of preliminary hazard analysis for safety-critical systems*, [w:] International Doctoral Seminar 2012: proceeding. Smolenice Castle, SR, May 20-22, 2012, Trnava.

Štrbo M., Tanuška P., Gese A., Smolarik L. (2014), *The methodology proposal for the model-oriented safety analysis of dynamical systems*, Bratislava.