Trnava University in Trnava
Faculty of Education

Department of Mathematics and Computer Science

Proposal for Strictly Model-oriented Safety Analysis of Dynamic Technological Systems

Monograph

2019

Ing. Milan Štrbo, PhD.

Proposal for Strictly Model-oriented Safety Analysis of Dynamic Technological Systems

Reviewers:

prof. Ing. Pavol Tanuška, PhD.

doc. Ing. Andrej Trnka, PhD.

Translations:

Mgr. Hana Vančová, PhD.

Technical redactor:

Mgr. Ing. Roman Horváth, PhD.

ISBN 978-80-568-0308-0

Acknowledgement

I would like to thank my family and colleagues for their support and valuable advice throughout the process of writing of this monograph. This monograph was supported by the Grant scheme number TU-2019.

I would also like to express my gratitude to the reviewers of this monograph, prof. Ing. Pavol Tanuška, PhD. and prof. Ing. Veronika Stoffová, CSc., who read it carefully and whose valuable comments undoubtedly contributed to its improvement.

Summary

Štrbo, Milan: Proposal for strictly model-oriented safety analysis of dynamic technological systems. [Monograph] – Trnava University in Trnava. Faculty of Education; Department of Mathematics and Computer Science.

Keywords: safety analysis, dynamic technological system, modelling.

The submitted monograph deals with the proposal for a strict model-oriented safety analysis of dynamic technological systems.

The first chapter provides the essential terminology of the theory of systems and automation.

The remaining part of the monograph deals with the proposal for the implementation of safety analysis for safety-critical dynamic technological systems. This part explains specific steps in the implementation of this analysis. The chapter summarizes theoretical findings on modelling of safety-critical processes and contains a detailed description of problems in designing dynamic system models, including a proposal for a possible solution using the SQMD method. The method is based on monitoring the safety-critical processes by hybrid models made by the composition of mathematical and qualitative models. The conclusion of the monograph is focused on the summary of the achieved results.

Abstract

The aim of the submitted monograph is the proposal for the methods for strictly performed safety analysis of dynamic technological systems. Safety analysis is carried out in the process of development of control systems, particularly for safety-critical processes of system operation. We propose to concentrate the security analysis to be based on models. Models are proposed to be created for the safety-critical processes of system operation, which would be hazardous for the system operation itself. The following part of the work describes the principle of control of safety-critical processes appearing in dynamic systems based on the designed models.

Contents

List of figures and tables

Introduction

Since the 1960s, safety engineering has been in development and implementation, primarily in the electronics industry that works with a high number of elements. The main role of the safety engineering is to analyse the reliability of the systems. Gradually, it expanded into other areas of industry, such as aviation, astronautics and power engineering. Its primary role is to design systems, operation of which does not present any hazard for people or the environment. Safety analysis can achieve the higher operational safety of these systems.

Safety and health care for people, their property and the environment belong to contemporary preconditions for the control system development. Safety-critical system operation represents the surrounding danger with the intensity of damage caused by undesirable system events possibly reaching huge levels. Based on this knowledge, a possible risk analysis must be particularly emphasized during the control system development. Safety risk analysis is designing a tool for helping developers identify and solve dangerous situations in the early stages of safety-critical system development. At first glance, safety is a very obvious concept. However, the sequence of steps necessary to be taken for its implementation in a particular system is very demanding. The process of safety analysing is a challenging and tedious process, and this article/monograph is presented to propose a methodology for its implementation.

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 to obtain an 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. Based on these issues, it also takes qualitative procedures 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. A qualitative model can distinguish these states, thus enabling describing dynamical systems attributes. The fact that the dynamic characteristics can be described only inaccurately or that 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 (Strnád, 2010).

From a safety point of view, it is crucial what damage (especially on human life) the malfunction of the control system can cause. It is closely related to the frequency of such events. While road traffic deaths occur practically every day and they are tolerated by society, air or rail disasters are perceived far more sensitive. On the events in nuclear power plants, which have an incomparably lower frequency, not to mention. It relates this to the magnitude of the catastrophe that the error can cause. An interesting psychological phenomenon is that sometimes we are willing to consider automatically ourselves as a potential victim of a disaster (see nuclear or air transport), while in other cases not (road transport). This seems to be closely related to the sense of self-control of the process (road transport), or the impossibility of influencing the process itself (nuclear energy). It is a sad paradox for us technicians that this false feeling persists, as today's technical control systems are more secure and reliable than any well-trained person. While one in a thousand human decisions are wrong, the technical system, if it made one safety-relevant decision per second, would make one mistake in 32 years. A human fails every 17 minutes at the same pace of work. Control systems have only one minor weakness – people design them, and those, as mentioned above, make mistakes. It is incredible that we can still design systems that are six times more reliable than their creators (Strnád, 2010).

The quality of the system is generally understood as the sum of the properties that make the system capable of performing the desired function concerning the intended method and conditions of use. The most important groups of properties that determine the quality of the system can be arranged by their importance. These are technical and functional properties, reliable operation, material and energy demands, technological level, aesthetic, ergonomic and ecological properties. In particular, the first two groups represent the most important quality properties:

- Functional and technical attributes, which include mainly physical-technical characteristics and technical parameters of the system.
- Attributes displayed especially while using the device in operation. These include reliability, ease of use and safety in handling (Bigoš, 2011).

The reliability of a technical system is characterized by its complex quality that expresses the general ability to maintain functional properties at a given time and under specified conditions. The most important partial qualities of reliability are:

- **Trouble-free operation** – the ability of a technical system to fulfil the functions which are continuously required for a specified period and under defined conditions.
- **Sustainability** – the property that characterises the ability to prevent failures by prescribed maintenance.
- **Serviceability** – the capability of the technical system to identify the causes of the faults and their remedy by repair.
- **Availability** – the technical system is characterized by reliability and serviceability.
- **Safety** – the property of a technical system not to endanger human health, or the environment in performing the prescribed function.
- **Durability** – the ability of the system to perform the required functions after reaching the limit state (safety, loss of parameter values, reduction of effective operation, the necessity of major repair; Bigoš, 2011).

Reliability can be characterized as the matter of the regularity of the failure. Failure is a phenomenon that results in the loss of an object's ability to perform the required functions. The mechanism of failure is a summary of the physical, chemical and other processes leading to the failure.

The classification of failures according to consequences is mainly applied in systems, perceived as complex and distinguished:

- **Critical failures** that result in loss of operational capability with endangering the health or life of persons, endangering the environment, or causing great material damage.
- **Essential failures** that lead to loss of serviceability but without endangering the health or life of persons, endangering the environment or causing material damage.
- **Non-essential failures** that do not result in loss of serviceability, only material losses, e. g. production interruption.
- **Emergency failures** that are sudden and complete.
- **Degradation failures** that are gradual and partial (Bigoš, 2011).

1 Definition of terms

The introductory chapter of the monograph introduces the essential terms of the theory of systems and automation. In systems theory, the focus is on the distinction between continuous and event-oriented systems and on the complex and dynamic systems. The scope of terms in process automation contains many areas, and these cannot always be interpreted unambiguously.

1.1 System theory concepts

Machinery, means of transport, devices and equipment are systems (Simulation von Logistik, 1996). For this concept, the literature provides numerous definitions. The fact that the term system is used in a multidisciplinary way can explain this in a multidisciplinary way.

System: is a limited arrangement of components that are in a certain relationship with each other. A system is a set of cooperating elements that perform a certain task together. In this work, the word "system" is understood as a technical process.

The internal relations or dynamic properties of the system are determined in terms of transition functions to describe transitions between states (state transition). State transition plays an important role in this work (Simulation von Logistik, 1996).

Status variables: are system variables knowledge of which at the exact time course of the input variables enables to investigate accurately the system properties in the future.

The state variables are time-dependent, i.e. the completeness of their instantaneous values determines the state of the system. If all state variables are not known, then further behaviour of the system is not entirely predictable. In a physical sense, state variables are usually assigned to objects whose energy can be stored in some form (Simulation von Logistik, 1996).

State transition: describes the change of system or subsystem status.

The values of at least one state variable must change on the basis of the processes in the system. If the state variables change continuously over time, we are talking about a continuous system. If, in contrast, discontinuous state transitions occur, i. at certain points in time, parameter values leap, it is a time-discrete system. Continuous state transitions are described using differential equations, state transitions discreetly over time, for instance, based on events. If the parameters are not converted back to one type of state variable, then a hybrid system is created (Simulation von Logistik, 1996).

Hybrid system: if the behaviour of a system is influenced by variables that change their values in leaps, the system state comprises both a discrete component and an analogue component, and such a system is called a hybrid system (Nenninger, 2001).

If we combine states that follow one another in time, we get trajectories. The system state variables change values along the trajectory in the state space. From the trajectory, it is possible to read important system features regarding system behaviour.

To assess the behaviour of systems over time, it is necessary to take into account the time course of their state variables. If all state variables are constant, it is a static system. Otherwise, it is a dynamic system. In particular, the temporal properties of dynamic systems affect the overall modelling and simulation in a very special way (Brack, 1974).

Complexity is an important classification feature of dynamic systems. The concept of complexity is defined differently from discipline to discipline. There are many definitions, which can lead to misinterpretations (Frank, 1998). Complexity can be divided into functional and structural complexity (Hurme, 1992).

Functional complexity: we speak about functional complexity when relations between quantities are little known, difficult to describe or calculate (Hurme, 1992).

Structural complexity: systems are structurally complex when they comprise numerous variables having very diverse relationships with each other (Hurme, 1992).

Generally, complex systems cannot be modelled as a whole if they require a certain systematic approach. The key to such a system is the structuring of such complex systems where the output of the system can be broken down hierarchically into clear, more easily modellable subsystems. The essence of system structuring can be characterized by the concepts of decomposition, topology and system hierarchy (Panreck, 1999).

Decomposition: decomposition means decomposition of a system into subsystems. It is motivated by functional aspects, within the intended problem of analysis or synthesis, i.e. the subsystems are chosen precisely to give priority to the specific, specially formulated questions needed for system aspects (Panreck, 1999).

Topology: individual subsystems exchange information through interconnections. All system connections create a link structure or topology (Panreck, 1999).

Hierarchy: it is recommended to divide the subsystem into smaller subsystems for an even more detailed understanding of the system. This decomposition is referred to as hierarchization and can be performed at several hierarchical levels. This hierarchical decomposition ends with elementary subsystems that can no longer be decomposed (Panreck, 1999).

1.2 Process automation terminology

The term process automation consists of words process and automation. Process is a procedure for transformation, transport or accumulation (storage) of matter, energy or information (Lauber 1, 1999).

Process: A group (collection, summary) of reciprocal procedures in a system, that form (change, reshape), transport or store a matter, energy (Lauber 1, 1999).

Automation is derived from the term automaton. Automat is an artificial system that automatically monitors a program. On the basis the program, the system makes decisions that are based on connection of inputs with the corresponding system states and result in outputs. Therefore, automation is putting the automaton into operation, so that one or more devices totally or partially work according to their purpose without human cooperation. The degree of automation is defined by the extent of automation of the operation or process (Lauber 1, 1999).

The process controlling system consists of: user, controlling computer system and technical process (Lauber 1, 1999).

Technical process: A process, in which the binary and analogue process quantities (state quantities) can be measured, controlled and regulated by technical means.

Process or state quantities can be divided into following categories:

- input quantities are brought (enter) the process, act upon the process and affect the process state,
- output quantities exit the process,
- defective quantities act from the environment and randomly (Lauber 2, 1999).

Tasks of the process controlling system are based on observation of the course of process and the subsequent supervision and management of the process (Lauber 2, 1999).

Process control: Regular course control of the process (also called "operation according to regulations") should early detect the possible changes in irregularity of malfunction or the potential dangerous states. Diagnostics of the possible causes of the irregular operation course and the place of occurrence of the malfunction belongs to the tasks of control (Lauber 2, 1999).

Process management: Influencing the energy and mass flows of a technical process to determine the outcome of a process (a certain process output), such as a product or condition – to achieve it as economically as possible while respecting the required boundary conditions such as environmental protection. Process management includes both the control and regulation of individual process variables and the entire technical equipment or also operational process control (Lauber 2, 1999).

1.3 Process modelling terms

Models are used to simulate the real system behaviour. This approach is applied in all areas of science. In relation to the application of management projects (automation), the following model concept is appropriate (Schmidt, 2000).

Model: A simplified representation of an existing or projected system with its processes into another conceptual or subject system. It differs from its original (example) regarding the relevance of the examined properties, only within the margin of tolerance depending on the aim of the investigation. It is used to solve certain tasks which, through direct operations on the original, are not possible or would be very expensive (Schmidt, 2000).

The established tolerance framework, in which the behaviour of the model differs from behaviour of the original, depends on the complexity of the system. It is in complex systems that the behaviour of the system in the model must be idealized or examined in abstraction. The abstraction is, therefore, an important aid in model building (Schmidt, 2000).

Abstraction (generalization): A process to reduce the complexity of a problem by dividing the problem details into certain aspects of problem-solving into important and unimportant (Schmidt, 2000).

Abstraction leads to a better understanding of the system and a reduction in the cost of preparing the data, reducing the time to get results and the cost of saving (storing) the data. There are two approaches to abstraction:

- reduction: withdrawing from displaying details that are not important,
- idealization: simplification of real possibilities (Schmidt, 2000).

Abstract models are deployed in many areas. In engineering sciences, these are referred to as process models (Schmidt, 2000).

Process model: An abstract model of a technical process that contains physical process variables as elements of a model and describes statically or dynamically the relationships between these process variables. The structure of the process must then be determined in the model (Lauber 2, 1999).

It is used for planning and controlling the process. Models can be divided into continuous process models, dynamic flow processes and event-oriented process models, sequential and transport (lump) processes. Two types of dynamic models can be distinguished depending on whether the process variables are described qualitatively or enter their model in quantitative values:

- qualitative process models,
- quantitative process models.

The aim of quantitative models is to display (express) the selected behaviour of the process where possible numerically and corresponding to reality (Lauber 2, 1999). Mathematical models are generally used for this purpose.

Mathematical model: A mathematical model is called if the model expresses a mathematical formula according to which the values of the output quantities can be calculated for any moment of time and for any input quantities.

The qualitative models are principally described and thus the qualitative behaviour of the system. It is based on physical or the chemical relations, the selected context and the course of the process quantities are taken into account only principally and qualitatively (Lauber 2, 1999).

Qualitative model: A discrete abstraction or a discrete approximation of a continuous process model.

The design of the qualitative model displays (represents), therefore always the consideration between contradictory objectives “accuracy” and “understanding of complexity”. The qualitative behaviour of the continuous system in the future cannot generally be predicted unambiguously on the basis of the final selection of the past course. In other words, the qualitative behaviour of a continuous system is, according to all rules, nondeterministic. However, the forms of behaviour generated by the qualitative model are not created by the system, so we will call them inapplicable (invalid) solutions (Lunze, 1995).

In the field of artificial intelligence (AI), the term qualitative termination is often used (Lunze, 1995). Qualitative termination deals with the visualization and analysis of physical systems, and unlike physics or engineering sciences, it does not focus on a quantitative but a qualitative description (Struss, 1996).

The combined quantitative and qualitative models are called hybrid models (Manz, 2000).

1.4 Process control terms

During the operation of the technical process, the task of controlling the process is to determine whether the technical process is regular, i.e. as prescribed. The control is performed on-line, i.e. in parallel with the ongoing process. The current process status, the reporting of unwanted or unauthorized process states are indicated, and appropriate measures are taken. Deviations from the process state cause errors for various reasons. Errors without countermeasures in a shorter or longer time will result in malfunctions and failures. The control is designed to prevent these malfunctions and outages (Isermann, 2001).

Error: Unauthorized deviation of at least one feature of the observed module (Eusemann, 2001).

Failure: From the onset of the occurrence (induction, loading), a certain error lasting (Eusemann, 2001).

Outage: From the start of use (load), abolished the ability to perform tasks assigned to the observed model, based on the underlying causes and within the permissible (permitted) use (load) (Eusemann, 2001).

The role of each control system is to identify its failure and determine the cause. Errors can be detected from the measured values and information can be provided to prevent damage (Lunze, 1995). In this work, control contributes to both observation and error analysis (Manz, 2002).

Observation: Finding the current state of the process from existing measured quantities (Manz, 2002).

Error analysis: Analysis of possible deviations of the current process state from the process state specified by the regulation. Error analysis is divided into error detection and damage prognosis (Manz, 2002).

Error detection: Determination of the time of occurrence of errors in a technical process that causes unwanted behaviour of the entire device (Manz, 2002).

Damage prognosis: Location of the fault and identification of the type and cause so that appropriate countermeasure can be taken.

The difference between the measured and calculated quantities is also called a residue. Redundancy is preferably used to generate residues. If we use mathematical process models to create redundancy, we are talking about analytical redundancy and using qualitative models of knowledge redundancy (Isermann, 2001).

1.5 Other related terms

Operation according to regulation (operating instructions): Expected operation of the technical system (normal operation).

Situation according to regulation (desired situation): Describes the scenario for prescribed operation.

Deviation: Inadmissible deviation of at least one parameter of the monitored module.

Error model: Displays all identified errors in the engineering process. These are used to detect process control errors.

Hazard: A fact where the risk is greater than the limit risk.

Threat analysis (risk analysis): identifying and examining the potential of a system threat.

Operation at risk: The behaviour of a faulted technical system that leads to a conclusion on the effect of the fault.

Dangerous situation: Describes a dangerous operation scenario.

Determinism: The model behaves deterministically when each state can be determined (calculated) from the basic state.

Nondeterminism: A system is nondeterministic when the state of the system cannot be derived from the basic state.

Elementary component: A model of a system element that cannot be further broken down (atomic components).

Hybrid component: Comprises a dynamic and qualitative component of the model.

Comments: Describe information and qualitative states and show modelling results.

Composition: Joint assignment of components to the system.

Qualitative variables: Physical variables that are available on component interfaces or are important for remembering the internal state.

Quasi-dynamic: Only sequential processes (transfers) between situations in the situation table are described. Transition duration times are not taken into account.

Pathological models: Error models that are used to detect process control errors.

Damage: Damage to the body, psyche and the environment.

Damage prognosis: Location of errors and determination of types of errors and causes of errors.

Situation: The state of the selected system element or system itself, which is comparable to the detected state. In the SQMA method, the situation comprises a combination of interval values, and in this way describes the possible scenario of the system element or system.

Situation rules: A set of arithmetic and logical expressions that define a defined situation space with qualitative variables.

Situation table: The table contains ranges of values of qualitative variables with all technical combinations. It describes the static behaviour of components.

SQMA: Modelling method for describing the qualitative behaviour of static systems. It is used in safety analysis.

SQMD: Modelling method for describing the qualitative behaviour of dynamic systems. It is used for process control.

System equations: Equations describing the structure of the system based on physical laws.

System component: A system model for a flat structure, system components contain only elementary components, for a hierarchical structure, it can contain subsystem components.

Components: A subsystem component comprises many elementary subsystem components.

Transaction: Transitions between situations. They describe the quasi-dynamic properties of a system or system element.

Transaction rules: Determine the possible transaction arrivals between situations and situation tables.

Undesirable operation: Faulty operation of a technical system that can be assigned at least one cause of failure.

Undesirable situation: An undesirable situation describes an adverse traffic scenario.

Cause and effect graph: An error graph that illustrates the relationship between cause (adverse status) and effect (dangerous status).

Status: The situation group is assigned to the status. The status is used to show the model results.

Status table: A table containing all possible states.

2 Proposal for a safety analysis methodology

The following chapter introduces a proposal for the safety analysis of the dynamic technological systems.

Figure 1 presents a methodology for modelling safety-critical processes, specifically for modelling dynamic technological systems. The methodology is illustrated using an ordinary UML state diagram comprising a sequence of eleven successive steps. The final step of the methodology is the "Final Control System".

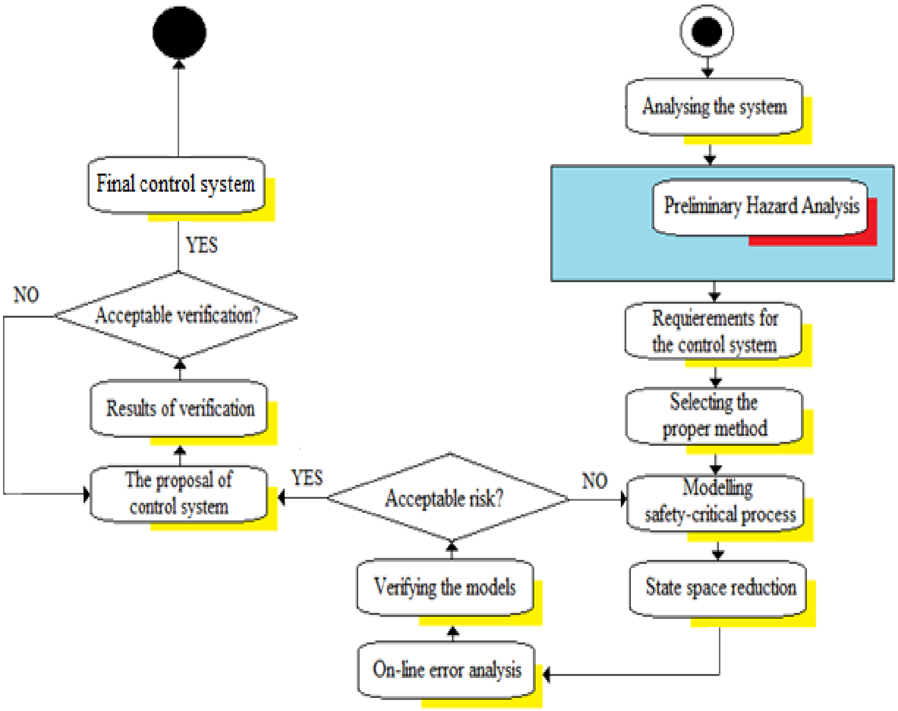

Figure 1: Proposal for a methodology of modelling dynamic systems.

Consequently, there is the description of the operations and tasks that are needed to be performed in the individual steps of the proposal.

2.1 Analysing the dynamic technological system

The first step in the proposal is the necessity to analyse a concrete safety-critical dynamic technological system.

The purpose of this step is to analyse a specific dynamical technology system. It is important to state that the analysis is carried out with a focus on safety analysis. It means that it is necessary to become familiar with the system and its features and to identify all possible operation states of the system. On the one hand, current conditions and basic operating parameters and conditions on the other will to be analysed. The analysis of restrictions in individual states, gap analysis, risk assessment, and all available system resources evaluation is closely related to this step. Further, a top-down method is an important part of the analysis of a particular system. Its tools allow system decomposition from a global perspective into the individual system sub-processes. Each system has a certain set of states or processes. This analysis aims to select and analyse the safety-critical operation processes of the system and divide them into deterministic and stochastic processes.

Carrying out a detailed analysis of these processes, the measuring requirements, functions of process monitoring, or actuator controller requirements can be obtained. For critical processes, information sources providing service staff with information on the process will be selected. Finally, it is necessary to define the inputs for individual processes, relations between the system processes and, of course the output characteristics of these processes. The aim of this step is also to identify requirements for safety analysis and process monitoring in terms of origin, course and critical state (error) evaluation. This can be understood as determining the individual hardware and software requirements on the control system for safety-critical processes.

2.2 The proposal for the preliminary hazard analysis

The second step in the proposal is the Preliminary Hazard Analysis. The preliminary analysis comprises PHI and PHA methods. PHI is to identify all possible risks during the operation of the system. PHA is to analyse these risks. The proposal for the Preliminary hazard analysis is shown in figure 2.

2.2.1 PHI – Preliminary Hazard Identification

Preliminary hazard identification is carried out at the beginning of the project. PHI aims to identify all potential hazards that could have been made in the design of every subsystem nested and to test if this system is certainly safety-relevant (Schwarz, 2004). All the risks and potential events have to be identified. Therefore, it is very important to consider all parts of the system, safety systems, modes of operation and maintenance. Therefore, PHI tries to answer the question of what dangers and accidents may influence this system in the early stages of the project. In the process of identifying risks, it is necessary to be thoroughly familiar with the system, which we want to analyse. It is necessary to know what system depends on (inputs) on, what activities are being done by the system (feature) and what services are the system providing (outputs). To identify all hazards and events, it is often necessary to divide the system into manageable parts (process units), individual activities and to the group “who and what all” are exposed to risk. To support the predictions of what might happen in the future is necessary to know what happened in the past. We use for it a variety of reports on accidents – database (MARS, facts, MHIDAS, WOAD), accident statistics, reports from institutions or state agencies or expertise (Rausand, 2005).

To identify all hazards, we need to gain expertise, where appropriate, experience in dealing with the problem. We use it for different mechanisms. The most important mechanisms of risk analysis used in PHI are (Rausand, 2005):

- Examine and look over similar existing systems.
- The control of previous hazard analysis for similar systems.
- The control of hazard (hazard checklists and standards).
- Consider flow of energy by system.
- Consider the bases of toxic substances.
- Consider the interactions between components in system.
- Controlment of operation specifications and considering all environmental factors.
- Use brainstorming in teams.
- Consider human beings in the opposite of machine technology.

- Consider changes in mode usage.
- Try small scale testing and theoretical analysis.
- Thinking in worst cases – what-if analysis.

The output of the PHI method is a list of risks, which contains all 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 the individual risks of this list will be analysed.

2.2.2 PHA – Preliminary Hazard Analysis

It is an inductive method, which is applied at all stages of system service and points to danger and dangerous events, which can cause an accident (Pačaiová, 2003). The PHA is based on the results of PHI and is used in a more detailed analysis of identified hazards. Furthermore, we will examine the risk related to the functional requirements of the system to assign safety inserts to individual functions. Except that, by now it is possible to develop various alternatives of system design while respecting identified hazards (Schwarz, 2004). The PHA method joins various restrictions, while notably, the risks that must be anticipated by designers and the effects of interactions between risks are not easy to recognize. PHA considers (Rausand, 2005):

- Hazardous components.
- Safety-related interfaces between various system elements, including software.
- Environmental constraints including operating environments.
- Operating, test, maintenance, built-in-tests, diagnostics and emergency procedures.
- Facilities, real property installed equipment, support equipment and training.
- Safety-related equipment, safeguards and possible alternative approaches.
- Malfunctions of the system, subsystems or software.

The proposal for PHA content is to establish procedures to ensure that the elimination of hazards and control measures have been effectively incorporated into the design. It is important to prepare a risk report for each hazard. We must verify whether the system eliminates or adequately manages the risks. During the life cycle of the control system, we can perform PHA updates. The reasons can be manifold, for instance, if the system has matured and we know about it more, or there has been an accident or an accident nearly occurred, or when maintenance and operating procedures have been changed. Alternatively, the equipment of the system was somehow modified: changes in environmental conditions, changes of operational parameters or changes of stress (Rausand, 2005).

2.2.3 The proposal for preliminary hazard analysis

Our proposal during the preliminary analysis is shown in figure 2. The proposal consists of a sequence of steps of two methods, namely preliminary hazard identification (PHI) and preliminary hazard analysis (PHA). The hazard analysis proceeds gradually from one step to another.

The individual steps of our proposal for preliminary hazard analysis:

2.2.3.1 Selection of risk

We will build on the results of the previous step and hence the list of risks. Gradually, we will select and analyse the individual risks of this list. After selecting a risk, we will continue identifying the causes of this risk.

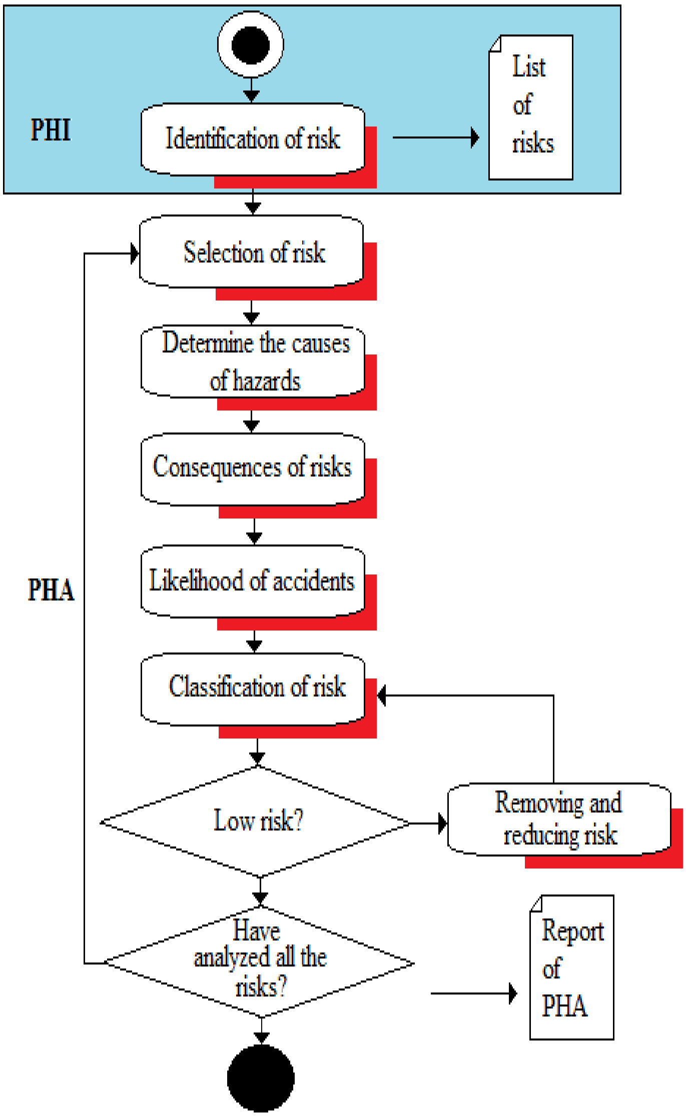

Figure 2: Proposal for procedure PHA.

2.2.3.2 Determine the causes of hazards

We must determine all the possibilities formation of individual risks. Based on the analysis of this step is possible to determine mechanisms for removing these causes or control the risk, which would have reduced the effects of threatening. Risk arises under certain conditions, especially if:

- There is a risk factor (source of danger).
- There is the presence of a risk factor for objects in dangerous levels of exposure.
- The object is susceptible (sensitive) to activities and factors which inducing hazards.

The output of this step is a list of causes of individual hazards. This list will be used later to eliminate all possible causes of risk. Where we cannot eliminate the causes of the risks, we propose mechanisms to control potential risks.

2.2.3.3 Consequences of risks

We use a hypothetical opinion in determining the potential consequences of risks. We assume that the mechanisms for removal respectively to control the risk reduce the consequences to a minimum. It is important to determine who and what everything is at stake in the formation of individual risk. The output will be a report of the potential consequences of the hazard. The report will include what the consequences are threatened in the presence of risk and a set of measures to reduce these effects.

2.2.3.4 Likelihood of accidents

A risk assessment depends on a set of factors. When we want to determine risk, we must estimate the frequency and severity of any accidents. The frequency of events may be classified into rather broad classes. An example of such a classification is (Rausand, 2005):

- Very unlikely once per 1,000 years or more rarely.
- Remote once per 100 years.
- Occasional once per 10 years.
- Probable once per year.
- Frequent once per month or more often.

The output will be a report containing the likely occurrence for each risk. At this step, we can use the database of previous accidents and accident statistics.

2.2.3.5 Classification of risk

There are many mechanisms to classify risk. It is especially important to determine properly the risk to the level of risk. We determine with the classification of risk, whether to reduce the risk or whether it has reached safety. If it needs to reduce the risk, we choose the security measures and the procedure is repeated. If adopted new measures, the designer must check whether arise the further risk of new threats. The emergence of other threats, they must be added to the list of threats. We can classify the risk using the following mathematical formula (Pačaiová, 2003).

$$R = P \times D$$

Where: R – degree of risk

P – probability of the event

D – consequence of the observed events

Level of risk (Rausand, 2005):

H – The high risk is unacceptable. Further analysis should be performed to get a better estimate of risk. If this analysis shows still unacceptable risk or medium risk, then design changes or other changes should be introduced to reduce the criticism.

M – The medium risk may be acceptable, but REDESIGN or other changes should be considered in the case as reasonably practical. In assessing the need for corrective action, we should take into account the number of events occurring at this level of risk.

L – The risk is low and further risk reduction measures are unnecessary.

2.2.3.6 Removing and reducing risk

After a risk analysis, it is necessary to design proper mechanisms to remove and reduce risk. These mechanisms remove a hazard completely or help us reduce the intensity of the hazard to an acceptable degree. The protective equipment must be safe for the operation of safety-critical systems and employees and the surrounding environment. When we have the recommended protective equipment, workers must be trained, and they must be familiar with the manner of its use. It is important that additional safety measures proposed in this step were sufficient.

2.2.4 The proposal for removing and reducing risk

The mechanism for the removal or reduction of risk is illustrated in figure 3.

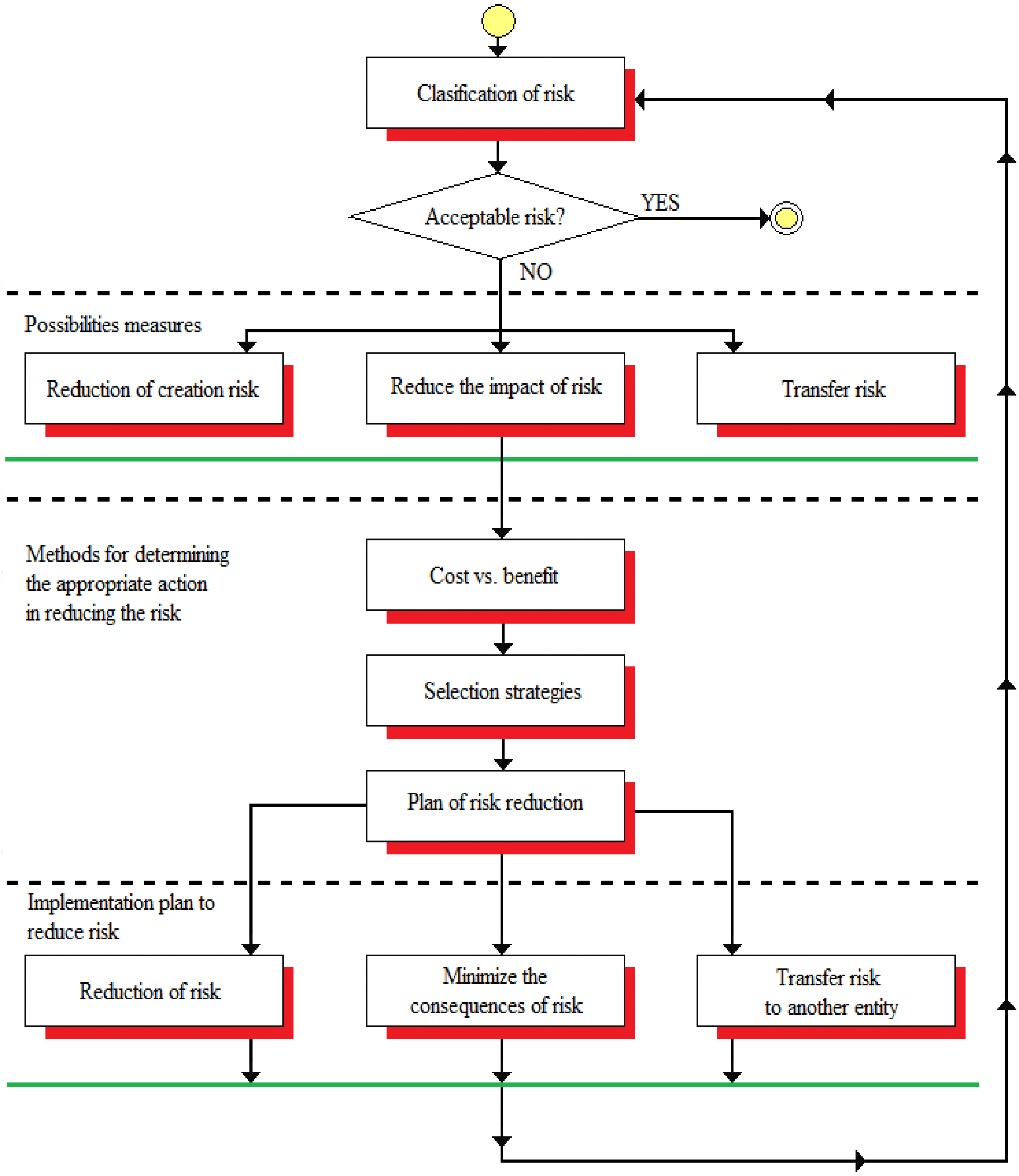
Clasification of risk
Acceptable risk?
YES
NO
Possibilities measures
Reduction of creation risk
Reduce the impact of risk
Transfer risk
Methods for determining the appropriate action in reducing the risk
Cost vs. benefit
Selection strategies
Plan of risk reduction
Implementation plan to reduce risk
Reduction of risk
Minimize the consequences of risk
Transfer risk to another entity

Figure 3: Proposal for procedure on risk elimination.

These principles will govern the comparison of cost and risk during regulation:

there should be a transparent bias on the side of health and safety. For duty holders, the test of ‘gross disproportion’ implies that, at least, there is a need to err on the side of safety in the computation of health and safety costs and benefits. Many companies adopt the same approach when comparing costs and benefits and, moreover, the extent of the bias (i.e. the relationship between action and risk) has to be argued in the light of all the circumstances applying to the case and the precautionary approach that these circumstances warrant.

Whenever possible, standards should be improved or at least maintained. Normally risk reduction action can be taken using good practice as a baseline – the working assumption being that the appropriate balance between costs and risks was struck when the good practice was formally adopted, and the good practice adopted then is not out of date. However, there will be cases where some form of computation between costs and risks will form part of the decision-making process. Typical examples include major investments in safety measures where good practice is not established.

2.2.4.1 Report of PHA

The output of the preliminary risk analysis respectively results of PHA, are used as input to a more detailed analysis of the risk. Reported as PHA by letter. Typical PHA letter contains various attributes such as: hazard, accidents, probable cause, an analyst for analyse, emergency preventive actions, hazard classification and others. We use the results of the step "determine the causes of hazards" in implementing risk reduction. We tried to eliminate these causes, reduce or move to another entity that is not serious threats.

2.3 Requirements for the control system

The aim of this step is to establish requirements for the safety analysis or requirements for the control of the 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 by an analysis of conditions obtained in step one. Each process has some set of states. In this step, we will work only with safety-critical states. By a detailed analysis of these states, we obtain the requirements for measurement, control functions during the states or requirements of the actuator controllers. We must take into account all relevant standards and the implementation safety-critical states to the 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). Using the Luenberger's observer is for deterministic states and Kalman's observer (filter) is for stochastic states, the determination of the methods and processes is for safety analysis. It is necessary to mention the top-down method, which allows us to decompose a system from a global perspective to the individual subprocesses.

2.4 Selection of a suitable method for safety analysis

The management of safety-critical processes requires a specific approach in engineering, the primary objective of which is the elimination or reduction of risks arising from running of safety-critical technological operations. As a rule, a demonstrable achievable level of comprehensive safety is required when implementing a proposal and effectuating functional safety principles (Mudrončík, 2009). Acceptable system security can be achieved using the right safety analysis methods.

2.4.1 Overview of the most commonly used safety methods

THERP (Technique for Human Error Rate Prediction)**:** A method of predicting human error intensity that describes and decomposes human activity in detail and depth, by selecting appropriate probability estimates of HEP (Human Error Probability) and based on the diagnostic model of the task it allows time quantification. THERP identifies the influencing factor of the human reliability of PSF and thus gives a detailed overview of the vulnerabilities and possible system failures (Havlíková, 2009).

FMEA (Failure Mode and Effect Analysis)**:** The method belongs to a group of fundamental analytical methods used in the quality management process, in the management of reliability and safety. It is one of the fundamental methods used in semi-quantitative risk analysis that is applied not only to production processes and products but also to services, financial, social and other processes. Currently, it is widely used in the automotive industry (Buganová, 2011).

FTA (Fault Tree Analysis)**:** The FTA, or Fault State Tree, proceeds systematically from the symptoms of the problems to their causes and provides a clear image of the causes of the failures at different levels. The use of the method leads to an increase in the reliability of the system since it allows investigating the causes of failure and determines the probable occurrence of the analysed key problem by estimating the probability of occurrence of elementary (primary) events.

SQMD (Situation-based Qualitative Monitoring and Diagnosis)**:** SQMD consists of quantitative and qualitative modelling methods. It uses hybrid models to monitor and detect real-time. This type of hybrid model combines the advantages of both methods as it contains qualitative and dynamic elements. In this way, we can imagine online monitoring and diagnostics for fault detection and localization in complex dynamic systems (Manz, 2002).

Each of these methods is used in a different area and provides a different perspective on possible safety risks and causes of failures. Their use provides an overview of the vulnerabilities and possible system failures and facilitates the detection and location of failures in complex systems (Havlíkova, 2009).

2.4.2 Selection of the appropriate method for modelling safety-critical processes

To develop a suitable method for monitoring dynamic technology systems, the following objectives must be taken into account:

1. Modelling dynamic systems.
2. Observing dynamic systems.
3. Analysing errors of dynamic systems.

Based on these objectives, there are the following solutions. Signal-oriented methods are used the most extensively. They detect errors in the technical process directly from the measured quantities. Controlling the limit values where physical quantities change only in certain pre-specified limit values is the simplest form of process control. As soon as the controlled quantities, such as level, temperature or concentration drop or exceed the pre-set limit value, the alarm is activated (Frank, 1994).

In many cases, this type of control is not sufficient. Therefore, it is more effective to apply analytical process knowledge in the form of process models, which model the real system. At the same time, the existing dependencies of the process variables are mutually analysed on the basis of the measured variables so that is it possible to provide (perform) reverse decisions on the erroneous course. These modelling-based methods have the advantage that they can recognize more errors in comparison to the examination of the limit values or can also "predicted" some errors (Frank, 1994).

As a rule, quantitative process models are used to control the process with the model, and analytical redundancy is used. These procedures are often not applicable to complex systems. For this reason, qualitative models are also used to control the process. The next section outlines different quantitative and qualitative procedures for model-based process control (Frank, 1994).

Detailed system analysis can provide all the information necessary for safety analysis. Based on the system analysis, selecting the appropriate method for creating models required for automated monitoring of dynamic system operation is much easier. We propose to use the SQMD (Situation based Qualitative Monitoring and Diagnosis) method for developing models for the 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 the advantages of both methods. On-line monitoring and diagnostics to detect and locate 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 existing mathematical models that are combined with qualitative models 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 to require less processing power (Manz, 2004).

2.5 Modelling safety-critical processes of dynamic systems

The automation of continuous-discrete technical processes greatly depends 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 is often mathematical models, to get 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 the state respectively an estimate of parameters. Qualitative procedures for complex systems based on these problems are also taken into account. The qualitative models may not accurately reflect internal physical connections, only those situations when something "does" are included in models. The qualitative model distinguishes these situations and allows the characterization of complex systems. The disadvantage of qualitative models is mainly that the dynamic properties cannot be at all or only very inaccurately described. However, this is a necessary condition for the control of the 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 the description of the dynamics (Manz, 2004).

One way to get these complications under control is to combine qualitative and mathematical models to create a hybrid model. Within the research topic “The development of hybrid component models for monitoring of complex dynamic systems” the SQMD method was developed (Situation based Qualitative Monitoring and Diagnosis).

The method is characterised by simple, precisely component-oriented modelling. Components without remembering the effects of the technical process are modelled only qualitatively. In this case, the proposer assigns to each physical variable a different range of values that qualitatively describe the correct and flawless function of the component. The dynamic description is needed only for memory components and is used to model the dynamic properties of systems with a qualitative model.

Within the on-line inspection, all components and reduced state space are linked to each other within a certain time window. This is based on the hybrid model components, system structures and data from sensors and actuators in the engineering process. The reduced state space can be examined for possible error properties of the technical process.

In this step, it is important to describe correctly 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 fuzzy logic to create qualitative models of individual processes. Alternatively, Petri nets can be used for causal networks 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 other 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.

2.5.1 Introduction to model development and process control

The errors and failures of the hardware components, software errors or errors in the design, which have not been taken into account for the operating conditions, may cause dangerous situations in the operation of technical processes. The role of an appropriate model of the process is to provide quantitative or qualitative measurable parameters concerning the properties of the system and from these, we can in real-time detect deviations during the process. The models that should be deployed in the controlling process rarely meet the requirements of a simple description of reality. Regarding 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. Except for models for the desired operating conditions also appropriate models for degraded modes of the operation arise in this way. When checking the models for the desired state, these are compared with the course of reality. As soon as a discrepancy is found between the model and reality, it is considered 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 (Fröhlich, 1996).

2.5.2 Modelling tasks

Models that should be deployed in process control rarely meet the requirements of the simple description of reality. Regarding the inspection in addition to the description of the required mode of operation, it is necessary to identify additionally all possible errors in the real process to reflect them in the model. Besides the models for the required operating states, this also results in corresponding models for the operating fault states. During the control, models are deployed for the required states, and they are compared with the course of reality. Once there is a discrepancy between the model and reality, it is considered a failure. In this case, the error mode models determine the type and location of the error (Fröhlich, 1996).

An important task of model development is, therefore, to take into account all possible model errors. These approaches are described in the following chapters (Fröhlich, 1996).

2.5.2.1 Types of errors in technical processes

Errors in automatized systems can occur everywhere both in the engineering process and in the control system, i.e. in the process management system and it's technical and software means. Since the control electronics are usually operated in a suitable environment, they are less susceptible to errors than the parts of devices that typically operate in a "rougher process environment". Therefore, errors in the technical process are usually considered (Frank, 1994).

According to figure 4, there are different effects of errors on the technical process, on actuator errors, on process components and sensor errors. Errors can be generally described as external effects. Besides these, they often occur in the process malfunctions and parameter deviations, which are not critical to the process and, therefore, may not be detected, but which may cause error diagnostics, particularly in model-supported methods. These effects can be considered unknown input variables, contrary to the known input variables (Frank, 1994).

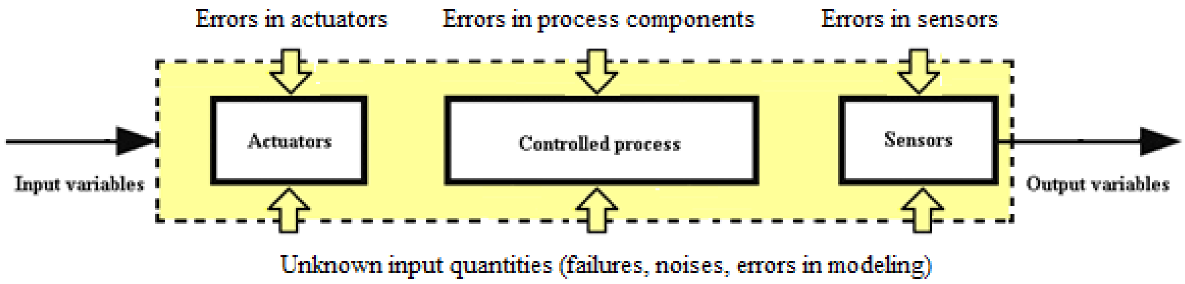

Figure 4: Different effects of errors in the technical process (Frank, 1994).

Errors can be recognized as deviations of process parameters or deviations of state variables. Most errors are reflected in the parameter names. Only selected specific errors, such as short circuits in electrical systems or cracks in the pipeline, directly affect state variables (Frank, 1994).

2.5.2.2 Error modelling

Based on process knowledge and experience, the following types of models are used for modelling:

- Models for fault-free operation (model for the desired mode)
- Fault Mode Models (model for error mode; Lauber 1, 1999).

Models for fault-free operation describe the required behaviour of the system under test. They copy the process with sufficient accuracy. If anomalies begin to occur in the process, the corresponding characteristics will be changed without permission. This characteristic can be, for instance, a process variable, the course of which does not correspond to the displayed properties (Lauber 1, 1999).

The characteristic deviation, i.e. residue can still be recognized in the desired model, but not localize and assess its effects. For this purpose, the error operation model is used (Lauber 1, 1999).

The fault mode model describes how errors and outages affect the technical process. These effects are called "error signatures". Based on these error signatures and the residues created, there is a possibility to determine the type and location of the emerging errors (Lauber 2, 1999).

2.5.2.3 Process control tasks

Regardless of the type of model, the basic tasks and objectives of the models for control are described first. The following tasks are relevant for process control:

- Examination of the current process status from the measured process signals and status indication for service personnel,
- Examination of the defective subsystems caused by deviations from the regular operation and, consequently, induced incentives for action taken by operations personnel,
- The output of alarm messages for immediate outages,
- Automatic protection of technical equipment in hazardous or emergencies,
- Early recognition of emerging errors and outages (Lauber 2, 1999).

2.5.3 The development of model and control 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.

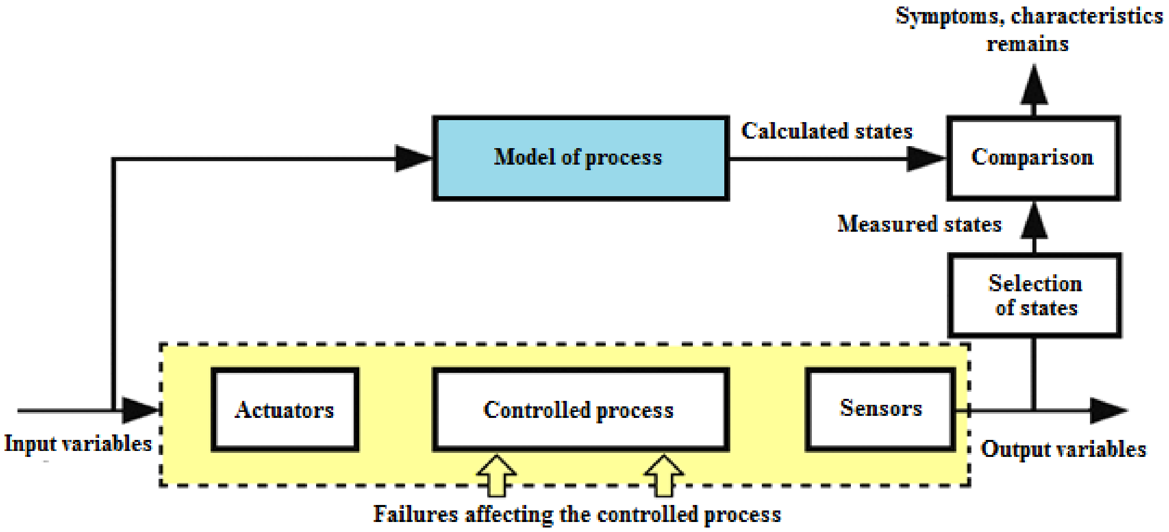

Figure 5: Principle of control based on the model of the real process.

Figure 5 shows the principle of control loaded at the model. The process model is carried out online, i.e. parallel to the controlled process. Based on the input data is impossible to determine the behaviour of the real process using output values (measured situation). This measured behaviour 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 (Lauber 1, 1999).

There are different types of process models that are used for control. A more detailed description of these models is presented in the following section.

2.5.3.1 Classification of procedures on the basis of model in process control of dynamic systems

In many scientific fields, two different modelling procedures are used for control. On the one hand, there are analytical methods based on models derived from classical control (control theory). These methods use quantitative dynamic models to estimate non-measurable quantities or parameters for error detection. On the other hand, qualitative models that were developed in the field of AI have been used more intensely in recent years. A special type of qualitative models is applied to a qualitative evaluation of physical process models (Fröhlich, 1996).

The difference between qualitative and quantitative models lies in the degree of abstraction and is presented in figure 6. The starting point of modelling is the real system. A qualitative model is obtained by dividing the real system into components and informally describing the relations between the components. With the increasing degree of qualification of the form of expressions, they are always more formal, and the syntactic rules of expression become more precise. This quantification is performed by accurate transcription of the relation between the components in which exact rules of mathematical notation are used. The result is a quantitative model from which quantitative methods can describe the quantitative behaviour of the system (Fröhlich, 1996).

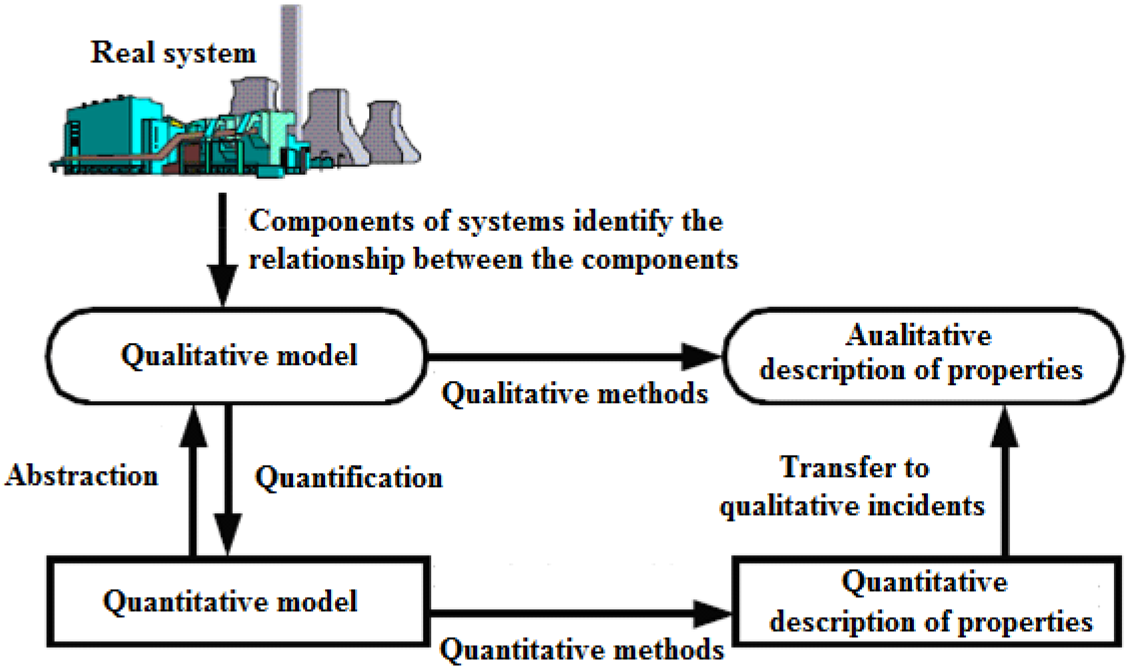
Real system
Components of systems identify the relationship between the components
Qualitative model
Qualitative methods
Aualitative description of properties
Abstraction
Quantification
Transfer to qualitative incidents
Quantitative model
Quantitative methods
Quantitative description of properties

Figure 6: Degrees of abstraction in qualitative and quantitative description (Fröhlich, 1996).

The most important quantitative and qualitative modelling procedures are described below. An overview is presented in figure 7. It takes only mathematical models without and with the estimation of the unknown quantities of the process into consideration as quantitative models. Causal networks or qualitative variables can express qualitative models. A more detailed breakdown will be presented in the following chapters (Fröhlich, 1996).

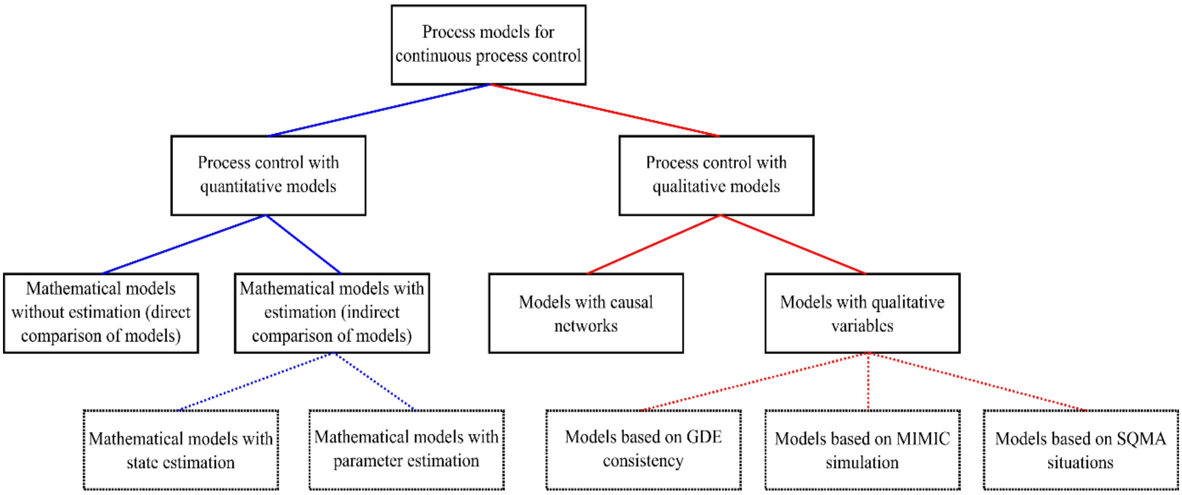
Process models for continuous process control
Process control with quantitative models
Process control with qualitative models
Mathematical models without estimation (direct comparison of models)
Mathematical models with estimation (indirect comparison of models)
Models with causal networks
Models with qualitative variables
Mathematical models with state estimation
Mathematical models with parameter estimation
Models based on GDE consistency
Models based on MIMIC simulation
Models based on SQMA situations

Figure 7: Classification of process models for continuous process control (Fröhlich, 1996).

2.5.4 Process control based on quantitative models

Quantitative or mathematical models of processes enable an accurate description of the process. They are in the form of differential or difference equations, and these provide dependencies of the measured input and output signals so it can provide corresponding statements about system properties. Based on these measured values of signals, it is also possible to estimate internal variables such as parameters and states. This estimate is necessary for error location (Lauber 2, 1999).

Quantitative models are deterministic, compact and adaptable. Deterministic means that quantitative models allow accurate prediction of system behaviour. The system of equations describes the time course of output quantities for all initial conditions and for the time course of input quantities (Lauber 2, 1999).

Models can be used when the accurate prediction of system behaviour is required and all included parameters are measurable. In addition, the current state of the system must be known, which is expressed by the initial conditions of differential or difference equations. When using the quantitative process models for error modelling, the measured properties of the real process are compared with the properties that are determined by the mathematical model for the detection and location of errors and outages. While using mathematical models, a distinction is made between methods of direct and indirect model comparisons. Unlike direct model comparisons, indirect model comparisons include estimates of unknown input variables (Lauber 2, 1999).

2.5.4.1 Direct comparison of models

The direct comparison of models compares the characteristics of the model specified by the prescription directly with the properties of the real technical process, as shown in figure 8 (Lauber 2, 1999).

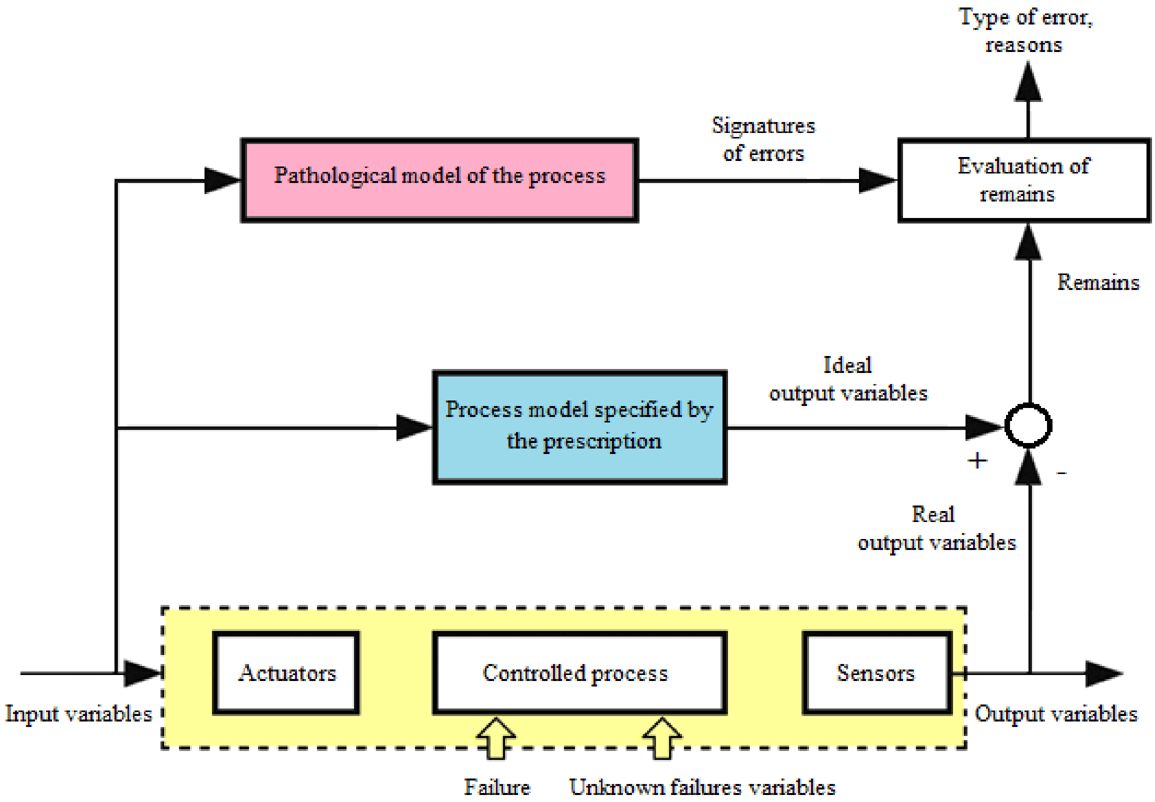

Figure 8: Process control by direct comparison of model.

The process model specified by the prescription (required model) creates a set of ideal output variables with the same input variables that affect the real process. The difference between ideal and real output quantities determines the residue. If the residue is within predetermined threshold values, it is the desired operation. However, if the residue is outside the threshold values, it is an error (failure) and the next step is to analyse the error based on the pathological model into which the same input varies. This procedure is referred to as residue evaluation. It is a logical decision-making process that transforms quantitative knowledge into qualitative knowledge. The aim is to decide when and why an error occurred (Lauber 2, 1999).

If not all process parameters or state variables are measurable, the indirect model comparison is followed (Lauber 2, 1999).

2.5.4.2 Indirect model comparison

In the indirect comparison of models, measurable quantities are observed. Based on measurable quantities and the application of certain algorithms, there is a possibility to estimate non-measurable quantities. The internal process variables that are not directly measurable and therefore must be estimated are state variables and real process parameters. On this basis, the terms “state estimation” and “parameter estimation” are important means for control (Lauber 2, 1999).

2.5.4.2.1 State estimation

In the indirect comparison of the model with the state estimate for the estimation of non-measurable quantities, a state observer is used. The state observer also referred to as a Luenberger observer, is also used in classical control theory when not all state variables are measurable in a regulated system. There must be a mathematical model of the state space for state estimation.

Figure 9 shows the process control by indirectly comparing a model based on state estimation using a status observer (Lauber 2, 1999).

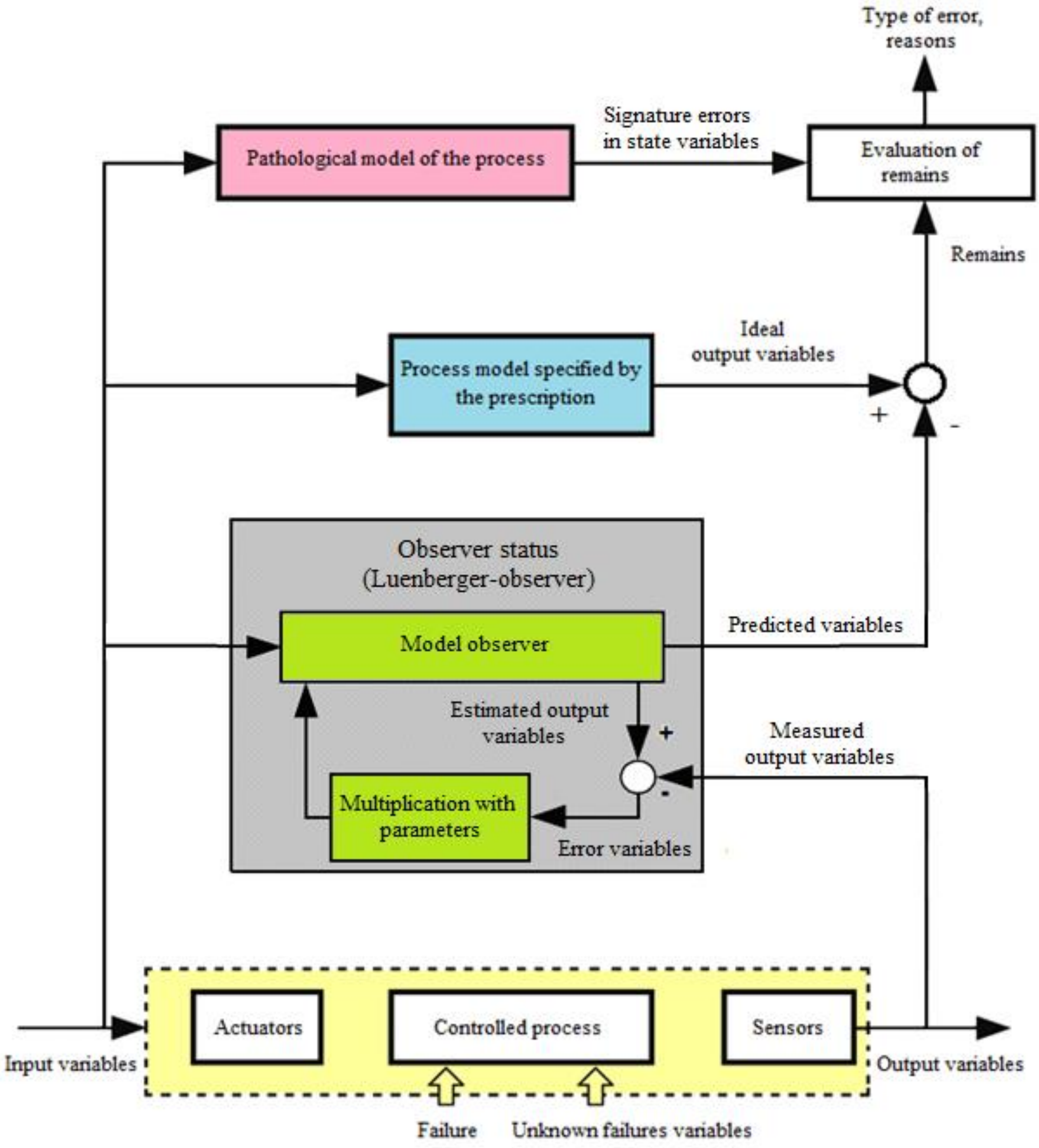
Type of error, reasons
Signature errors in state variables
Pathological model of the process
Evaluation of remains
Remains
Ideal output variables
Process model specified by the prescription
+
-
Observer status (Luenberger-observer)
Model observer
Predicted variables
Estimated output variables
+
Measured output variables
-
Multiplication with parameters
Error variables
Actuators
Controlled process
Sensors
Input variables
Output variables
Failure
Unknown failures variables

Figure 9: Process monitoring with model observer (Lauber 2, 1999).

When evaluating the direct comparison of the models of figure 8, the state observer providing the estimated state variables is placed before the desired and pathological model. The status observer contains the observed model. Thus, the output quantities are estimated from the input quantities. These estimated output quantities are compared with the real measured output quantities. Error variables are derived from the difference. These are multiplied with appropriately selected parameters to bring the state variables of the model closer to real state variables. If the desired match is obtained, the multi-application parameters for correcting the error of state variables in the model are stored and the state variables are estimated based on the corrective factor. By comparison with the desired state variables, it forms a residue. Residue evaluation is performed using error signatures of status variables, so it is possible to make a backward decision on the error and causes (Lauber 2, 1999).

2.5.4.2.2 Parameter estimation

When comparing models indirectly with parameter estimation, the observer model is deployed in parallel to the real process. One possibility of parameter estimation is shown in figure 10, analogous to state observer, error variables are generated from the difference between model output variables and real output variables. Here, the estimation of the model parameters is based on deviations, so they change until the sum of the squares of deviations is minimal (Lauber, 1995).

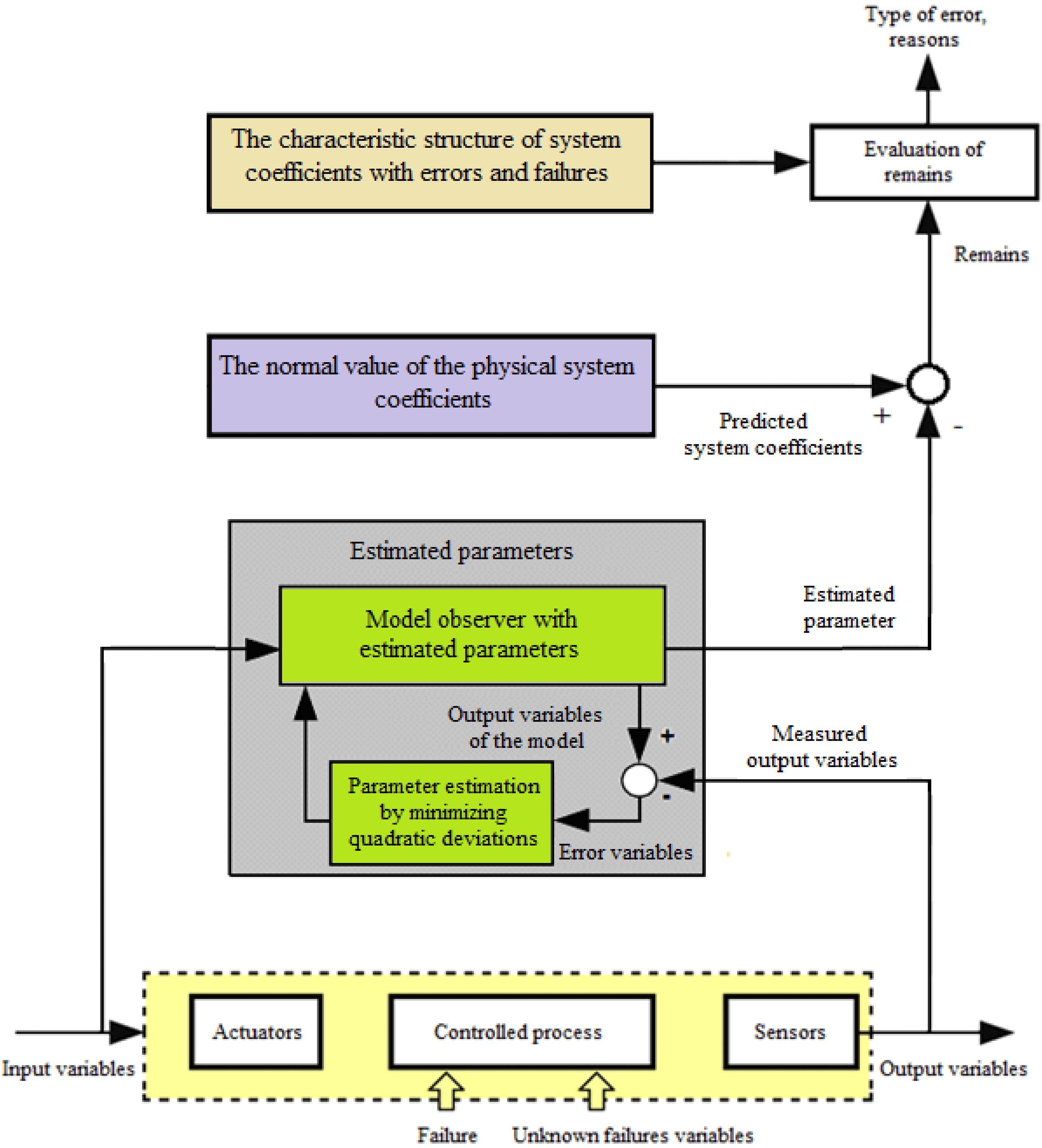
Type of error, reasons
The characteristic structure of system coefficients with errors and failures
Evaluation of remains
Remains
The normal value of the physical system coefficients
Predicted system coefficients
+
-
Estimated parameters
Model observer with estimated parameters
Estimated parameter
Output variables of the model
+
Measured output variables
Parameter estimation by minimizing quadratic deviations
-
Error variables
Actuators
Controlled process
Sensors
Input variables
Output variables
Failure
Unknown failures variables

Figure 10: Process control by parameter estimation (Lauber, 1995).

From the estimated model parameters, it is possible to calculate the system coefficients on which the model parameters depend. Based on the aforementioned, it is possible to estimate the unknown coefficients of the system. A residue is a change in the system coefficient from normal values. This residue is compared with the characteristic changes in system coefficients for deviations and outages. The result of this residue evaluation then determines the error and its cause (Lauber, 1995).

2.5.5 Process control based on qualitative models

In many practical cases, the controlled process is so complex or difficult to understand that it is not possible to assemble its accurate or estimated quantitative model. However, this is not always necessary for all process control tasks. Often it is sufficient to know only the system events that are important as a threshold check. In such cases, quantitative models can substitute qualitative models. In such models, the signals are described roughly, for instance, by intervals (Lauber, 1995).

The deployment of the qualitative models follows the structure described in figure 5. The qualitative process model runs in parallel with the real process and calculates the corresponding qualitative output quantities from the input data. Output quantities are compared with real output quantities, and on this basis, the possible types of deviations and location of deviations are evaluated. Qualitative models are deployed (applied) when the following characteristics are missing from the system under review:

- **Incomplete process knowledge:** due to the complexity of the system, it is not possible to describe the overall behaviour of the process, or some process parameters are unknown.
- **Incomplete measurement:** system variables can only be measured inaccurately (very roughly).
- **An accurate prediction** of system properties is not necessary, it is sufficient to describe only the key characteristics and qualitatively different forms of system movement (Lauber, 1995).

Where the relevant quantitative model is not suitable for the generation of residues according to the previous characteristics, the residues shall be generated using a qualitative model. For this purpose, it applies causal networks or models with qualitative variables as already shown in figure 7 (Lauber, 1995).

2.5.6 Models with causal networks

Causal networks (Rays/Probabilistic networks) are cause-effect relationships for residue evaluation and deviation diagnostics. In doing so, they evaluate the possible relationships between all causes of deviations and effects to assess the causes of misconduct. This “causal evaluation” can be used for prognosis and diagnosis and may itself be very incomplete. The causal network is a graphical notation of a mathematical model for system dependencies. Oriented links represent a direct impact. Quantitatively, oriented links can be described by conditional probability. The consequences are drawn along both the connection and the direction of the oriented connection. Compared to other methods, causal networks provide a significant advantage in that uncertain contexts may adequately describe the application of the “laws of probability theory” (Lauber, 1995).

As an example, figure 11 shows a part of the causal graph for the process of washing. The causes are on the left there and the effects on the right. These effects result in events or outages or observable symptoms. For example, the “laundry is dry” status can be transferred back to the “power failure" or "water supply valve closed" event via the "water supply blocked" event. In this way, the error diagnostics is carried out by reversing the known symptoms. The conclusion on the causes in not always unambiguous (Fröhlich, 1996).

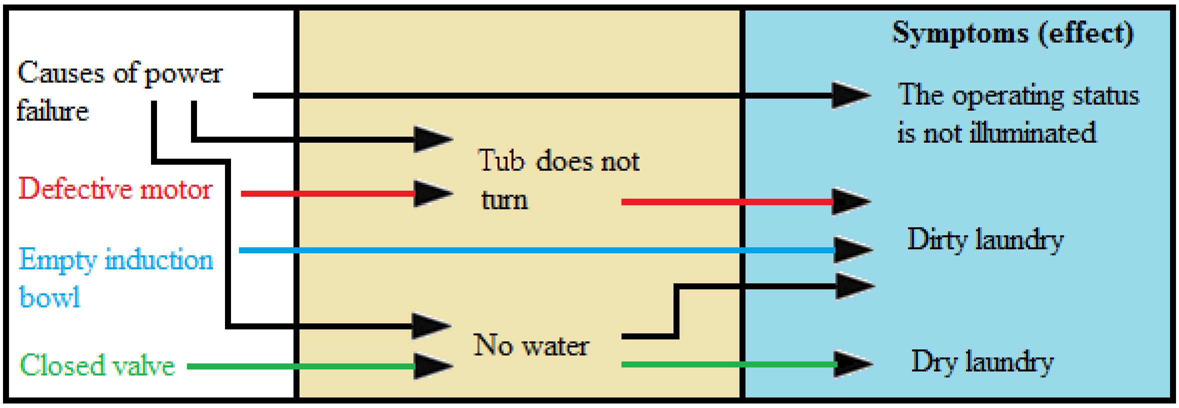

Figure 11: Causal graph of washing process (cut-out).

The causal model contains in-depth knowledge and represents knowledge of the mutual effects and their directions. The problem of causal networks is that it cannot take all process states into account. The proposal for the causal network depends on the knowledge of experts, and it is very difficult to automate. This approach makes it complicated to describe fully the properties, as it is very easy to forget the causes and symptoms. Using models with qualitative variables can eliminate these problems (Fröhlich, 1996).

2.5.7 Models with qualitative variables

The application of qualitative variables for model-oriented process control comes from the field of qualitative deduction. The basic idea is to solve the natural human speech as a means of expression and thus to approach human deduction. This concept was first used in the 1970s by Zadeh, using the linguistic variables in fuzzy logic. The development of fuzzy logic shows that qualitative models based on verbal expression can be applied effectively (Zadeh, 1975).

The deployment of qualitative variables is based on model analytical processes that represent deep knowledge, similar to quantitative models. The advantage in the application of qualitative variables is a qualitative interpretation of the process flow based on qualitative arithmetic. First, the numerical space is discretized in such a way that the continuous quantities of the real process are transformed into the discrete region. Qualitative arithmetic is an important evaluation of quantitative dependencies of physical process quantities. For this reason, the most important basic operations must be applied. It is important for qualitative inferences that each discrete area is assigned a symbol or a linguistic concept. These differences, which were created by discretization, apply to the type of deduction (Forbus, 1984).

The qualitative expression is firstly performed on the basis of a range of variable values so that the real process variables are divided according to defined ranges of values or intervals, and secondly, it is performed on the basis of fuzzy variables so that the defined intervals are expressed by a function of belonging to fuzzy logic. The simplest variables according to the value range are signum variables that were developed for AI under the name qualitative physics. Signum variables take only three qualitative values {−, 0, +} and correspond to the sign of the relevant quantity. The extension of signum variables represents a qualitative description of process variables with interval variables. Instead of only three (predicted) intervals used, the "negative", "zero" and "positive" ranges are divided into any number of intervals (Forbus, 1984).

2.5.7.1 Situation-based models

SQMA (Situationsbasierte Qualitative Modellbildung und Analyse) is a situation-based qualitative modelling method. SQMA contains ENVISION and QSIM models with approximately the same characteristics.

System description: the system description is component-oriented, based also on the "No-function-in-structure" principle. As in ENVISION, the system model contains structure information and a description of the behaviour of individual components (Manz, 2000).

Qualitative variables: discretization is done by interval variables with strictly determined limits. Each physical quantity of a component is assigned different intervals that describe the normal and error-loaded behaviour of the component (Manz, 2000).

Qualitative description of behaviour: all combinations of qualitative variable intervals create a complete situational table for the components. Based on situational rules, qualitative variables are assigned to each other analogously to physical laws to remove physically impossible situations from the situational table. The resulting table contains only situations that describe the required and error behaviour of the component. With commented rules, similar situations can be sorted and tagged. Consequently, the transfer rules allow specifying transitions between situations (Manz, 2000).

Process control: SQMA was developed primarily for safety analysis, which is performed in offline system operation (mode); (Lauf, 1996). To verify the dynamic properties of the component, the dynamic model equations that were derived from differential equations were introduced to verify the SQMA method. The resulting SQMA model was deployed in parallel to the technical process and evaluated on-line. The evaluation aims to estimate the parameters for the immediate control cycle.

The advantage of SQMA lies in its focus on components that are used also in GDE. Unlike the GDE, signing arithmetic was extended to freely defined intervals, which are also used in QSIM. Situation orientation and the assignment of markings or comments for each situation allow the development of clear models. Dynamic properties are oriented through component model dynamic equations. It means that overlapping parameter links that are interconnected by time relationships cannot be taken into account in the components. Next, hard boundaries of the interval allow only hard transitions, which are generally determined by specific parameter thresholds. These do not correspond exactly to reality, and it is advantageous to determine the intervals with an evaluation function with which fine transitions can also be realised. This is possible with, for example, fuzzy-variables (Manz, 2000).

2.5.8 Evaluation of the described models and the resulting requirements

Following the introduction of the most important quantitative and qualitative methods for process control, their shortcomings are summarized and compared. This implies requirements for the formulation of the task in this work. The criteria follow the evaluation of the described quantitative and qualitative methods and the deduction of deficiencies according to table 1. It divides these criteria into the areas of modelling, observation and error analysis (Manz, 2000).

Table 1: Catalogue of criteria for the evaluation of quantitative and qualitative methods (Manz, 2000).

	Criteria	Description
Modelling	Treatment of functional complexity	The relations among quantities are little known, difficult to describe or very difficult to calculate.
	Treatment of structural complexity	There are many variables in the systems that have interrelated relationships.
	Component-oriented modelling	For complex systems, the possibility of decomposition and hierarchization of the system is important.
	Automated modelling	Support for modelling with, for instance, an existing component library, automated structural analysis, etc.
	Deterministic behaviour	Process behaviour can be observed also with incomplete or inaccurate information to derive reliable conclusions about the process.
Observation	Processing incomplete or inaccurate information	Also, with incomplete or incorrect information, to derive reliable conclusions about the process.
Error analysis	Control of complex dynamic systems	The model must be evaluated on-line and continuously (in real time), which must not be time-consuming.
	Reliable prediction of the behaviour of complex dynamic systems processes	A reliable evaluation of the observed process behaviour must also be possible in complex dynamic systems.

2.5.8.1 Deficiencies in process control with quantitative models

Table 2 contains the evaluation of quantitative methods in process control by comparing individual models according to the criteria catalogue. The benefits of a quantitative approach lie in several criteria. For example, quantitative models allow a deterministic approach. This is, however, solved in indirect comparison with the process behaviour model based on estimated state variables or values of parameters, nevertheless, it is possible to base on high reliability of prediction. The disadvantages of the quantitative method are the lack of the possibility of component-oriented modelling. Dependencies of physical quantities are found in several components. Structural complexity is generally described in one system of differential equations. Consideration of these dependencies is associated with complications in dynamic systems, and it makes it difficult to automate model building. Moreover, not all relationships between quantities are always known. This limits the modelling of functional complexity and the processing of incomplete and inaccurate information. Consequently, the control of dynamic systems based on quantitative models is associated with problems (Manz, 2000).

Table 2: Evaluation of the deployment of quantitative models for process control (Manz, 2000).

		Direct model comparison	Indirect model comparison	
			Status estimation method	Parameter estimation method
Modelling	Treatment of functional complexity	◐	◐	◐
	Treatment of structural complexity	◐	◐	◐
	Component-oriented modelling	○	○	○
	Automated modelling	○	○	○
	Deterministic behaviour	●	●	●
Observation	Processing incomplete or inaccurate information	○	●	◐
Error analysis	Control of complex dynamic systems	◐	◐	◐
	Reliable prediction of dynamic systems processes behaviour	●	●	●

● – fulfilled, ◐ – partially fulfilled, ○ – unfulfilled

Block-oriented simulation programs (e.g. MATLAB/Simulink) are an exception. However, these do not facilitate the treatment of structural complexity and will therefore not be further explained.

2.5.8.2 Deficiencies in process control with qualitative models

Table 3 evaluates the qualitative models of the criteria catalogue. The question is whether the deficits of the quantitative model in table 2 can be compared with the qualitative models. The consideration of table 3 shows that qualitative modelling has advantages where quantitative modelling has constraints. These advantages are found especially when considering functional complexity. The interdependencies of physical quantities may not be described mathematically accurately, but abstracted models concentrate on a description of behaviour that is sufficient for control. Accordingly, it is also possible to process incomplete and inaccurate information in dynamic systems (Manz, 2000).

Nondeterministic behaviour is considered the disadvantage of qualitative models. It is then difficult, especially for complex systems, to make reliable process behaviour predictions. This problem, coupled with the 'combinatorial explosion' problem, makes the control of dynamic systems more difficult. The combinatorial explosion means that, as the complexity of the system increases, the size of the qualitative model grows exponentially (Manz, 2000).

Table 3: Evaluation of the application of qualitative models for process control (Manz, 2000).

		Causal networks	Qualitative variables		
			ENVISIOM/ GDE	QSIM/ MIMIC	SQMA
Modelling	Treatment of functional complexity	●	●	●	●
	Treatment of structural complexity	○	◐	◐	◐
	Component-oriented modelling	○	●	◐	●
	Automated modelling	○	●	●	●
	Deterministic behaviour	○	○	○	○
Observation	Processing of incomplete or inaccurate information	●	●	●	●
Error analysis	Control of complex dynamic systems	◐	◐	◐	◐
	Reliable prediction of the dynamic systems processes behaviour	○	◐	◐	◐

● – fulfilled, ◐ – partially fulfilled, ○ – unfulfilled

2.5.9 The selection of a suitable method for controlling the processes of dynamic systems

When comparing table 2 and table 3, it is clear that the control of dynamic systems cannot be adequately ensured by quantitative or qualitative methods. In quantitative methods, this deficiency stems from the fact that this method cannot model functional complexity. Furthermore, the possibility of component-oriented modelling and system hierarchy is absent. These deficiencies do not occur in qualitative models. Here, there are no deterministic modelling methods and partly satisfactory modelling of structural complexity. For this reason, it is confirmed that complex engineering applications alone are neither sufficient for quantitative nor qualitative models (Lunze, 1995).

This implies a partial aim of this work, to develop models (in this case combined) for sufficiently precise control of dynamic systems and thus minimize the shortcomings of both forms of models. The combined models will hereinafter be referred to as hybrid models. It is now necessary to derive from the tables the best appropriate combination of quantitative and qualitative models.

2.5.9.1 Selection of a suitable quantitative method according to table 2

Any suitable mathematical model can be used as a quantitative method. Methods of differential equation systems that describe dynamic behaviour are based on direct or indirect model comparisons. In most cases, it is sufficient that only known process variables in the quantitative model are used for further processing. In this case, measured values for qualitative models are further used in direct comparison with the model. Also, however, it is left as an open principle option to apply estimation methods (Manz, 2000).

2.5.9.2 The selection of suitable qualitative method according to table 3

In the aforementioned methods, the principle of decomposition and the associated hierarchy of the dynamic system have proven to be an important indicator of modelling. Accordingly, only GDE and SQMA are applicable from table 3. Unlike GDE and the used signum variables, SQMA provides freely definable intervals for flexible modelling of structural complexity. Based on this, SQMA provides a suitable platform for further development in conjunction with quantitative models. By selection, it can be deduced that mathematical models can be effectively combined with SQMA models. This combination is the basis for further investigation (Manz, 2000).

2.5.10 Resulting requirements for dynamic system process control

Concerning the selected hybrid form of the model in the previous chapter, the defined objectives of the work will be further modified and organized into requirements. This arrangement is essential for the concept of a practical combination of mathematical models with SQMA models and the concept of deployment options for process control. The first aim concerns the modelling of dynamic systems. This requires a simple and fast assembly of the model. In particular, models need to include sufficient information both to reduce the non-determinism typical for qualitative models and secondly to integrate the static and dynamic behaviour of the system, considering the errors. Accordingly, the following requirements may be specified for the first aim:

1. **Modelling of complex dynamic systems** (Manz, 2000)**:**
   1.1. Simple and quick assembly of the model;
   1.2. Reduction of nondeterminism;
   1.3. Modelling of static and dynamic system properties (including error properties).

Once models are assembled, it deploys these requirements to observe dynamic systems. It requires rapid observation of current behaviour and an estimate of future behaviour (including error properties). Based on the above, it is possible to specify the requirements for the observation area:

2. **Observation of complex dynamic systems** (Manz, 2000)**:**
   2.1. Observation of the immediate behaviour (including the error properties);
   2.2. An estimate of future behaviour (including the error properties);
   2.3. Rapid observation.

Observation of dynamic systems is part of the process control and a prerequisite for error analysis. Especially for this third aim, special methods and procedures had to be developed for real-time detection of unwanted behaviour and real-time implementation. There must be no or minimal misinterpretations.

These requirements are defined as follows:

3. **Error analysis in complex dynamic systems** (Manz, 2000)**:**
   3.1. Real-time detection of unsolicited behaviour;
   3.2. Real-time measures;
   3.3. Misinterpretations, none or only a limited number.

2.6 State space reduction

The focus of the overall concept is the on-line state space reduction, allowing monitoring of dynamic systems. After constructing 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 the time interval specified in advance. It contains all the possible states of the system for a defined time interval. These states can be evaluated in the following point of the methodology, in the on-line failure analysis.

2.6.1 Overview of on-line state space reduction

Figure 12 shows the second step of the overall concept. This fulfils the second requirement of "Dynamic System Monitoring" and includes online state space reduction. The aim is to specify a reduced quality state space for a predetermined time interval (time window) $[t_a, t_b]$ for $0 \leq t_a \leq t_b$. It contains all possible states of the system for a predetermined time interval and they can then be evaluated in the third step of the on-line analysis.

The state space reduction is periodically carried out by the SQMD observer illustrated in figure 12 in three consequent sub-steps 2a, 2b, and 2c. The following sub-steps include specifically the following activities (Manz, 2004):

- **Determination of quantitative trajectories (2a)**

In the first partial step, the current sensor and actuator data are used, as well as dynamic descriptions of the used hybrid model. This input is processed by the observer during the operation of the technical process. Also, a certain time interval $[t_a, t_b]$ is determined for the calculation in advance. A trajectory calculation based on the dynamic model is performed for this time interval. Based on the initial and final states of the calculated quantitative trajectories, it is possible to perform a reduction of all the qualitative components of the model in the next partial step.

- **State space reduction on the level of components (2b)**

At the component level, all situations determined by the initial and final states of the quantitative trajectories and the qualitative description of the components that the trajectories do not cross (which do not lie on these trajectories) are abolished. The course of the trajectory from start to end is derived from qualitative transactions (transitions). This leads to a reduction of the situation tables of all components. The reduced situation tables contain relevant information valid for the time interval and are included in the reduced system model in the next step.

- **Composition of the components (2c)**

In the last partial step, the composition of all qualitative components of the model takes place. The result of the composition is a reduced qualitative state space of the system. This is examined in the next step in the on-line analysis for adverse and dangerous conditions.

The advantage of reducing the state space at the component level is the removal of the combinatorial explosion. Analysis and evaluation are not carried out in the whole state space but are performed only for the time corresponding to the relevant part of the space. Direct evaluation 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. It increases the accuracy of the model in this way (Manz, 2004).

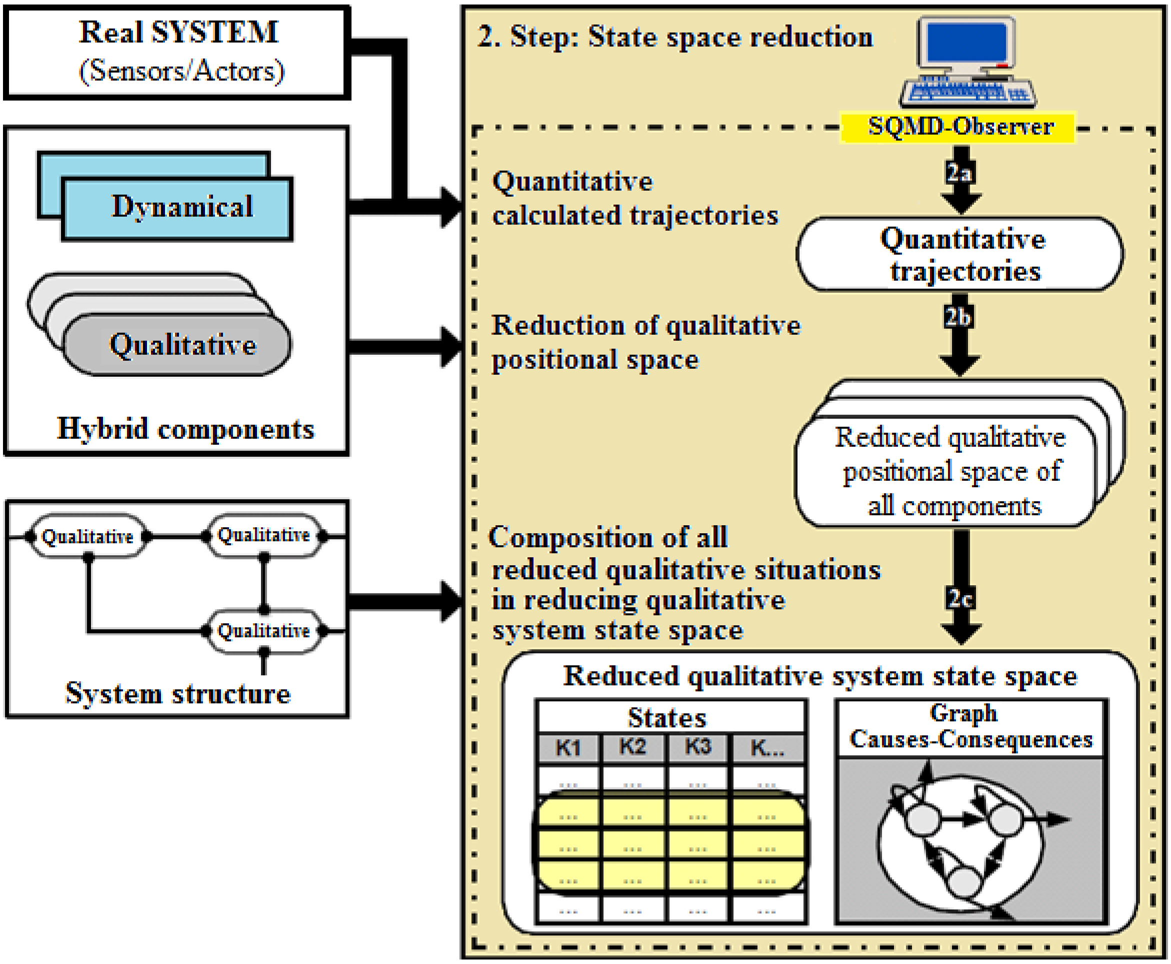

Figure 12: Concept of state space reduction (Manz, 1999).

2.6.2 Quantitative calculation of trajectories

Quantitative trajectories are determined by dynamic model equations. Their numerical solutions are obtained by the commercial simulation tool MATLAB/Simulink. The vector method of writing equations 1, 2 to describe a dynamic system has a simple geometric explanation. The elements of the state vector x can be considered as coordinates of a point in the state space. These are subject to a continuous time change; their course is described by the status curve or system trajectory. The trajectory is unambiguously determined when the initial state vector $x(0)$ at time point $t = 0$ s, as well as the external action vector (input vector) $u(t)$, are specified for all time points $t \geq 0$ s. Time t acts as a trajectory parameter (Manz, 1999).

Equation 1: $\dot{x}(t) = f(x(t), u(t))$,

Equation 2: $y(t) = g(x(t), u(t))$.

The differential equation $\dot{x} = f(x, u)$ determines, in addition to the state vector x, the vector of the corresponding state change. This vector can be displayed in the phase plane as a starting arrow. The length of the arrow is a measure of the rate of change of state. The arrow is oriented to represent the tangent to the trajectory which results from the relationship (Manz, 1999):

$$\frac{\dot{x}_2}{\dot{x}_1} = \frac{\frac{dx_2}{dt}}{\frac{dx_1}{dt}} = \frac{\partial x_2}{\partial x_1}.$$

The time derivative ratio corresponds to the slope of the curve. If the change arrows are plotted on the raster at the state level, then the first optical impression of the dynamic properties of the system under investigation is created. We call this type of field a vector field in which the arrows are directional vectors of the system (Manz, 1999).

2.7 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. Figure 13 shows the concept of on-line analysis. As shown in the figure, the concept of on-line analysis can be divided into two partial steps "Error detection (recognition) – 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 detect the potential harm caused by undesirable proceedings.

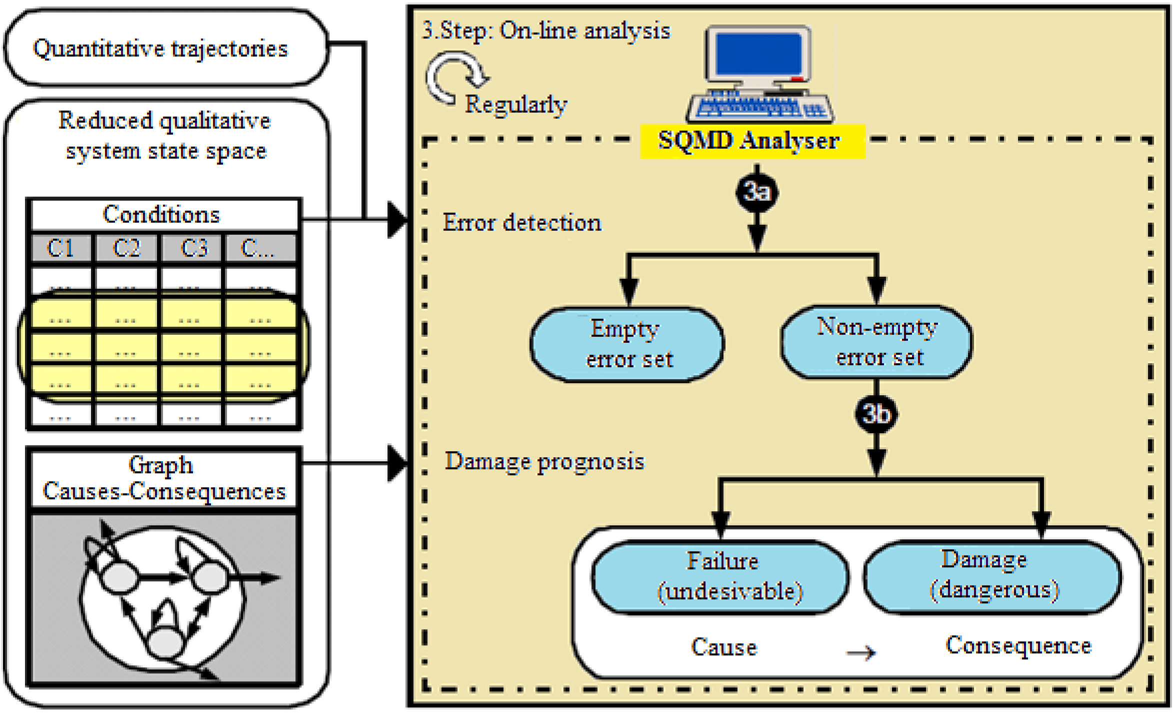

Figure 13: Concept of on-line analysis (Manz, 1999).

(3a) Error detection

The analyser shown in figure 13 evaluates the determined quantitative trajectories in a second step and derives a quantitative comparison. At the same time, the reduced quality state space is searched and the resulting set of errors (error set) is generated from this comparison. This error set contains all states that are labelled as unwanted (N) or dangerous (B). If this error contains no states, then the technical process is in the desired state (fault-free state, in the state specified by the operating instructions). If the set of errors is not empty, either a warning message follows or the next partial step, "damage prognosis", proceeds.

(3b) Damage prognosis

If there is at least one dangerous state in the error set, it is necessary to evaluate more precisely the causes and effects of the error in the technical process. The purpose of this assessment is to ensure the shutdown of the overall system in the case of damage. The analysis is performed on a cause-effect graph. This allows forward tracking of possible errors and their effects on the overall system.

Consequently, error set creation and error analysis are described in more detail.

2.8 Verification of the proposed model for safety-critical processes

The simulation will verify the obtaining of the solution. 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 the long-term and the short-term and also evaluate the effect of the proposed solutions concerning future possibilities. The purpose of the verification is to evaluate the correctness of the proposed models used for on-line monitoring operation of safety-critical processes in dynamical technology systems. Model verification can be performed using simulation tools such as MATLAB. In simulations, the noise affecting outcomes in real operation of individual systems cannot be overseen. It should be included, incorporated into the simulation model. If weaknesses in the proposed models are revealed during the verification, the safety analysis process returns to the step “modelling safety-critical process of dynamical systems”.

2.9 The proposal and development of the control system

The result of this step will be the conceptual design of the structures system for safety analysis (control of the process) of the dynamic process. It is important to evaluate all possible solutions, opportunities and strategies in terms of fulfilment expectations and in 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 the system and we get a real design of hardware and software of control system.

The system proposal is realised on the basis of requirements from the customer and also the results of the safety analysis. not only the proposal of software system, but also the proposal of the necessary hardware, that will ensure the correct functionality of the proposal of the proposed system belongs here.

2.10 The results of verification and validation

The next important step of our proposal is the control processes of the submitted control system for a specific safety-critical dynamic technological system. We verify the correctness of the product according to the real requirements of the user. We propose verification and validation in cooperation with future users of the control system. It is important to verify the correctness of all functions and tools to achieve the functionality of the control system. The primary aim is to ensure that the submitted control product meets the needs of the customer. We know from experience that errors also arise during system development, but they must be eliminated as with as little cost as possible. This step also includes testing the system to verify the correct functionality and quality of the product. If verification and validation reveal unwanted errors, we need to go back one step to the proposal and development of the control system and eliminate the errors.

2.10.1 Software system testing

In the testing process, software engineers focus on the entire life cycle of testing, which begins with functional testing and ends with acceptance testing and includes (Tanuška, Schreiber):

- **Functional and module tests** – performed mostly by software engineers directly at the implementation stage.
- **Integration tests** – the actual testing of multiple modules simultaneously.
- **Regression tests** – it is tested whether a side effect has occurred by adding a new module or function (bug introduction).
- **Independent tests** – performed by independent external subjects.
- **Alpha and beta tests** – which is testing the system in the real environment. For alpha testing, the system is tested without live data. It is tested by the customer at the developer. Beta testing uses real-time tracking data with immediate correction.
- **System tests** – it is a series of different tests that check the entire system (hardware, software environment, database, people…). Recovery testing, Security testing, Performance testing and Stress testing can also be included here. Similarly, we can include so-called Sensitivity testing, which attempts to discover combinations of data (within applicable limits) that can cause system instability.
- **Installation tests** – cover the general performance of a system that is first installed on particular hardware and operating system.
- **Validation tests** – verifies that the software meets the "reasonable expectations" of the customer as defined in the specified requirements. Validation testing is performed by black-box methods.
- **Acceptance tests** – it is actually the last milestone in the project testing. If it is successful, the project is officially accepted by the customer.

Errors can be introduced into the application at every stage of its development life cycle, including testing.

If a product is to be user-friendly, there are five fundamental aspects of testing (Tanuška, Schreiber):

Utility (functionality or utility)**:** Typically, the complexity of product control is tested, the performance of the most important functions of the product, whether the product is financially efficient, etc. Irrespective of the product correctness, these are the most important aspects that should be tested.

Reliability: Is critical to know the frequency of failures of the product and the impact of the failure. When a product fails, it is important to estimate how long it takes to remove the failure and more importantly, how long it takes to resolve the consequences of the error.

Robustness: A set of factors such as the range of control conditions, the possibility of unacceptable results from the accurate input data, etc. In the case of functional testing, the output data must correspond to the input conditions. For robustness testing, output data that do not correspond to the input conditions are intentionally given to input and tested for the response of the product.

Performance: Products performing real-time are characterized by time constraints, such as action-specific response, sampling time, etc. When testing performance, it is critical to test exactly those system parameters that are vital to its operation. For instance, data collection from the reactor is performed every tenth of a second. If the system could not process and evaluate these data within the required time interval, it would behave like a system without sufficient performance.

Correctness: The product is correct if it meets the specified technical conditions and is independent of the used sources.

2.11 The final control system

The final step of our proposal is the final control system ready for implementation into operation. During the implementation of the system, adjustments are made according to customer requirements. The setting is always verified with real data and after validation put into live operation. At the same time, it is possible to make various adjustments, deliver output reports, exports, or process connections to superior systems.

Next, we should focus on creating a test environment. All key participants should have access to the test environment. In particular, the complexity of functionalities should be checked. Also, access rights should be configured for individual workers who can come into contact with the control system. Deficiencies should be reported to the development and configuration team for further completion.

2.11.1 User manual

It aims to introduce individual functions and features to the end-users of the control system. In the introduction, we should briefly describe the system to the users, its primary purpose, the basic functions and features.

The description of operations with this system should follow. We will introduce the users to the basic interface or the main desktop, in which all essential tasks will be performed. A detailed description of this interface is required, in particular, its parts and their location. An important section of this guide is the introduction of the system functions themselves. As we know, users may have different access rights to work with the system, so the user guide should be created differently for each type of user.

Conclusion

The monograph aimed to propose a safety analysis in the risks in the process of the development of the control systems for the complex dynamic technological 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.

One step from our proposal is the proposal of sequence steps of the preliminary risk analysis in the development process of the safety-critical control system. The model consists of two methods. Initially, the preliminary identification of all risks is made the preliminary identification of all risks. Consequently, these hazards will be analysed by the sequence of six steps. Safety analysis is a difficult and lengthy process. The result of the preliminary analysis will give us important information, which we will need in the next phase for the development of a safety-critical control system. We will continue with these results in the overall safety analysis of these systems.

In monograph, we also presented the principle of hybrid models method for monitoring dynamic systems is introduced. The method concept is divided into three steps: “model building”, “on-line state-space reduction” and “on-line analysis”. In the first step, hybrid model components are designed and constructed. Dynamic properties (dependencies) are integrated into qualitative models based on dynamic equations. This integration is performed in the second step. Within the on-line state space reduction, qualitative model components are reduced based on dynamic models and data obtained from sensors and actuators. Consequently, a system is assembled. The reduced qualitative state space of the system is valid for a given time interval and can be analysed in the third step according to deviations from the desired system behaviour.

Although the preparation and implementation of safety analysis is a very demanding process, we believe that the investment is very necessary, important and worth it, since we live in a period of widespread automation and daily possibility of disasters directly related to the operation of controlling systems.

References

1. P. Bigoš, E. Faltínová: Spoľahlivosť technických systémov. Technická univerzita v Košiciach, 2011, pp. 171.
2. G. Brack: Dynamik technischer Systeme, VEB Deutscher Verlag für Grundstoffindustrie, Leipzip, 1974.
3. K. Buganová, M. Lusková: Analýza rizík v podniku metódou FMEA (Failure Mode and Effect Analysis). Žilinská univerzita v Žiline, Január 2011.
4. K. D. Forbus: Qualitative Process Theory, Cambridge, MA, MIT AI Lab., 1984.
5. P. M. Frank: Diagnoseverfahren in der Automatisierungstechnik, at Automatisierungstechnik, Band 4, Feb. 1994, pp. 47–64.
6. P. M. Frank: Komplexe Systeme – Nichtlineare Rückkopplungssysteme jenseits der Stabilität, at Automatisierungstechnik, Band 46, Nr. 4, April 1998, pp. 167–179.
7. P. Fröhlich: Überwachung verfahrenstechnischer Prozesse unter Verwendung eines qualitativen Modellierungsverfahrens, Institut für Automatisierungs- und Softwaretechnik (IAS), Universität Stuttgart, Dissertation, Universität Stuttgart, 1996.
8. M. Havlíková: Lidský faktor v systémech MMS. Január 2009.
9. M. Hurme, M. Dohnal, M. Järveläinen: Qualitative reasoning in chemical and safety engineering, European Symposium on Computer Aided Process Engineering, 2, 1992.
10. R. Isermann: Überwachung und Fehlerdiagnose, Moderne Methoden und ihre Anwendungen bei technischen Systemen, Düsseldorf, VDI-Verlag GmbH, 1994.
11. R. Lauber: Regelungstechnik 2 – Manuskript zur Vorlesung, Universität Stuttgart, Institut für Automatisierungs- und Softwaretechnik. Vorlesungsmanuskript, 1995.
12. R. Lauber, P. Göhner: Prozessautomatisierung 1, Band 1, 3. Auflage, Berlin Heidelberg, Springer-Verlag, 1999.
13. R. Lauber, P. Göhner: Prozessautomatisierung 2, Band 2, 1. Auflage, Berlin Heidelberg, Springer-Verlag, 1999.
14. J. Lunze: Künstliche Intelligenz für Ingenieure. Band 2: Technische Anwendungen, Band 2, München, Oldenburg Verlag GmbH, 1995.
15. S. Manz: On-line monitoring and diagnosis based on hybrid component models, Institute of Industrial Automation and Software Engineering University of Stuttgart, Germany, 1999.
16. S. Manz: Einsatzhybrider Komponenten Modelle zur online – Prozessverfolgung dynamischer Systeme, 7. Berichtskolloquium GKPVS, Universität Stuttgart, 2000.
17. S. Manz: Development of hybrid component models for online monitoring of complex dynamic systems. In Modelling, Analysis and Design of Hybrid Systems. S. Engell, G. Frehse, E. Schnieder (Hg.), Berlin Heidelberg, Springer-Verlag, 2002.
18. S. Manz: Entwicklung hybrider Komponentenmodelle zur Prozessüberwachung komplexer dynamischer Systeme, Institut für Automatisierungs- und Softwaretechnik, Universität Stuttgart, Band 1/2004.

19. D. Mudrončík, M. Gálik: Normy pre tvorbu softvéru riadiacich systémov. MTF STU v Trnave, Apríl 2009.

20. G. M. Nenninger, B. Nixdorf, V. K. Krebs, J. Lunze: Erreichbarkeitsanalyse hybrider Systeme, at Automatisierungstechnik, Band 49, Nr. 2, Feb. 2001, pp. 75–85.

21. H. Pačaiová: Risk assessment – comparison of definitions, methods and procedures, Motivation for the panel discussion forum BOZP, Krpáčovo 2. – 4. apríla 2003, Institute of safety, quality and environmental, department of safety and production, the technical university of Košice.

22. K. Panreck: Systembeschreibungen zur Modellierung komplexer Systeme, at Automatisierungstechnik, Band 47, Nr. 4, April 1999, p. 157.

23. M. Rausand: Preliminary hazard analysis, October 7, 2005 System reliability theory (2nd ed.), Wiley, 2004, 1/36, Department of production and quality engineering, Norwegian university of science and technology.

24. F. Schmidt: Simulation komplexer technischer Anlagen – Manuskript zur Vorlesung, Universität Stuttgart, Institut für Kernenergetik und Energie Systeme, Abteilung Wissensverarbeitung und Numerik. Vorlesungsmanuskript, 2000.

25. M. A. Schwarz: Introduction to software engineering for safe and reliable software, Institute of informatics, working group software engineering Warburger street 100, 33098 Paderborn, 2004.

26. Simulation von Logistik-, Materialfluss- und Produktionssystemen, VDI Richtlinie 3633 – Begriffsdefinitionen. VDI Richtlinien, November 1996.

27. Ing. Ondrej Strnád, CSc. „Riadenie rizík informačnej bezpečnosti,“ vydavateľstvo Amos, 15. 10. 2010.

28. P. Struss: “Modellierung, qualitative”, “Schließen, qualitatives” und “System, modellbasiertes”. Drei Artikel im Wörterbuch der Kognitionswissenschaft. In: Wörterbuch der Kognitionswissenschaft, Strube, Gerd, Stuttgart, Klett-Cotta, 1996.

29. M. Štrbo, P. Tanuška, A. Gese, L. Smolárik: The methodology proposal for the model-oriented safety analysis of dynamical systems, Faculty of Materials Science and Technology, Slovak University of Technology in Bratislava, 2014.

30. prof. Ing. Pavol Tanuška, PhD., doc. Ing. Peter Schreiber, CSc.: Proces testovania softvérových produktov. STU v Bratislave, MTF v Trnave, Katedra aplikovanej informatiky a automatizácie.

31. L. A. Zadeh: The concept of a linguistic variable and its application to approximate reasoning parts 1 and 2, Informatics Science, Band 8, 1975, pp. 199–249, 301–357.

Other relevant sources (not identified in the text)

32. STN EN 1050 – Safety of machines, principles of risk assessment, august 1998.

33. M. Štrbo: The Process of preliminary hazard analysis for safety-critical systems, Faculty of Materials Science and Technology, Slovak University of Technology in Bratislava.

34. M. Štrbo, P. Tanuška, A. Gese, L. Smolárik: The methodology proposal for the model-oriented safety analysis of dynamical systems, Faculty of Materials Science and Technology, Slovak University of Technology in Bratislava, 2014.

35. M. Štrbo, P. Tanuška, A. Gese, I. Hagara, L. Smolárik: Safety Analysis for Complex Dynamic Systems, Faculty of Materials Science and Technology, Slovak University of Technology in Bratislava, 2014.

Ing. Milan Štrbo, PhD. (born 1986) completed his Master’s level at the Faculty of Materials Science and Technology in Trnava in the study field Automation, Applied Informatics in 2011. Subsequently, he continued his doctoral studies at the same faculty, where he completed his studies and received a PhD. in 2014. After graduation, he started to work as a university lecturer at the Pedagogical Faculty of Trnava University, where he has been working at the Department of Mathematics and Computer Science up to this day.