Journal of ELECTRICAL ENGINEERING, VOL. 53, NO. 5-6, 2002, 167–176

REVIEWS - LETTERS - REPORTS

SAFETY PROBLEMS AND FAULT DETECTION IN PROCESS INDUSTRY

Drago Valh [*] — **Boris Tovornik** [*] — **Zoran Vukič** [**] [*]

The present article integrates the demands for safe processing and fault detection techniques. The first part deals with safety of (chemical) process industry in general. Three main hazardous events with their causes and consequences are shortly described. The section points out the idea that safety analysis should predict parts of the process where early fault detection is indespensible. This is important to have the proper sensors installed. Early fault detection can improve the quality of production and increase the occupational and environmental safety through detecting the faults before they develop to a failure that might cause an accident with all its consequences such as material detriment, environmental damage or lose of human life. The second part briefly describes some analytical model-based fault detection techniques.

Keywords: process safety, fault detection, fault isolation, parameter estimation, state observers

1 INTRODUCTION

An expansion of new scientific discoveries, technical solutions, automation of technological processes and robotics makes the human population dependent on some machines that can be our friends or/and mortal enemies if not designed, handled and maintained properly. This is also the case where desired global competitiveness cannot be achieved. The global competitiveness depends to a large extent on the effectiveness of the use of factory automation. The early 1980s heralded the creation of the "Factory of the future". The prevalent image then was a "lights off" factory heavily populated by robots, with a few human supervisors keeping track of operations by watching monitors in a central control room. In many cases, this image was not fulfilled. In few words, workers (and wider environment, living and non-living) are still exposed to harmful effects of the working area and accidents, caused either by process malfunction or incompetence of their colleague workers.

Some studies [1] have shown that main causes of the accidents related to automation or control were poor instrumentation (19 %) and operator error (19 %). Most of the human errors are usually made during start-up operation of the process. The following conclusion can be taken out from the previous discussion: If the degree of automation were higher, the consequences of a human error might be smaller. In addition the co-operation between automation and human operator, it is important to avoid human errors during operation. The occurrence of equipment faults as causes of accidents brings up the requirement that potential failures both in measurement and control equipment, and in process equipment, should be studied. The process design should be prepared for them, thus an equipment failure of the system should not lead to the accident. One of the possible solutions is early detection of malfunctions, called Fault Detection and Isolation (FDI).

2 SOME PROCESS INDUSTRY SAFETY FEATURES

Three types of event are traditionally associated with the chemical branch of the process industry. These are releases and spills, fires, and explosions. They can cause damage through two distinct processes, as shown in Fig. 1.

A certain conflict can arise between process need and safety. Chemical processes, for instance, need reactive substances but, on the other hand, the reactivity of the substances is a key aspect of the danger they pose. As a chemical process needs substances showing hazardous properties, they must be reliably contained in the process equipment and uncontrolled reactions must not take place. The danger is greater, the larger the quantities of substances and energy released. There are two essential goals of the process safety efforts:

1. To minimise the quantities of substances.
2. To control the potential risk that remains objective.

The last require the following:

- process equipment must withstand the anticipated stresses caused by hazardous substances;
- process parameters must not take on values such that the substances can undergo uncontrolled reactions.

A point of special interest is where the regions begin in which uncontrolled reactions cannot occur. Critical parameters are called safety ratings. At the planning and

[*] Faculty of Electrical Engineering and Computer Science, Smetanova 17, 2000 Maribor, Slovenia, E-mail: boris.tovornik@uni-mb.si
[**] Faculty of Electrical Engineering and Computer Science, Unska 4, 10000 Zagreb, Croatia

ISSN 1335-3632 © 2002 FEI STU

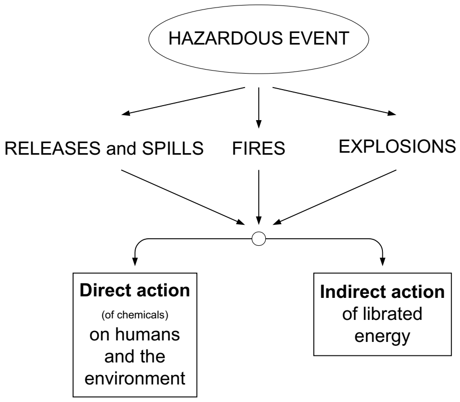
HAZARDOUS EVENT
RELEASES and SPILLS
FIRES
EXPLOSIONS
Direct action (of chemicals) on humans and the environment
Indirect action of librated energy

Fig. 1. Three hazardous events interact with humans and environment directly and/or indirectly.

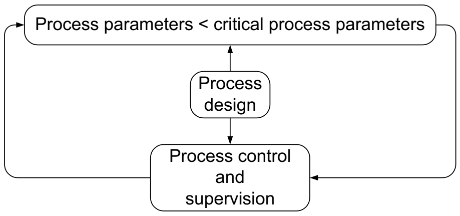
Process parameters < critical process parameters
Process design
Process control and supervision

Fig. 2. Process design must ensure that process parameters do not exceed their critical values. It also dictates control and supervision of the process (plant). Control and supervision work on-line.

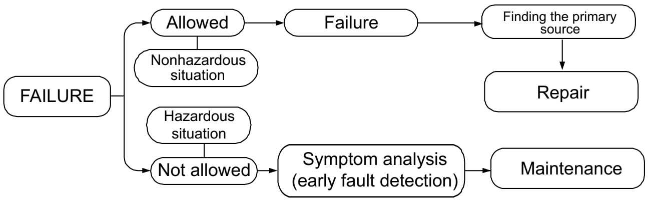

Fig. 3. If a failure is not allowed, FDI should to be applied with the supervision system. However, if the process can sustain a failure, a primary source has to be located.

design stage, plant and process safety requires taking steps so that critical concentrations, temperatures and pressures are not reached. This is achieved by appropriate process design and control engineering (Fig. 2).

Critical process parameters and hazardous potential ignition sources must not occur in the plant as a result of process upsets or even human error. These become an additional concern of plant safety requiring a painstaking cause and effect analysis of all possible errors and malfunctions and the institutions of measures to prevent or neutralise situations that could lead to an unsafe condition. Such measures could be technical or organisational.

The complete absence of all possible hazards (absolute safety) is not possible for two reasons:

- it cannot be ruled out that several safety measures will fail simultaneously;
- people make mistakes, misjudge things, assess them wrongly, fail to notice them.

To go even further, failures usually do not appear without any reason. They must have been caused by groups of events from the past (change of parameters due to ageing, disallowed change of one of unmeasured variables, *etc.*). The causes from the past (recent or distant) would initiate the symptoms of a failure before it happens. If they are known or pre-studied and if one is able to detect them, a process or its component can be maintained on time to prevent from failure. If a failure is allowed, its primary source has to be found (Fig. 3). Figure 3 can easily be explained by the following example: *If a failure causes hazardous situation, it has to be detected in its early stage to prevent it from happening (eg, Control valve is a component. If measurements of signals of its drive are carried out on-line, reduced surface of the brushes can be detected, replaced on time thus preventing the failure from happening* [2]*). If necessary measurements for early fault detection are not available or early fault detection is not demanded, the primary source of the failure can be found on line after the fault has occurred with all its (non-hazardous (!)) consequences, by alarm analysis, for example.*

This is one of the recent tasks of process automation. Modern equipment should provide enough measurement signals to be able to apply early fault detection (if necessary) also for safety reasons.

3 DEFINITIONS FOR "SAFETY" AND RELATED CONCEPTS

Safety describes a non-existence of risk posed by a system or to the system. The basic elements of safety are the causes and consequences of events (accidents). The consequences are defined to be the effects on human life, property or the environment. In general, safety is a measurable concept. It is possible to say whether the system is in a safe state or an unsafe state. However, another consideration is whether, or not, it is possible to define if a system will be safe enough through its whole life cycle. In some of the definitions safe means zero-risk under defined conditions. Unfortunately, that would mean that the plant is not operating. Thus a more realistic safety policy is risk minimisation. This includes the aspect of concentrating on weak points of the system in order to make them safer.

Danger is the diametric opposite of safety, where the risk of a process is greater than the acceptable limiting risk (DIN/VDE 31 100).

Discussing causes of accidents, the concepts of *failure, fault, error and mistake* are often mentioned.

System failure is the inability of a system to fulfil its operational requirements.

Systematic failures cause the system to fail under some particular combinations of inputs or under some particular environmental condition. Systematic failures could arise at any part of the safety life cycle.

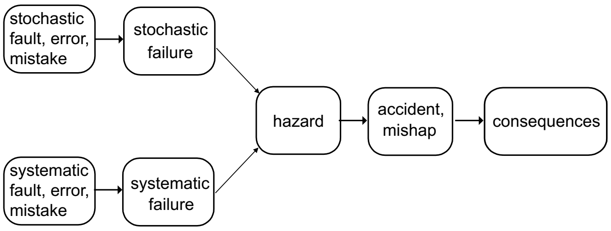

Fig. 4. The accident is caused by unintended events in human activity, in the technical equipment or in the environment.

Other types of failures are those whose occurrence follows a stochastic model (failures due to ageing of mechanical components, and random failures of electronic components).

Fault and error are causes for failure.

A *mistake* is a human error or fault.

Hazard describes the potential of accidents. It comes up frequently in accident research.

The concept of an *accident* lies between causes and consequences. The limit where the accident event begins and where it ends is not exact. The greater the hazard potential, the better safety measures are needed to lower the probability of occurrence of the undesired event to the level that the level of risk is at or below the acceptable risk level.

Finally, causes of accidents can be divided into systematic failures and stochastic failures in systems. A software failure, failures caused by errors and mistakes in specification, design, construction, operation or maintenance are always systematic failures. The occurrence of failure does not cause the accident directly. A specific state of the process, or a combination of failures, are needed for a hazard to occur and to develop to be an accident [1], see Fig. 4.

A viewpoint is that all the accidents are caused by a human being, either by the design organisation which has not designed the system to be safe enough, or by the occupational organisation which has not been able to handle the disturbance situations.

4 THE SAFE PLANT OBJECTIVES AND CONCERNS

The goal of the plant safety is to eliminate or minimise the possible hazards. In practice, safety design consists of identifying possible process disturbances and potential accidents, whereafter preventive measures are designed for them. The safety tasks can be broken down to the process itself and into the safe design and operations of the technical facility required for the process. Safe plant design and operation are achieved by:

1. Achieve safe process design by:

- identifying all types of hazards;
  For all substances to be processed, safety ratings and toxicologically and ecologically relevant data must be acquired. A comparison of process parameters and design data with safety ratings, step by step through the process, reveals where danger sources exist, or may arise.
- assessing the hazard potentials;
- minimising the hazard potentials;
  Determine whether the hazard potentials can be reduced through suitable process design.
- deactivating the hazard potentials.
  Any hazard potentials that remain must be deactivated in such a way that they cannot manifest themselves in the process.

2. Achieve safe plant design and operation by:

- systematically analysing danger sources;
  The plant must be systematically searched for danger sources (possible defects and failures that can activate the deactivated hazard potential).
- qualitatively evaluating the probabilities of occurrence of the danger sources; When possible faults are identified, their frequencies or probabilities of occurrence must be evaluated so that appropriate safety measures can be taken.
- minimising sources of trouble and error;
  All possibilities for minimising sources of trouble and error must be exhausted. Early fault detection can alarm maintenance measures thus preventing from failure and/or hazardous situation.
- employing fault-tolerant design.
  As far as possible, the facility must be designed and equipped so that faults do not result in harm.

This can be accomplished by applying redundant (multiple) safety devices.

Safe processing can be achieved through fire protection, explosion prevention and protection, release and spill protection, and process control. In general, strategies of safe processing could be divided into passive (fire protection, explosion prevention and protection, release and spill protection) and active (safe operation of the plant by application of process control and supervision strategies). This terminology was chosen as control systems can constantly influence the system behaviour. All the methods that do not fall into process control engineering are called passive.

The article will focus merely on safe processing based on process control engineering for achieving safety objectives in process control plants. Technical or organisational measures, or a combination can be employed. Safety concepts for specific safety objectives set down in technical regulations must take first priority. Safety objective refers to preventing injuries to persons, major environmental damage, and major equipment damage to property. Safety precautions for electrical installations and equipment, occupational safety practices, or measures taken to safeguard machinery are excluded. Safety requirements and the measures required are more stringent the greater the risk that must be covered. The risk must be reduced at least to the acceptable limit by measures that do not base on process control engineering.

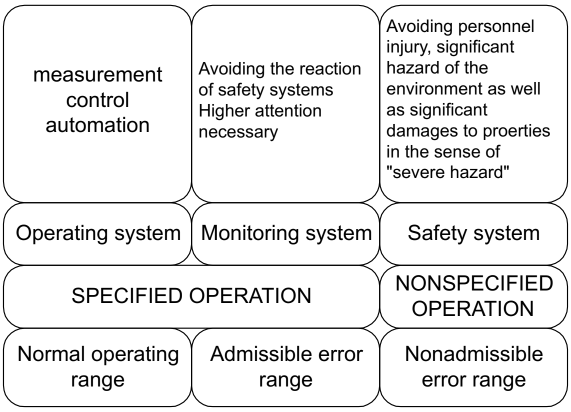
measurement control automation
Avoiding the reaction of safety systems Higher attention necessary
Avoiding personnel injury, significant hazard of the environment as well as significant damages to proerties in the sense of "severe hazard"
Operating system
Monitoring system
Safety system
SPECIFIED OPERATION
NONSPECIFIED OPERATION
Normal operating range
Admissible error range
Nonadmissible error range

Fig. 5. Functions of process control engineering equipment

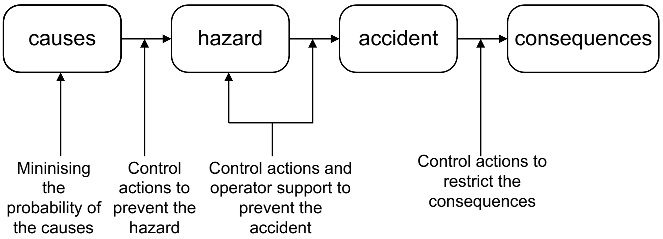
causes
hazard
accident
consequences
Mininising the probability of the causes
Control actions to prevent the hazard
Control actions and operator support to prevent the accident
Control actions to restrict the consequences

Fig. 6. The automation engineer can effect the probability and severity of accidents in many ways

Table 1. Classification of consequences from occurrences of faults.

Hazard Classes	Consequence Description
0	No consequence
1	Decreased performance (productivity degradation, quality degradation)
2	Damage on machinery and surroundings, contamination of environment
3	Injury to people

Active safety measures commonly reduce only a portion of the risk resulting from a unit. The reminder is usually dealt by passive safety measures. The safety requirements for process control engineering is diverse.

Figure 5 illustrates the functions of systems, treated by process control engineering equipment.

The effect of automation on process safety is not clear. On the other hand, automation is blamed for posing risk and for increasing the chance of human error in situations involving disturbances; however, automation enables sophisticated process control and handling of disturbance situations without human interference. The methods of safety analysis can be applied during the designing stages of safe process automation.

However, automation itself is rather safe. No great amount of energy is bound to it. The hazards arise in the process controlled by automation. The safety of a process plant is based on the process design, which define the number of possible unsafe states and their probability. But, responsibility for many safety features is allocated to the automation design. In a hazardous situation, the target of the control system is to prevent an accident from happening by keeping the process in a safe state or by bringing the process back to a safe state before any serious consequences have occurred. If it is not possible to maintain a safe state, the control should minimise the consequences. Another important safety-related target of the automation design is to prevent hazardous situations from being caused by automation itself.

When designing the process automation, designer has the following options for reducing the risk related to the specific accident [1] (Fig. 6).

The physical consequence of a fault event can often have a major economical, or social impact. Main classification is done with respect to criticality (Tab. 1) [3]. This classification into hazard classes indicates the importance of the consequence and can be used to determine the requirements to tolerance to faults before a set of remedy actions are specified.

Safety analysis of process automation should be a part of overall safety analysis of a plant. Proper automation equipment should be predicted in the designing phase. Overall hazard analysis should point out parts of the plant (plant elements, automation equipment), where and what kind of fault detection should be installed. This is of big importance to install required sensors which sometimes do not play an important role in production itself, but are required for safety reasons. It should be discussed whether early fault detection is needed. In addition the safety and availability performance of process automation affects the flexibility and profitability of production. Accidents and injuries not only cause economic losses, they may cause human suffering and environmental damage. To judge whether the design is safe enough or should be improved, the designer must have a concept of what kind of safety and availability performance is required.

Automation designers do not get data on the safety requirements for automation from the process engineers in a form which allows direct verification. The automation engineer has to analyse the hazards associated with the process, safety analysis methods can be used here. The hazard and operability study is one of the most common methods applied to analyse the safety of process engineering. Other methods adaptable to automation engineering, and which could be used in co- operation with process engineers, are action error analysis, fault tree analysis and event tree analysis. The reliability and safety features of the automation or control system can be further studied by means of failure mode and effect analysis. Quantitative reliability assessment can be combined with other methods to get comparative values for the hazards.

An important feature in automation safety is information on process states given to the operator. The safety analysis methods do not consider this aspect explicitly. However, safety analysis provide information on the process disturbances which might lead to unsafe states, and, thus the analysis can be used as a standpoint when designing the operator interface. To avoid operator error in fault accommodation process, the tendency to automated fault detection, identification and accommodation is an important subject for automation engineers nowadays.

5 FAULT AND FAILURE DETECTION IN DYNAMIC SYSTEMS

Modern technology has advanced to the point where it has become possible and highly desirable to increase the reliability, availability and safety of technical processes. This is especially true for automatically controlled processes. Therefore health and operation of elements of controlled systems must also be observed by automated monitoring. This procedure begins with monitoring the status of each element of the process, actuators, sensors, control equipment-including their behaviour in open and closed loop operation. Initial fault monitoring is followed by appropriate actions and management to cope with faults, failures and disturbances to meet reliability and safety requirements. The monitoring procedure as a whole ends with the management of maintenance and repair. Human factors are also important, *eg* for an appropriate division of functions and a suitable interface between man and machine.

However, fault diagnosis has become an issue of primary importance in modern process automation and as it provides the pre-requisites for fault tolerance, reliability or security, which constitute fundamental design features in any complex engineering system. The main difference is between:

- fault detection and insulation (FDI) methods based on mathematical or dynamic model of process system;
- knowledge based methods, which are in many cases more failure oriented (searching the primary component indicating a failure).

In general, fault monitoring systems must be tolerant to signal deviations caused by process parameter uncertainty, disturbances, non-linearities, *etc.* which are normal functions of the operation of most engineering requirements. The robustness and application considerations are also important considerations in applications to three major types of subsystems of an automated plant:

- actuators;
- main structure (process);
- instrumentation (sensors).

The use of *analytical redundancy* is the main idea in the issue of FDI. Three or more dissimilar sensors measuring different variables and therefore producing entirely different signals, can be used in a comparison scheme. Even though the sensors are dissimilar, they are all driven by the same dynamic state of the system and are therefore functionally related. The functionally redundant FDI schemes are basically signal processing techniques employing state estimation, parameter estimation, adaptive filtering, variable threshold logic, statistical decision theory, and various combinatorial and logical operations, all of which can be performed in electrical circuits or digital computers.

On-line parameter identification, for example, provides a powerful way of detecting faults in dynamic systems by estimating physical parameters wherever they can be defined. The method can be used for component and sensor fault detection.

An example of an instrument fault detection scheme is the following: assume that there are m sensors, that one of them is known to be reliable, and that a state estimator driven by the reliable sensor signal and the inputs of the monitored plant can be constructed. In that case it is possible to generate estimated values of the entire set of m sensor signals. These can then be compared with the corresponding actual sensor signals, and any differences will only be due to small discrepancies as the errors in the state estimators noise in the sensors. Simple threshold logic can then be applied to the difference signals. The thresholds are usually unlike zero to prevent false alarms.

There are certain criteria for assessing the performance of an FDI scheme:

a) promptness of detection;

b) sensitivity to incipient faults;

c) false alarm rate;

d) missed fault detection;

e) incorrect fault identification.

Each of the criteria depends on the demands of the process. Some additional remarks are needed for FDI in feedback control systems.

5.1 Fault Detection, Isolation and Accommodation in Feedback Control Systems [3]

Consequences, of even simple faults, may be dramatic and there are considerable incentives to enhance computerised feedback loops with methods for fault detection and accommodation. A large step can be taken with mathematical methods from control engineering, but in order to arrive at efficient solutions for use in large volume, progress in the area of hybrid systems is mandatory.

Most automated industrial systems are hybrid by nature. They consist of continuous time process controlled by real time computers. Sensors on the plant provide measurements of process variables, and actuators convert control signals to physical inputs to the process as visualised in Fig. 7.

Feedback is established because actuator demands are calculated from the difference between a reference value and sensor measurements. Any deviation between these signals will cause an immediate reaction on the actuators when actuator demands are updated. The discrete time control algorithm makes use of both current and previous events in the plant. This makes it possible to employ, for

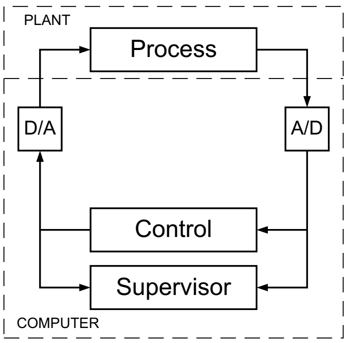

Fig. 7. Supervision of the process under control

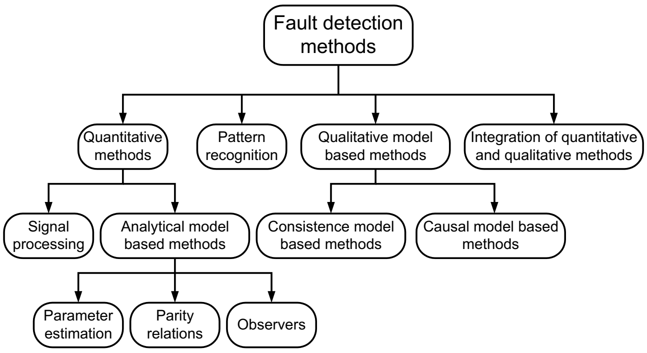
Fault detection methods
Quantitative methods
Pattern recognition
Qualitative model based methods
Integration of quantitative and qualitative methods
Signal processing
Analytical model based methods
Consistence model based methods
Causal model based methods
Parameter estimation
Parity relations
Observers

Fig. 8. Simple classification of the fault detection algorithms

example, prediction methods to give the control loop desired characteristics. Response time to changes in the setpoint, disturbance rejection properties, noise sensitivity, and stability properties are key attributes that are always quantified in the requirements to a particular closed loop design.

Feedback control systems are particular sensitive to faults. Faults in feedback loops are in general difficult to handle. They can be categorised in generic types:

- reference value (setpoint) fault;
- actuator element fault;
- feedback element fault;
- execution fault including timing fault;
- application software, system or hardware fault in computer based controller;
- fault in physical plant.

If a fault develops gradually, the closed loop will attempt to compensate for it and in this way hide the development of the malfunction. The fault may not be discovered until the control loop stops normal operation. If faults arise suddenly, the effect is amplified by the closed loop control. Production stops, process damage, or other undesired consequences may be the result. A feedback sensor fault, for example, may cause a large deviation between measurement and reference. This will in most cases cause large actuator demands and eventually lead to rapid change of process state. Unacceptable excursions in process state followed by production stop, plant failure or direct damage are experiences from actual events in industry.

In normal operation, feedback control should keep the process state equal to a desired setpoint while the influence from process disturbances and measurement noise are kept minimal. This can be achieved by employing methods that estimate process states and perform optimal dynamic filtering in combination with techniques that adopt parameters in the control method to current process conditions.

In abnormal operation, when faults have occurred, the control loop should react immediately in a way that prevents a fault from developing into malfunction of the system being controlled. This requires added functionality to well established methods in control theory.

A general method for the design of fault handling associated with closed loop control includes the following steps:

1. Make a failure modes and effect analysis related to control system components.
2. Define desired reactions to faults for each case identified by the analysis from (1).
3. Select an appropriate method for generation of residuals. This implies consideration of system architecture, available signals, and elementary models of components. Disturbance and noise characteristics should be incorporated in the design if available.
4. Select a method for input-output and plant fault detection and isolation. This implies a decision of whether an event is a fault and, if this is the case, the determination of which element is faulty.
5. Consider the control method performance and design appropriate detectors for supervision of control effectiveness. This implies surveillance, *eg*, of closed loop stability which may be affected by changes in plant parameters if controller robustness is insufficient. Design of appropriate reactions.
6. Design a method for accommodation of faults according to points 2 and 5.
7. Implement the completed design. Separate control code from fault handling code by implementation as a supervisor structure.

5.2 Short Overview of Some FDI Methods Based on Analytical Models

The chosen diagnostic procedure depends mostly on fault detection demands and available process models. Figure 8 shows a simple classification of the diagnostic algorithms.

Some of the three basic FDI methods based on analytical models will be presented in the next sections:

- parity space approach;
- observer approach;
- parameter estimation approach.

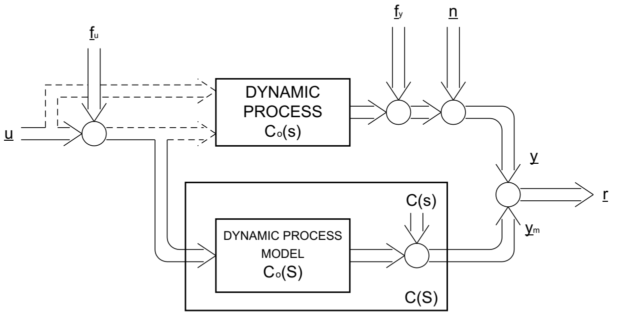

Fig. 9. Principle of the parity space approach to fault detection

Parity Space Approach

The parity space approach means a comparison of the mathematical model of the plant and of the measured variables. Any fault can be detected through differences between the compared signals. Consider a dynamic system with input vector, $\boldsymbol{u}$, output vector, $\boldsymbol{y}$, and a feedback control system. The plant in general consists of actuators, plant dynamics (components), and sensors. For a realistic representation it is important to model all effects that can lead to alarms and false alarms. Such effects are:

- faults in the actuators, or in the components of the plant dynamics, or in the sensors;
- modelling errors between the actual system and its mathematical model;
- system noise and measurement noise.

The analytical redundancy approach requires that the residual generator performs some kind of validation of the nominal relationships of the system, using the actual input and measured output (Fig. 9). The redundancy relationships to be evaluated can simply be interpreted as input-output relations of the dynamics of the system. It is highly desirable to have input and output signals of the actuators of the plant available. This is especially important if the actuators are highly non-linear because then the required system equations do not contain the actuators non-linearities. If a fault occurs, the redundancy relations are no longer satisfied and a residual, $r_i \neq 0$, occurs. The residual is then used to form appropriate decision functions. They are evaluated in the fault decision logic in order to monitor both the time of occurrence and location of the fault. For residual generation, three kinds of models are required:

- nominal;
- actual (observed);
- model of the faulty process.

The output from the parity equations are signals showing inconsistency between normal and faulty operation. In normal process operation the parity equations output is approximately zero. In the case of faults the output will be nonzero. Fault insulation is achieved with structured parity equations. One element of the residual vector is unaffected by a specific fault while all the others will be affected. In that way the determination of fault is possible.

The parity equations are designed as follows:

$$\begin{aligned} \boldsymbol{e}(s) &= \Delta\mathbf{Y}(s) - C(s)\cdot\Delta\mathbf{U}(s) = \mathbf{Y}(s) - C(s)\cdot\mathbf{U}(s) \\ \boldsymbol{r}(s) &= W(s)\cdot\boldsymbol{e}(s)\,. \end{aligned} \tag{1}$$

The residual vector $\boldsymbol{r}(s)$ is found by multiplying the weighting filter $W(s)$ with the error $\boldsymbol{e}(s)$. The filter is designed to make the j^{th} residual unaffected to the i^{th} fault. Unfortunately, the residual is also affected by measurement noise $\boldsymbol{n}$ and modelling uncertainty ΔC, not only by the fault vector $\boldsymbol{f}$ (2).

$$\mathbf{Y}(s) = (C + \Delta C)\cdot\mathbf{U}(s) + \boldsymbol{n}(s) + S\cdot\boldsymbol{f}(s)\,, \tag{2}$$

$$\boldsymbol{e}(s) = \mathbf{Y}(s) - \mathbf{Y}_m(s) = S\cdot\boldsymbol{f}(s) + \boldsymbol{n} + \Delta C\cdot\mathbf{U}\,. \tag{3}$$

In general, the residual vector $\boldsymbol{r}(s)$ is affected by all faults $\boldsymbol{f}(s)$:

$$\boldsymbol{r} = [r_1, r_2, \dots, r_n]^\top = \boldsymbol{r}(f_1, f_2, \dots, f_n)\,. \tag{4}$$

Residual r_i should be made unaffected by fault f_i. This is achieved if matrix $[W\cdot S]$ has the following structure (5):

$$r_i \neq r_i(f_i) \iff W\cdot S =$$
$$\begin{bmatrix} 0 & \sum\limits_{i=1}^{n} w_{1i}s_{i2} & \dots & \sum\limits_{i=1}^{n} w_{1i}s_{in} \\ \sum\limits_{i=1}^{n} w_{2i}s_{i1} & 0 & \dots & \sum\limits_{i=1}^{n} w_{2i}s_{in} \\ \vdots & \vdots & \ddots & \vdots \\ \sum\limits_{i=1}^{n} w_{ni}s_{i1} & \sum\limits_{i=1}^{n} w_{ni}s_{i2} & \dots & 0 \end{bmatrix} \tag{5}$$

or $\sum\limits_{i,j=1}^{n} w_{ji}\cdot s_{ij} = 0$ if $i = j$.

Here, the first residual, r_1, depends on all but the first fault, the second residual, r_2, on all but the second fault and so on; that is:

$$\begin{aligned} r_1 &= r_1(f_2, f_3, \dots, f_n) \\ r_2 &= r_2(f_1, f_3, \dots, f_n) \\ &\vdots \\ r_i &= r_i(f_1, f_2, \dots, f_{i-1}f_{i+1}, \dots, f_n) \\ &\vdots \\ r_n &= r_i(f_1, f_2, \dots, f_{n-1})\,. \end{aligned} \tag{6}$$

The decision function for the logical evaluation of the residuals could then be as follows:

$$\begin{aligned} &\text{if } \big(r_2 \wedge r_3 \wedge \dots \wedge r_n \neq 0\big)\wedge\big(r_1 = 0\big) \implies f_1 \\ &\text{if } \big(r_1 \wedge r_3 \wedge \dots \wedge r_n \neq 0\big)\wedge\big(r_2 = 0\big) \implies f_2 \\ &\dots \end{aligned} \tag{7}$$

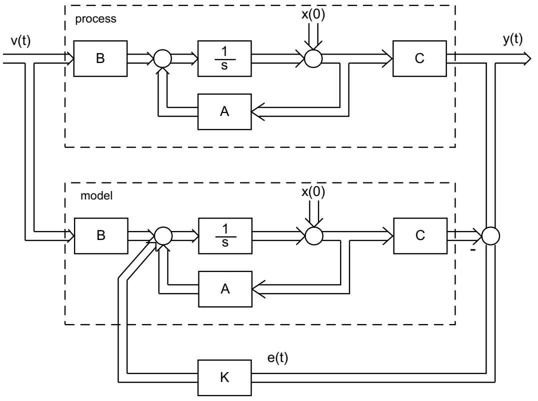

Fig. 10. Residual generation with full-order observer

Robust Fault Diagnosis Using Parity Space Approach in State Space Description and Optimal Time Domain Approximation

A unified approach to the design of robust observer schemes for sensor, actuator and component fault detection and isolation in dynamic systems has been described by several authors [4], [5]. Residual generation can be achieved by providing effective discrimination between different faults in the presence of unknown inputs such as system disturbances, modelling uncertainties, process parameter variations and measurement noise. The approach is based on the theory of unknown input observers providing complete fault decoupling and disturbance invariance under certain conditions independent of the modes of the faults and disturbances. If the underlying conditions are not given, there can be an optimal compromise that minimises the ratio of a norm of the sensitivity with respect to unknown inputs to the norm of the sensitivity with respect to fault in linear systems.

For state estimation one can use linear or non-linear observers, full or reduced-order state observers or Kalman filters, when noise is considered. In either case a mathematical model of a plant is involved. The standard observer configuration for the case of a full order observer is shown in Fig. 10. The simple parallel model usually is not sufficient thus the feedback is required for the following reasons:

- to compensate the effects of different initial conditions;
- to stabilise the observer which is particularly important in the case of unstable system;
- to provide freedom for the design of the observer, for example, to decouple the desired effects of faults, from the effects of unknown inputs, or the effects of different faults from each other.

The key problem of the observer-based fault detection is generation of a set of residuals that permits unique distinction between faults. This goal can, in general, be achieved by a bank of observers or an observer scheme.

The parity-space approach is similar to the design of a dead-beat fault detection observer, robust to unknown inputs. The theoretical background is described by the following steps:

Suppose the system is given by the linear discrete state equations:

$$\boldsymbol{x}(k+1) = \mathbf{A} \cdot \boldsymbol{x}(k) + \mathbf{B} \cdot \boldsymbol{u}(k) \tag{8}$$

$$\boldsymbol{y}(k) = \mathbf{C} \cdot \boldsymbol{x}(k) \tag{9}$$

where $\boldsymbol{x}$ is the $n \times 1$ state vector, $\boldsymbol{u}$ the $p \times 1$ actuator input vector, $\boldsymbol{y}$ the $q \times 1$ sensor output vector. The redundancy relations are specified mathematically. Let the subspace of $(s+1)q$ dimensional vectors $\mathbf{v}$ be defined by (10):

$$P = \left\{ \mathbf{v} \mid \mathbf{v}^{\top} \cdot \begin{bmatrix} C \\ C \cdot A \\ \vdots \\ C \cdot A^{s} \end{bmatrix} = 0 \right\} \tag{10}$$

which is called the parity space of order s. Every vector $\mathbf{v}$ can be used at any time k for a parity check:

$$r(k) = \mathbf{v}^{\top} \left[\begin{bmatrix} y(k-s) \\ \vdots \\ y(k) \end{bmatrix} - \mathbf{H}_1 \begin{bmatrix} u(k-s) \\ \vdots \\ u(k) \end{bmatrix} \right] \tag{11}$$

with

$$\mathbf{H}_1 = \begin{bmatrix} 0 & 0 & 0 \,\ldots\ldots\ldots\ldots & 0 \\ C{\cdot}B & 0 & 0 \,\ldots\ldots\ldots\ldots & 0 \\ C{\cdot}A{\cdot}B & C{\cdot}B & 0 \,\ldots\ldots\ldots\ldots & 0 \\ \vdots & \ldots\ldots\ldots\ldots\ldots\ldots & & 0 \\ C{\cdot}A^{s-1}{\cdot}B & \ldots\ldots\; C{\cdot}A{\cdot}B & C{\cdot}B & 0 \end{bmatrix}. \tag{12}$$

Substituting the state equations (8) and (9) in $r(k)$ yields:

$$r(k) = \mathbf{v}^{\top} \cdot \begin{bmatrix} C \\ C{\cdot}A \\ \vdots \\ C{\cdot}A^{s} \end{bmatrix} \cdot \boldsymbol{x}(k-s)\,. \tag{13}$$

$r(k)$ is zero if no faults occur. The redundancy relation is simply an input-output model for a part of the dynamics of the system. The robustness of the FDI scheme is achieved by choosing the most reliable relations instead of overall mathematical model.

Let the model from (8) be improved taking unknown inputs and the fault vector into account. The system description is then as follows:

$$\boldsymbol{x}(k+1) = \mathbf{A} \cdot \boldsymbol{x}(k) + \mathbf{B} \cdot \boldsymbol{u}(k) + \mathbf{E} \cdot \boldsymbol{d}(k) + \mathbf{K} \cdot \boldsymbol{f}(k) \tag{14}$$

$$\boldsymbol{y}(k) = \mathbf{C} \cdot \boldsymbol{x}(k)\,. \tag{15}$$

$\mathbf{E}$ is a $n \times s$ dimensional distribution matrix of the unknown input signal, $\vec{d}(k)$, $\mathbf{K}$ is the $n \times 1$ dimensional distribution matrix of the fault vector, $\boldsymbol{f}(k)$. The problem of complete disturbance decoupling can be solved by transformation of the system to so called Kronecker canonical form. In many practical situations, complete decoupling may not be achievable, because there may be too many disturbances present in the system. The best compromise that can be achieved in such a case is to make the residual "optimal" in the sense of minimising a performance index which relates the effects of disturbances to the effects of faults. Let the performance index be a ratio of the Euclidean norm of the effects of disturbances to the Euclidean norm of the effects of faults:

$$P = \frac{\|\mathbf{v}^\top \cdot \mathbf{H}_2\|_2}{\|\mathbf{v}^\top \cdot \mathbf{H}_3\|_2} \tag{16}$$

where

$$\mathbf{H}_2 = \begin{bmatrix} 0 & 0 & 0 \,\dots\dots\dots\dots & 0 \\ C{\cdot}E & 0 & 0 \,\dots\dots\dots\dots & 0 \\ C{\cdot}A{\cdot}E & C{\cdot}E & 0 \,\dots\dots\dots\dots & 0 \\ \vdots & \dots\dots\dots\dots\dots\dots & & 0 \\ C{\cdot}A^{s-1}{\cdot}E & \dots\dots\dots & C{\cdot}A{\cdot}E \;\; C{\cdot}E & 0 \end{bmatrix} \tag{17}$$

$$\mathbf{H}_3 = \begin{bmatrix} 0 & 0 & 0 \,\dots\dots\dots\dots & 0 \\ C{\cdot}K & 0 & 0 \,\dots\dots\dots\dots & 0 \\ C{\cdot}A{\cdot}K & C{\cdot}K & 0 \,\dots\dots\dots\dots & 0 \\ \vdots & \dots\dots\dots\dots\dots\dots & & 0 \\ C{\cdot}A^{s-1}{\cdot}K & \dots\dots\dots & C{\cdot}A{\cdot}K \;\; C{\cdot}E & 0 \end{bmatrix}. \tag{18}$$

The system from (14) and (15) can now be written as:

$$\begin{aligned} \begin{bmatrix} y(k-s) \\ y(k-s+1) \\ \vdots \\ y(k) \end{bmatrix} &= \begin{bmatrix} C \\ C{\cdot}A \\ \vdots \\ C{\cdot}A^s \end{bmatrix} \mathbf{x}(k-s) \\ &+ \mathbf{H}_1 \begin{bmatrix} u(k-s) \\ u(k-s+1) \\ \vdots \\ u(k) \end{bmatrix} + \mathbf{H}_2 \begin{bmatrix} d(k-s) \\ d(k-s+1) \\ \vdots \\ d(k) \end{bmatrix} \\ &+ \mathbf{H}_3 \begin{bmatrix} f(k-s) \\ f(k-s+1) \\ \vdots \\ f(k) \end{bmatrix} \end{aligned} \tag{19}$$

In order to generate a scalar residual $r(k)$, one has to check if the above state equations hold for the available input and output data. This can be done by calculating equation (20) on-line at each sampling time k:

$$r(k) = \mathbf{v}^\top \cdot \left[\begin{bmatrix} y(k-s) \\ y(k-s+1) \\ \vdots \\ y(k) \end{bmatrix} - \mathbf{H}_1 \cdot \begin{bmatrix} u(k-s) \\ u(k-s+1) \\ \vdots \\ u(k) \end{bmatrix} \right]. \tag{20}$$

In order to make the residual $r(k)$ independent of any initial conditions $\mathbf{x}(k-s)$, vector $\mathbf{v}^\top$ has to be chosen by equation (10). As the residual has to be affected by the faults, the following must hold:

$$\mathbf{v}^\top \cdot \mathbf{H}_3 \neq 0\,. \tag{21}$$

But $\mathbf{v}^\top$ has to be determined as to satisfy the condition:

$$\mathbf{v}^\top \cdot \mathbf{H}_2 = 0\,. \tag{22}$$

which implies that the residual is not affected by the unknown input vector $\boldsymbol{d}$. This would be an ideal solution. A performance index P from equation (16) is a proper compromise if it is minimised. To ensure that equation (10) is fulfilled, the problem is reformulated to finding a vector $\boldsymbol{w}^\top$ such that the performance index

$$P = \frac{\|\mathbf{v}^\top \cdot \mathbf{V}_0 \cdot \mathbf{H}_2\|_2}{\|\mathbf{v}^\top \cdot \mathbf{V}_0 \cdot \mathbf{H}_3\|_2} \tag{23}$$

becomes minimal. $\mathbf{V}_0$ is a base for all possible solutions to equations (10). Hence $\boldsymbol{w}^\top$ singles out the best vector $v^\top$ of all possible solutions represented by $\mathbf{V}_0$. The solution to the optimisation problem according to equation (16) can be obtained by a differentiation of the performance index by $\boldsymbol{w}^\top$. This leads to the relation:

$$\boldsymbol{w}^\top \cdot \left(\mathbf{V}_0{\cdot}\mathbf{H}_2{\cdot}\mathbf{H}_2^\top{\cdot}\mathbf{V}_0^\top - P{\cdot}\mathbf{V}_0{\cdot}\mathbf{H}_3{\cdot}\mathbf{H}_3^\top{\cdot}\mathbf{V}_0^\top \right) = \mathbf{0}\,. \tag{24}$$

The solution to equation (24) gives the solution of the design problem. Thus the problem reduces to a generalised eigenvalue-eigenvector problem. The minimal eigenvalue is the optimal value of the performance index and the corresponding eigenvector is the selector for the optimal residual generator $\mathbf{v}^\top$.

Parameter Estimation Approach

W. Goedecke has used parameter estimation methods using linear equations for heat transfer, derived by Isermann, 1965, for fault detection in a tubular heat exchanger [6]. The derived model turned out to be quite simple as homogeneous temperature dispersion in the shell was considered due to steam used for heating the product. The heat transfer coefficients were identified and thus change in model parameters detected using continuous-time model. The parameter identification methods are well known and available in literature (see the work of Isermann, for instance) thus the method is only mentioned here. The identification algorithm can be applied in continuous or discrete time. If continuous-time is applied (no need for z-transform), the derivatives of the signals have to be either measured or obtained using observers. Best results were obtained using state variable filters [7]. Another method of obtaining signal derivatives is by using real differenciators. Signals have to be properly filtered before application, thus a high sample rate is required.

6 DISCUSSION AND CONCLUSIONS

There are three main hazardous events associated with the process industry, especially its chemical branch. These are releases and spills, fires, explosions. Each of these has its causes, (called also the symptoms) and consequences. These events can react with humans and environment directly and/or indirectly. In general, there are two different ways of preventing these hazardous events from happening. The *passive* methods mean safe operation achieved through process engineering methods as minimising fire loads, protection from ignition sources, implementation of fire-protective equipment, fire-safe enclosures, keeping the concentrations of flammable substances outside the explosion range, keeping the temperatures below the flash point, minimising the concentrations of oxidising agent, implementation of proper barriers included with the vessels, use of proper equipment materials. The active methods are achieved through process control engineering and include the process automation equipment that works online. The automation should be able to minimise the probability of the causes for the hazardous situation, it should activate proper control actions to prevent the hazard, be able to support proper operator actions and release proper actions to restrict the consequences. Proper measurement equipment for safety reasons and fault detection has to be predicted and installed during planning and installation phase of the plant as some process variables and parameters are not important for the production itself but are of significant meaning for quality of production and safe processing. The studies have shown that poor instrumentation and operator errors are the main causes for accidents in chemical plants. This proves that hazard studies are important and that the automation level should be as high as technology enables. Hazard studies should also determine the points and parts of the plant where early fault detection and insulation is of significant meaning.

The complete Fault Detection and Isolation (FDI) scheme includes a combination of analytical and heuristic methods. The analytical redundancy is an alternative approach to physical redundancy. Physical redundancy means that redundant signals are generated by means of a set of equal redundant sensors through which the failed ones can be detected. Analytical redundancy uses mathematical models and observers to generate redundant signals. Changes in model parameters can be detected by parameter estimation methods. A set of observers can be used to detect either sensor, component or actuator faults. If the symptoms of a fault are well known, the fault can be detected on time to prevent it to arise to a failure that could lead environmental damage (vessel leakage, release, fire, explosion) or loss of human life. Nevertheless, implementation of FDI schemes increases the occupational safety as human is excluded from the process. However, an appeared fault is detected automatically and proper reconfiguration is carried out to keep the process in a safe state.

There are several ways of testing the FDI scheme performance. It can be tested either through simulations, where the main problem is that disturbances, unknown inputs and noise cannot be modelled properly. Another way is to work off-line and test the performance of the FDI scheme on previously measured signals. The main problem here is that behaviour of the closed loop system cannot be tested.

References

[1] TOOLA, A.: The Safety of Process Automation, Automatica **29** No. 2 (1993), 541–548.

[2] ISERMANN, R.: Fault Diagnosis of Machines via Parameter Estimation and Knowledge Processing-Tutorial Paper, Automatica **29** No. 4 (1993), 815–835.

[3] BLANKE, M.—NIELSEN, S. B.—JORGENSEN, R. B.: Fault Accommodation in Feedback Control Systems, Department of Control Engineering, Research Report R93-4013, April 1993.

[4] PATTON, R.—FRANK, P.—CLARK, R. (Ed.): Fault Diagnosis in Dynamic Systems, Prentice Hall, New York, 1989.

[5] FRANK, P. M.: Fault Diagnosis in Dynamic Systems Using Analytical and Knowledge-Based Redundancy — a Survey and Some New Results, Automatica **26** No. 3 (1990), 459–470.

[6] GOEDECKE, W.: Fault Detection in a Tubular Heat Exchanger Based on Modelling and Parameter Estimation, In: IFAC Identification and Parameter Estimation 1985, York, UK, 1985.

[7] YOUNG, P.—JAKEMAN, A.: Refined Instrumental Variable Methods of Recursive Time-Series Analysis, International Journal of Control **31** (1969), 741–746.

Received 9 September 2000

Drago Valh, born in Maribor, Slovenia, in 1973, graduated in electrical Engineering from the University of Maribor in 1997. He started his MSc studies the same year at Polytechnic, Nova Gorica, Slovenia. His field of research interest is above all fault detection and accommodation in industrial processes.

Boris Tovornik, born in Maribor, Slovenia, graduated from the University of Ljubljana in 1974 and received the MSc and PhD degrees in electrical engineering from the University of Maribor, in 1984 and 1991, respectively. He is with the same university, Faculty of Electrical Engineering and Computer Science, at present as Associate Professor. His fields of research interests are computer control of industrial processes, modelling and process identification, fuzzy control, intelligent systems, fault detection, supervision and safety. He is a member of IEEE, KoREMA, Automatic Control Society of Slovenia,

Zoran Vukić, born in Zagreb, Croatia, graduated from the Faculty of Electrical Engineering and Computer Science and received MSc and PhD degrees in Electrical Engineering from the University of Zagreb in 1972 and 1989 respectively. He is with the same university, Faculty of Electrical Engineering and Computer Science, at present as Associate Professor. His fields of research interests are marine control, process automation, process identification, intelligent control. He is a member of IFAC, IEEE, KoREMA, Tau, Beta pi, EtaKapaNu.