1. Introduction

The control system faults are one of the main causes of breakdowns in industrial processes. According to presented by ABB data, 36% of all problems are caused by failures of control system components, including faults of sensors and actuators primarily. These devices are installed on the process installation, which creates for them negative conditions, the control units, installed in the control rooms, are damaged relatively rare. If we consider damages caused by control systems exclusively, then not more than 10% of them are caused by faults of control units. The others are the consequences of faults of sensors and actuators. In contrast, paradoxically different redundant solutions are developed and are commercially available primarily for any kind of controllers and computer networks.

Examples of serious industrial accidents caused by damage to the measuring equipment are:

- Damage in the fuel storage Buncefield, on 11 December 2005. A fault of the level sensor caused overflow of the fuel tank and ignition. Next, a series of explosions and fire of aviation fuel occurred. It was the largest fire in Europe. There were 40 injuries and substantial material damage (£ 5bn) [1].
- Damage in Texas City, USA, on 23 March 2005, in the largest oil refinery BP International. During a start-up procedure of the separator plant at the Isomerization Department, producing high octane unleaded gasoline additives, level sensors have failed. It caused the level overflow in the distillation column, resulting in a rapid evaporation, a pressure increase, a raffinate ejections, and consequently explosion and fire. 15 people were killed and 170 were injured. Separator plant and evaporation of hydrocarbons plant were destroyed [2].
- Damage in Texas City, USA, on 23 March 2005, in the largest oil refinery BP International. During a start-up procedure of the separator plant at the Isomerization Department, producing high octane unleaded gasoline additives, level sensors have failed. It caused the level overflow in the distillation column, resulting in a rapid evaporation, a pressure increase, a raffinate ejections, and consequently explosion and fire. 15 people were killed and 170 were injured. Separator plant and evaporation of hydrocarbons plant were destroyed [2].
- Damage in Texas City, USA, on 23 March 2005, in the largest oil refinery BP International. During a start-up procedure of the separator plant at the Isomerization Department, producing high octane unleaded gasoline additives, level sensors have failed. It caused the level overflow in the distillation column, resulting in a rapid evaporation, a pressure increase, a raffinate ejections, and consequently explosion and fire. 15 people were killed and 170 were injured. Separator plant and evaporation of hydrocarbons plant were destroyed [2].

The need to ensure an adequate level of security, i.e. reducing the risk to an acceptable level, was the cause of the development of international standards of functional safety. Functional safety related to all activities in the life cycle of the E/E/PE control systems (containing the electrical/ electronic/ programmable electronic components), constitutes an important aspect of functional safety. Various standards have been developed, e.g. in the area of general principles of functional safety - IEC 61508 [11,20,21], in the field of industrial processes - EN 61511, in the scope of machines - EN 62061 [12] and in the scope of nuclear energy - IEC 61513.

The most important is the new version of IEC 61508 standard [21]. It was adopted as a European standard EN 61508, and next as a national standard PN-EN 61508 [33]. IEC 61511 standard is currently being updated and will be published with a delay as a European standard (EN) and national (EN). It contains a number of additions and refers more broadly to the current IEC 61508 standard, mainly of its parts 5, 6 and 7. New versions of these standards broadly include theoretical issues (numerous citation of recognized publications) and the requirements for mathematical models in terms of verification and validation of the proposed solutions [21].

(*) Teść artykułu w polskiej wersji językowej dostępny w elektronicznym wydaniu kwartalnika na stronie www.ein.org.pl
The concept of Fault Tolerant Control Systems (FTCS), has been discussed in the paper. According to the authors, these systems could provide a new protection layer within the meaning of the standards associated with the functional safety. Mainly faults of sensors and actuators are taken into account in FTC systems, which leads to a significant value increase of the reliability and safety coefficients of the control systems and thus of the whole process. An exemplary control system of the condensing turbine tolerating sensor faults, has been presented in the paper [29-32, 41]. The influence of diagnosis and fault tolerance on values of the reliability and safety coefficients, has been also discussed.

2. Protection layers

The purpose of safety-related control systems is to reduce the risk, and thus to decrease the frequency of occurrence of dangerous events or to reduce the effects of such events. The applied security systems have a layered structure as shown in Fig.1.

Fig. 1. The protection layers.

The first layer represents the process installation, which should be resistant to internal and external disturbances (security actions and technological blockades). The second layer is represented by a basic process control system (BPCS). It can be Distributed Control System (DCS), which integrates a control and monitoring tasks or system consisting of Supervisory Control and Data Acquisition (SCADA) and PLC/PAC (Programmable Logic Controller/Programmable Automation Controller). The third layer is a separate alarm system and operator’s intervention. SIS (Safety Instrumented System) constitutes the fourth layer. The aim of these four mentioned above layers is to prevent the occurrence of failures. The fifth layer engineering security systems, such as the safety valves, curtains, protective barriers, housing, etc., which aim is to reduce the effects of damage occurred. Even higher layers realize internal and external procedures, and technical measures, whose aim is to minimize human and material losses.

Commonly used SIS systems implement the safety automatic algorithms and the activation of blockades, whose task is to achieve the proper process operation. Signals generated by SIS systems, for instance, cut off supply or raw materials, block actuators in a safe position, run the shut-off valves, set a safe operating status of engines, pumps, ventilators, etc. Usually, SIS actions are associated with shut-off a part of the process installation or even the whole process, which leads to economic losses.

Therefore, in the lower layers (1, 2 and 3), it is advisable to use solutions that can guarantee the elimination of hazards in the early stages of their development. Methods of reducing the risk, which do not caused the process shut-off, are:

1. Robust construction of process installation thanks to solid design and high quality building and exploitation; passive solutions are used, which do not require any control as well as any operator’s intervention to avoid the dangerous situations,
2. Hardware and software redundancy of the control system elements,
3. Separate alarm-advisory systems,
4. Appropriately designed process visualization,
5. Training of operators, especially with use of process simulators, based on which the various emergency scenarios can be applied,
6. On-line diagnosis systems of the process and automation field devices,
7. Fault tolerant control systems (FTCS).

The first four solutions are commonly known and used. While the others are recently developed intensively [13,21,28]. The last three of the methods listed above are not covered sufficiently in safety standards.

3. Idea of fault tolerant control systems

The fault tolerant control algorithms are currently one of the most important directions of research and development in the field of automation. They were discussed, among others, in monographs [3, 8, 9, 13, 18, 25, 28, 36]. The first works on the FTC focused on the aerospace industry. Nowadays, however, in addition to applications in aircrafts, FTC systems are designed for industrial processes more frequently [14-16, 39, 38-41].

Integration of FTCS with diagnostic systems represent a new, additional layer for safety and protection of controlled processes. Block diagram of the automation system with a layer of the on-line diagnosis and fault tolerant control and security system SIS is shown in Fig. 2. The presented solution constitutes a modern concept of risk reduction while ensuring minimum of the economic losses caused by failures.

Fig. 2. Diagram of control system, on-line diagnosis and process security
The idea of development of active FTC systems lies in the implementation of on-line diagnostics and real-time reconfiguration of the hardware or software structure system in the cases when faults occur. Therefore, these systems have a variable structure, as given in Fig. 3.

A very important aspect of any of the FTC system is a realization method of fault detection and fault isolation. The solution adopted should provide an early detection of faults as well as such their distinguishability, which will allow to take a decision about the necessary reconfiguration of the system. Methods of diagnosis of industrial processes are discussed in monographs [5, 7, 17, 18, 22, 23, 27, 35, 42] and in many review articles, including works [4,6,14,19,23,24,26].

The concept of fault tolerant control systems is consistent with the structure of a dynamic redundancy of the type “1 oo 2”. The main difference lies in the fact that:

- Instead of a hardware redundancy, the analytical (information) redundancy (i.e. software redundancy) is used in FTC systems,
- In control systems, a dynamic redundancy is mostly used for controllers, while in FTC systems the sensor and actuator are taken into account especially,
- Different diagnostic methods are used:
  - to diagnosis of the controller faults - methods of system diagnosis,
  - to diagnosis of the sensor and actuator faults - methods of process diagnosis,
- Dynamic redundancy is introduced by system manufacturers (the designer can apply it or resign from it), while providing fault tolerance becomes the task of the designers.

In complex control systems, even in the absence of hardware redundancy, are usually a possibilities to reconfigure the automation system to avoid or to reduce the negative impact of the sensor faults on the process functioning [6,16,30,31,37,41]. The virtual sensors are most commonly used to reproduce signals from damaged sensors. They calculate the signal value based on the partial process models, used independently and designed for control the:

- \( S \) - setpoint of power (\( P_{1B} \), signal introduced from the operator interface),
- \( P \) - actual operating point, signal introduced by the operator,
- \( E \) - faults, D - disturbances,
- \( PV \) - process variables,
- \( CV \) - control variables,
- \( S \) - Noises

Fig. 3. The diagram of fault tolerant control systems (\( SP \) – SetPoints, \( CV \) – Control Variables, \( PV \) – Process Variables, \( E \) – Faults, D – Disturbances, S – Noises)

Development of FTC system requires for each possible fault, the design of a set of operation algorithms, enabling a proper system operation during the existence of each particular fault. It is also necessary to design the set of procedures for a bumpless switch to the redundant control for each of the faults. However, the condition for such changes is a quick detection and precise isolation of faults.

Research in the field of FTC systems is focused on advanced control systems, while more than 90% of all applications are associated with PID controllers. This is the reason of delay of the current state of technology in relation to the progress in research. The current control systems, enable design of FTC systems to a limited extent only. They are not equipped with adequate diagnostic and reconfiguration software. Nowadays, FTCs applications are related to research and pilot deployments.

An example of the control system of the condensing turbine, which tolerates the sensor faults, is described in chapter 4 [25-28, 41].

4. The example of the condensing turbine control system, tolerating faults of sensors

4.1. The control system structure

The task of a condensing turbine is to obtain the maximum electrical power from the generator working in an integrated set of boiler-turbine-generator making up the energy block. The national electricity grid consists of many such energy blocks. Some of them have a high power. This makes the failure of a single block may violate the security of the entire system. Therefore, much attention is given to increasing the reliability of the control systems in the individual energy blocks, and thus the entire national power system [15,40].

The proper work of a condensing turbine is ensured by the control system shown in Fig. 4. The system has two different functional structures [30, 31, 41], used independently and designed for control the:

- \( \text{rotary speed of the turbine} \), during the start-up of energy block,
- \( \text{turbine power control with varying loads} \), during the normal operation of the energy block.

In the first case, the controlled variable is the rotary speed of turbine, measured in a mode of static redundancy type “2 oo 3”. While the setpoint value is determined in accordance with the programmed gradient of growth of rotary speed, taking into account the critical speed bandwidth. The purpose of this system is to achieve synchronous rotation of the turbine, allowing the inclusion of the block to work in the national electricity grid (so called synchronisation).

In the second case, the controlled variable is the active power (P) of energy block. While the setpoint value is determined based on the following signals [29,41]:

1. \( \text{Base setpoint of power (} P_{b} \text{)} \), signal introduced from the operator interface,
2. \( \text{System setpoint of power (} Y_{1} \text{)} \), signal transmitted from ARCM system (automatic control of frequency and power of electro-energy system) [15,29], so called secondary control of electro-energy system,
3. \( \text{BPP (actual operating point)} \), signal introduced by the operator of electro-energy system,
4. \( \text{Correction signal related to the pressure of fresh steam (} p_{T} \text{)} \), generated by POM (steam power limiter),
5. \( \text{Correction signal related to the absolute vapor pressure in the condenser (} p_{S} \text{)} \), generated by PrOM (vapor power limiter),
6. \( \text{Signal of the primary control related to the frequency of the electro-energy system} \)

The energy block implementing this type of system control, varies the power depending on the voltage frequency changes in the power network.
Setpoint values defined in pp. 1-3 are introduced as one of three speeds ($V_{\text{min}}$, $V_{\text{avg}}$, $V_{\text{max}}$), formed by OSO (loading speed limiter).

PI controller is used in both cases. It generates a current control signal ($I$), which is transmitted through the operator console A/M (auto/manual) to the electrohydraulic transducer, which controls the complex set of high-pressure hydraulic valves (ZRWP). Switch-over of the system structure is made by the binary signal WG transmitted from switch of the turbine generator WG.

The list of signals used to control and protection of the condensing turbine, has been shown in Table 1. The signals 10, 11 and 12 are measured for diagnostic reasons exclusively.
The type of membership function (trapezoidal, triangular, Gaussian) and the number of fuzzy sets determines unambiguously the number of rules. The value ranges of the model inputs are determined on the basis of measured process data archived by the SCADA or DCS. The structure of artificial neural networks. The construction of NFS models is a combination of fuzzy modeling and expert knowledge.

### Table 1. List of signals used in the control system of the condensing turbine.

<table>
<thead>
<tr>
<th>No.</th>
<th>Analog signal</th>
<th>Symbol</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>active power of generator</td>
<td>(P)</td>
<td>MW</td>
</tr>
<tr>
<td>2</td>
<td>pressure of fresh steam</td>
<td>(P_t)</td>
<td>MPa</td>
</tr>
<tr>
<td>3</td>
<td>absolute vapor pressure in condenser (vacuum)</td>
<td>(P_v)</td>
<td>kPa (%)</td>
</tr>
<tr>
<td>4</td>
<td>mass flow of steam</td>
<td>(M_{DT})</td>
<td>t/h</td>
</tr>
<tr>
<td>5</td>
<td>base setpoint of power</td>
<td>(P_b)</td>
<td>MW</td>
</tr>
<tr>
<td>6</td>
<td>system setpoint of power</td>
<td>(Y_1)</td>
<td>MW</td>
</tr>
<tr>
<td>7</td>
<td>actual operating point</td>
<td>BPP</td>
<td>MW</td>
</tr>
<tr>
<td>8</td>
<td>frequency of electric current</td>
<td>(f)</td>
<td>Hz</td>
</tr>
<tr>
<td>9</td>
<td>rotational speed of turbine</td>
<td>(n)</td>
<td>1/min</td>
</tr>
<tr>
<td>10</td>
<td>control signal, current signal</td>
<td>(I)</td>
<td>mA</td>
</tr>
<tr>
<td>11</td>
<td>oil pressure pulse</td>
<td>(P_i)</td>
<td>MPa</td>
</tr>
<tr>
<td>12</td>
<td>opening degree of control valves</td>
<td>(X)</td>
<td>%</td>
</tr>
</tbody>
</table>

### 4.2. Fault Detection and Fault Isolation

There are two phases distinguish during a process diagnosis (Fig. 3): fault detection (FD) and fault isolation (FI). For FD purposes, the method based on relationships between values of process variables, is used in the considered example. On the basis of these relationships, the partial process models are designed, which constitute an information redundancy. The goal is to find models with possible simple structures which satisfactorily meet established requirements. The search for simple structures arises from the need to minimize the calculation time of model output. Adopted relationships should also take into account the dynamics of the value changes of the model parameters. Taking into account the above aspects, the following relations were distinguished for the modeling purposes:

\[
\Lambda P_t = f(M_{DT}, P_t-1) \tag{1}
\]

\[
\Lambda M_{DT} = f(X_t, M_{DT-1}) \tag{2}
\]

\[
\Lambda p_i = f(I) \tag{3}
\]

\[
\Lambda I = f(P, P_t) \tag{4}
\]

Symbols used in the formulas (1, 2, 3, 4), have been defined in Table 1.

One way to design models for diagnostic purposes is to use the idea of neural fuzzy systems, Takagi-Sugeno-Kang (NFS-TSK). This mathematical apparatus can be used for reliability analysis [10] or modeling for the purpose of analytical redundancy [38].

There are known algorithms of model identification, with the use of genetic optimization, in which the selection of TSK model structure and parameters is fully automatically implemented [38].

NFS model created in accordance with the formula (1), is shown in Fig. 5. On the other hand, Fig. 6 presents the trends of the following variables: \(M_{DT}\) - the mass flow of the steam, \(P\) - the active power of the generator, \(P_t^\prime\) - output from the model represented by the formula (1) with specified input signals, \(r_1\) - residuum of the model, understood as the difference \(r_1=P-P^\prime\). The residual chart confirms that model sufficiently reflects reality for diagnostic purposes.

The presented relationships were also tested in terms of their sensitivity to detect of sensor faults. The sensor faults can be classified into two basic types: catastrophic faults and parametric faults. The catastrophic faults cause a sudden change of the residuum value. Such a change implies the need to make immediate appropriate safety action. In contrast, the parametric faults are associated with the aging of the components. They are manifested in the form of accumulation of the residuum value. Measures of these changes are mean or variance of the residuum value. On the basis of these parameters a decisions about the need to change the operation parameters is made, or requires the model weights to be recalculated according to the selected neural network learning algorithm. The designed model should provide sufficient modeling accuracy for diagnostic purposes.

In order to verify the sensitivity of the model to detect disturbances in the measurement circuit of the active power of the generator, a special fault was simulated. The fault consisting in setting a fixed value of the signal, at a certain moment, for a certain time. Simulation effects of this disturbance, are shown in Fig. 7. The trends demonstrate that the residuum is sensitive to the simulated fault of the active power sensor. The average values of residuals in the sliding window, are used for detecting of faults of measuring circuits. This constitutes the simplest way of filtration.

The next step in the diagnostic process is the isolation of the damaged measuring circuit. There are many methods of fault isolation. One of the ways is to present relationship: faults-symptoms in the form of a binary diagnostic matrix. The elements of the matrix take on the value of the residuum chart confirms that model sufficiently reflects reality for diagnostic purposes.

The presented relationships were also tested in terms of their sensitivity to detect of sensor faults. The sensor faults...
a value of 0 or 1, wherein a value of 1 indicates that the residuum is sensitive to a given fault. The fault occurrence causes that the residuum deviates from zero. The exceeding of the defined threshold, is interpreted as a symptom occurrence.

During the design process, one should identify the sensitivity of all the residuals for each fault. The binary diagnostic matrix prepared for the analyzed control system is shown in Table 2.

**Table 2. The binary diagnostic matrix.**

<table>
<thead>
<tr>
<th>n = P – P</th>
<th>M_{DT}</th>
<th>P</th>
<th>p_{i}</th>
<th>\lambda</th>
<th>l</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>n = M_{DT} – M_{DF}</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>p_{i}</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>n = I – I</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
</table>

Detection of sensor fault must result in the reconfiguration of the control system structure or changing the control algorithm. The condensing turbine control system plays a very responsible role in the national power system, therefore immobilizing of the turbine due to fault of the measuring circuits of process variables is not allowed [31, 32].

### 4.3. Reconfiguration after the occurrence of faults

When starting to design the control system tolerating faults of measuring circuits, it is to specify a set of possible states of the operation (F) of the system, in the case of particular faults:

\[ F \equiv \{ f_{m} : m = 1, 2, ..., M \} \]

Brief description of the possible change of the system operation when occur the faults defined in Table. 1, has been presented in Table 3.

**Table 3. System reconfiguration after the occurrence of possible faults of measuring circuits.**

<table>
<thead>
<tr>
<th>State</th>
<th>Fault of measuring circuit</th>
<th>Possible change of operation when fault occur</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>Active power (P) produced by generator</td>
<td>Use of virtual power sensor or switching to manual control of turbine valves from operator console.</td>
</tr>
<tr>
<td>F2</td>
<td>Pressure of fresh steam (p_{i})</td>
<td>Disconnection of the primary control. Blockade of intervention power (blockade of Y1 signal). Turning off the steam power limiter (POM). Setting the minimum speed in the loading speed limiter (OSO).</td>
</tr>
<tr>
<td>F3</td>
<td>Absolute vapor pressure in condenser (vacuum) (p_{i})</td>
<td>Turning off the vacuum power limiter (PrOM). Blockade of intervention power (blockade of Y1 signal).</td>
</tr>
<tr>
<td>F4</td>
<td>Mass flow of steam (M_{DF})</td>
<td>Disconnection of the signal Y_{m} coupling of the boiler control system with the turbine control system.</td>
</tr>
<tr>
<td>F5</td>
<td>System setpoint of power (ARC-M1)</td>
<td>Disconnection of the signal Y1 from the secondary control (system power setpoint).</td>
</tr>
<tr>
<td>F6</td>
<td>Actual operating point (BPP)</td>
<td>Changing the setpoint from BPP on P_{b} – the base setpoint of power (on the operator panel).</td>
</tr>
<tr>
<td>F7</td>
<td>Frequency of the electric current (f)</td>
<td>Use of turbine rotary speed instead of a current frequency.</td>
</tr>
<tr>
<td>F8</td>
<td>The rotational speed of the turbine (n)</td>
<td>Rejection of measurements from a faulty sensor and work with the other two.</td>
</tr>
<tr>
<td>F9</td>
<td>Measurement of the control signal (l)</td>
<td>Reconfiguration of diagnostic system which supports the control system.</td>
</tr>
</tbody>
</table>

The oil pressure pulse (p_{i})

The opening degree of control valves (X)

One of the most important signals introduced to the control system for the purpose of control and safety, is the steam pressure p_{i}. In control systems with a leading turbine, checking the steam pressure is intended to protect the energetic block against the unacceptable power fluctuations. The power generated by the energetic block should be adapted to the current possibilities of water, air and fuel supply installations. Therefore, in case of fault detection of the steam pressure measuring circuit, one should change the operation manner of the con-

---

**Fig. 6. The modeling results for the data not covered by a training data set. Model was created on basis of formula (1)**

**Fig. 7. Simulation of a disturbance in the measurement circuit of the active power (P). Symbols used: P - active power generator, P^* - calculated output of the model based on formula (1), P^* - fault simulation of the power measurement circuit, MDF - steam mass flow, rI - model residuum**
control system so that the fault does not have a negative impact on the whole energetic block. For this purpose, it is necessary to reconfigure the system, consisting of the following actions:

1) Disconnection of the primary control system, because it is relatively fast and can have a negative impact on the operation of the energetic block, in the absence of appropriate value of the steam pressure,
2) Blockade of the binary signal Y1i of the intervention power,
3) Turning off the steam power limiter (POM). The characteristics of the output of this programming block is depending on the measured value of the steam pressure. Incorrectly measured pressure value may send false signals to the power setpoint for the whole energetic block,
4) Setting of minimum speed \( V_{\text{min}} \) [MW/min] in OSO (loading speed limiter).

With the above assumptions, the block can operate to a limited extent, even with the remote signals, as shown in Fig. 8. Additional protective signals \( Y_{\text{m}} \) and \( Y_{\text{p}} \), coupling the power control system with a control steam pressure in the boiler, which ensure to get the adequate power in the system with the leading turbine. In this kind of systems the turbine power control plays in the energetic block the primary role. In contrast, the boiler steam pressure control is subordinated. One should stress, however a general rule, that it is better to switch off the remote setpoint source, than defending the remote control mode at all costs. This could result in disconnection of the energetic block from the national electro-energy system.

5. Influence of diagnostics and fault tolerance on the coefficients of system reliability and system safety

A positive influence of fault tolerance and diagnosis carried out in real time on the reliability and security of the system can be demonstrated by analyzing the coefficients characterizing these properties. Definition of the fully operational system state and the faulty system states (e.g. F1-F9 states shown in Table 3), is given in Fig. 9. The characteristic time intervals have the following meaning:

- Mean time to failure (MTTF) - \( T_f \),
- Mean time to repair (MTTR), i.e. the average time interval from the failure occurring till the repair of a faulty device - \( T_r \),
- Mean time between failures (MTBF), i.e. \( MTBF = MTTF + MTTR \),
- Mean time of diagnosis - \( T_d \),
- Mean time of renewal, i.e. replacing the defective device to the efficient one together with the restoration of the system after repair/replacement - \( T_N \).

In case of the repairable systems, such as FTCS, the system availability coefficient, is widely used as the reliability indicator [44]. It is defined by the formula:
The formula (10) indicates that the performance of on-line diagnostic tests of all dangerous failures, gives the possibility to increase the diagnostic coverage factor $DC$ to 1. This reduces the risk, in other words decreases the probabilities $PFH_{SYS}$ or $PFH_{SYS}$. 

Another indicator illustrating the effect of diagnosis is the Safety Failure Fraction (SFF):

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}} = \frac{\lambda - \lambda_{DU}}{\lambda}$$  (11)

This factor is essential for SIL verification of the E/E/PE systems carried out on the basis of data related to the tolerability of hardware failures. The more failures are detectable, the value of this ratio increases, and with full detectability it reaches a value of 1.

In the definitions of $DC$ and $SFF$ specified in the standard, there are distinguished failures both detectable and undetected using on-line diagnostic tests. However, it looks like a mistake resulting from imprecise terminology. In fact, the condition for effective protective action is a precise failure isolation. Therefore, there is a need not only for detectability, but also distinguishability of each failure in the isolation phase.

The basic structure of the considered turbine control system (Fig. 10) is helpful in determination of the probability of dangerous failure ($PFH$).

The formula (10) indicates that the performance of on-line diagnostic tests of all dangerous failures, gives the possibility to increase the diagnostic coverage factor $DC$ to 1. This reduces the risk, in other words decreases the probabilities $PFH_{SYS}$ or $PFH_{SYS}$. 

Another indicator illustrating the effect of diagnosis is the Safety Failure Fraction (SFF):

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}} = \frac{\lambda - \lambda_{DU}}{\lambda}$$  (11)

This factor is essential for SIL verification of the E/E/PE systems carried out on the basis of data related to the tolerability of hardware failures. The more failures are detectable, the value of this ratio increases, and with full detectability it reaches a value of 1.

In the definitions of $DC$ and $SFF$ specified in the standard, there are distinguished failures both detectable and undetected using on-line diagnostic tests. However, it looks like a mistake resulting from imprecise terminology. In fact, the condition for effective protective action is a precise failure isolation. Therefore, there is a need not only for detectability, but also distinguishability of each failure in the isolation phase.

The basic structure of the considered turbine control system (Fig. 10) is helpful in determination of the probability of dangerous failure ($PFH$).

Probability $PFH_{SYS}$ of the entire system is defined by formula (12):

$$PFH_{SYS} = PFH_{Measurements} + PFH_{Control system} + PFH_{Valve servomotors}$$  (12)

In view of the fact that all the fault tolerance of measuring devices, $PFH_{Measurements}$ probability is zero and thus the value of the indicator $PFH$ of the entire system decreases.

The considered example shows that the implementation of fault tolerant control systems contributes significantly to improving the safety and reliability of control systems and controlled processes.

6. Summary

The integration of diagnostic software with control software is necessary to the implementation of fault tolerant control systems. Two solutions are possible. The first is based on integration of control software executed in PLC controllers with on-line diagnostic system implemented in a master computer. This diagnostic system receives necessary data from PLC controllers. Such a system is AMandD, designed in Institute of Automatic Control and Robotics at Warsaw University of Technology [23]. Information about faults transmitted from the diagnostic system to the controller initiates the necessary reconfiguration of control systems. AMandD system is still being developed under the name DiaSter, in cooperation with Rzeszow University of Technology, Silesian University of Technology and University of Zielona Gora [17, 38].

Such solution with a separate diagnostic system can cause too large delays in support of protective actions. A better solution is to implement necessary diagnostic software in PLC controllers. It should be an integral part of process control software. Speed of response to fault occurring in this case is much higher. The diagnostic methods should be used to ensure rapid detection of faults. They include methods...
based on models of objects. Such a solution has been implemented in the condensing turbine control system, in one of the national energetic blocks [29-32, 41].

It can be expected that in the nearest future, the rapid development of control systems equipped with software for process diagnosis and fault tolerance will take place. Also the number of industrial applications will grow in this field. Of course, such systems before deploying them to the industry, require full verification and validation of hardware and software, in accordance with the requirements of the relevant functional safety standards (PN-EN 61508 i PN-EN 61511 lub PN-EN 62061), in the overall functional safety management in the life cycle [20, 21]. A certain barrier for industrial applications is lack of sufficient number of appropriate specialists. However, now in many technical universities these issues are included in the curricula and young engineers will be prepared to implement innovative control systems.

References

30. Pawłak M, Karczewski J. Struktura UAR turbiny kondensacyjnej biorącej udział w regulacji systemu elektroenergetycznego – Structure of control system of condensation turbine taking part in control of electroenergy system. VII Konferencja Problemy Badawcze Energetyki

Mariusz PAWLAK
Jan Maciej KOŚCIELNY
Piotr WASIEWICZ
Institute of Automatic Control and Robotics
Warsaw University of Technology,
sw. Andrzeja Boboli 8, 02-525 Warsaw, Poland
E-mail: m.pawlak@mchtr.pw.edu.pl, jmk@mchtr.pw.edu.pl,
p.wasiewicz@mchtr.pw.edu.pl