Reliable Fault Tolerant Control design Based on Dynamic Safety Margin

M. Abdel-Geliel & E. Badreddin,
Automation Lab, University of Mannheim, Germany
elgeliel@ti.uni-mannheim.de **&** *badreddin@ti.uni-mannheim.de*

Abstract*— Dynamic safety margin (DSM) is a new performance index used to measure the distance between a predefined safety boundary in the state space and the system trajectory as it evolves. Controller design based on DSM is important to maintain a predefined margin of safety during the transient and in the presence of large disturbances particularly in safety-critical systems. Moreover, Designing a FTC system based on DSM is important to operate the system at an acceptable performance in addition to maintain a safe operation margin during the fault period. Some methods of implement DSM in controller design and adapting are introduced in this work mainly, PID and MPC controllers. Moreover, a framework of FTC system based on DSM is introduced.

1 INTRODUCTION

The evaluation of a control system depends mainly on the difference between the desired performance according to the given specifications and the actual performance. Safety is one of the most important specifications for the controlled system. Safety control problem requires moving the system from a given set of initial states in its state space to a predetermined safe region. Most of the work related to system safety use fault detection and isolation (FDI), fault tolerant control (FTC) or reliability study of system in order to protect the system and recover the system performance to be closer to the nominal values [1] -[4] .

The complexity of modern industrial processes makes high dependability an essential demand for reducing production loss, avoiding equipment damage, and increasing human safety. A more dependable system is a system that has the ability to: 1) detect faults as fast as possible; 2) diagnose them accurately; 3) recover the system to the nominal performance as much as possible. Therefore, a robust Fault Detection and Isolation (FDI) and a Fault Tolerant Control (FTC) system design have attained increased attention during the last decades.

An FTC system is a control system that can accommodate components faults in order to prevent faults from developing into failures. It has the ability to maintain stability and acceptable degree of performance when not only the system is fault-free but also when there are component malfunctions. The FTC system design can be classified as passive and active (PFTC and AFTC) [5] -[7] . A PFTC system deals with the faults as a source of modeling uncertainties or disturbance. Hence, PFTC systems do not need an FDI system. On contrary, the FDI system is necessary in an AFTC system in order to reconfigure the controller in case of fault. Although FTC is a recent research topic in control theory, the idea of controlling a system that deviates from nominal operating conditions has been investigated by many researchers. The method of dealing with this problem usually stem from linear quadratic, adaptive, or robust control [8] -[10] . Fault-tolerant control systems are characterized by their capabilities, after fault occurrence, to recover performance close to the nominal desired performance. In addition, their ability to be well-behave in a stable monotonic during a transient period between the fault occurrence and the performance recovery is an important feature.

In practice, however, because of a faulty part, the degree of the other system components capability could be significantly reduced. If the design objective still to maintain the original system performance, this will force the remaining parts to work beyond the nominal duty to compensate for the handicaps caused by the fault. This situation is highly undesirable in practice due to physical limitation of the other parts. The consequence of the so-designed FTC system may lead to a worse behavior and still cause further damage. Therefore, trade-off between achievable performance and safety requirements of the operation should be carefully considered in FTC system design [7] . Safety requirements appear as constraints in the state and control of the controlled system; which can be represented with DSM.

There are different control design techniques used in FTC scattered in literature see for example survey in [6] . Model Predictive Control (MPC) has the ability to handle explicitly hard constraints on control and states, which specify the actuator limits and safety operation. Moreover, the control objectives in normal and faulty case can be fulfilled using MPC either by adding new constraints, changing the internal model, and/or both. Therefore, MPC provide a suitable implementation architecture for FTC [12] , [14] .

Dynamic Safety Margin (DSM) is a new performance index for the control system design, which was introduced in [15] ,[16] and [17] . This index measures how far the system state trajectory is from a predefined safety boundary in the state space. The DSM concept, its computation methods, and its relationship to the state constraints are addressed in [16] , [18] . The DSM can be used in different control system applications; some of them are highlighted in [15] . To operate the system safely, The state variables of interest have to be inside that boundary region in normal operation and in case of uncertainties and/or disturbances.

Thus, controller design based on DSM permits to maintain a predefined margin of safety during transient and steady state of safety-critical systems. The inclusion of DSM into controller design can be achieved by various methods. Some of them are introduced in [15] , [18] , [17] , and [25] . In these contributions, adapting PID controller parameters, switching controller, Fuzzy controller, optimal control and/or MPC are highlighted.

The success of AFTC system is based on the correctness of FDI system. In practice, it is difficult to obtain either correct fault detection or an accurate and sufficient fault data because of the system disturbance and uncertainties. Therefore, a robust FDI system plays an important role in AFTC design. A robust FDI design based on DSM are introduced in [18] and [26] .

In some faulty situation, recovering the system performance to the nominal one cannot be fulfilled as stated before. As a result, reducing the output performance is necessary in order to increase the system availability. A framework of FTC system is introduced that combines the proposed FDI in [26] and the controllers design based on DSM, with accepted degraded performance in order to generate a reliable FTC system.
The fruitiness of the proposed approaches is illustrated using simulation and practical implementation results.

The paper is organized as follows: Dynamic safety margin and safety controller requirements are defined in section II. It is followed by the discussion about controller design based on specially, MPC and PID in Section III. The proposed FTC system based on MPC and DSM is explained in Section IV. An implementation example is illustrated in Section V. Finally, conclusion and future work are given in Section VI.

2 DSM Definition and Principle

The idea of DSM index is introduced in [15] and [16] . Briefly to explain the idea, let $\mathbf{X}$ be the state space in $\Re^n$, and consider that a subspace $\mathbf{\Phi} \subseteq \mathbf{X}$, which defines the safe operation region for some system state variables $\mathbf{x} \in \Re^m$ in the state subspace $\mathbf{\Phi}$, can be specified by a set of inequalities $\Phi=\{\mathbf{x} \mid \phi_i(\mathbf{x}) \le 0,\ i=1,...,q\}$, where ϕ_i: $\Re^m \to \Re$. $\phi_i(\mathbf{x}) > 0$ indicates unsafe operation (Figure 1) and $\partial\Phi=\{\mathbf{x} \mid \phi_i(\mathbf{x}) = 0,\ i=1,...,q\} \subset \Phi$ is the boundary of the safe region.. It is assumed that the system is stable in the sense of Lyapunov and that the safe region is fully contained in the stability region. Starting with the initial condition $\mathbf{x}_0$, the system trajectory will evolve to the operating point $\mathbf{x}_s$ traversing the state space with varying distance to the safety boundary. DSM is defined, in this case, as the instantaneous shortest distance $\delta(t)$, between the system state vector of interest and $\partial\Phi$ in this subspace of state variables. Therefore, the DSM can be obtained by solving the following optimization problem

$$\min_{\mathbf{x}_p} \left\| (\mathbf{x} - \mathbf{x}_p) \right\|_2^2 \quad ; \text{Subject to} \quad \mathbf{x}_p \in \partial\Phi \qquad (1)$$

and the DSM $\delta = s(t) \left\| (\mathbf{x} - \mathbf{x}_{p_o}) \right\|_2$ (2)

Where $\mathbf{x}_{po}$ is the solution of the previous optimization problem and

$$s(t) = \begin{cases} +1 \text{ if } \mathbf{x} \text{ inside the safe operation region} \\ -1 \text{ if } \mathbf{x} \text{ outside the safe operation region} \end{cases}$$

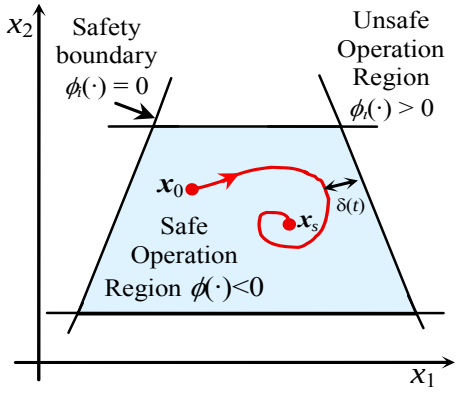


Figure 1: DSM definition

Variable q is the number of defined inequalities and m the number of state variables relevant to safety. Notice that $m \le n$, where n is the dimension of the state-space.

In most cases, the safe operation region can be defined by a set of linear inequalities as a polytope. In case that the boundary function is nonlinear, it can be subdivided into two or more linear constraints (piecewise linear approximation). Hence, safe region, Φ, can be formulated in general as a set of linear inequalities, in the form

$$\phi_i(\mathbf{x}) = \mathbf{a}_i^T \mathbf{x} - c_i \le 0 \qquad (3)$$

where $\mathbf{a}_i^T \in \Re^n$, $c_i \in \Re$ is a constant and $\phi_i(\cdot) = 0$ is a subspace of state vector $\mathbf{x}_i \subset \Phi$ where $\mathbf{a}_i^T \mathbf{x}_i = c_i$. Thus, for the state vector $\mathbf{x}$, $\delta_i(.)$ can be calculated [2] as

$$\delta i(t) = \frac{c_i - \mathbf{a}_i^T \mathbf{x}(t)}{\|\mathbf{a}_i\|_2} \begin{cases} \ge 0 & \text{iff } \phi_i(\mathbf{x}) < 0 \\ < 0 & \text{iff } \phi_i(\mathbf{x}) > 0 \end{cases} \qquad (4)$$

where $\delta_i(.)$ is the minimum distance between $\{\phi_i(\cdot) = 0\} \subset \partial\Phi$. For all boundaries, the distance vector

$$\mathbf{d}(t) = [\delta_1(t), \delta_2(t), \ldots, \delta_q(t)]^T$$

can be obtained from

$$\mathbf{d}(t) = \mathbf{d}_c - \mathbf{D}_a \mathbf{x}(t) \in \Re^q \qquad (5)$$

where $\mathbf{d}_c = \mathbf{D}_{ia} \mathbf{c}_c \in \Re^q$, $\mathbf{D}_a = \mathbf{D}_{ia} \mathbf{A}_c \in \Re^{q \times n}$

$$\mathbf{D}_{ia} = diag\left(\frac{1}{\|\mathbf{a}_1\|_2}, \frac{1}{\|\mathbf{a}_2\|_2}, \cdots, \frac{1}{\|\mathbf{a}_q\|_2} \right) \in \Re^{q \times q};$$

$\mathbf{c}_c = [c_1 \quad c_2 \quad \cdots \quad c_q]^T \in \Re^q$; $\mathbf{A}_c = [\mathbf{a}_1 \quad \mathbf{a}_2 \quad \cdots \quad \mathbf{a}_q]^T \in \Re^{q \times n}$

and $\delta(\cdot)$, DSM, is the minimum element in $\mathbf{d}(\cdot)$

one strategy to compute DSM is

$$\delta(t) = \min_{1 \le i \le q} \delta_i(t) \qquad (6)$$

Safety is one of the important specifications of the controlled system. Safety control problem requires moving the system from a given set of initial states in its state space to a predetermined safe region achieving, in addition, the desired nominal performance of the system. Thus, if the safe region $\mathbf{\Phi} \subseteq \mathbf{X}$ is defined as a set of inequality constraints $\{\phi(\boldsymbol{x}) \le 0\}$, then the controller should move the state in order to satisfy $\delta^*(\cdot) \ge 0$. A positive value of DSM, i.e. $\boldsymbol{d}(\cdot) \ge 0$, means that the nominal performance is achieved. Contrarily, a negative value of DSM $\delta^*(\cdot) \le 0$ means that the system has been exposed to a large disturbance and/or model uncertainties or a fault exists.

3 CONTROLLER DESIGN AND ADAPTING BASED ON DSM

To maintain the system states within a predefined margin of safety, the value of DSM must be considered in the controller design. The controller design based on DSM has the advantage that the system will be maintained within the safety region during the normal operation as well as in case of faults or disturbances. The introduction of DSM into the controller design can be achieved by various methods. The safety region Φ may be considered as a controlled invariant set [19] if there is a controller that assure DSM positive for the closed loop system.

In some cases, it is difficult to satisfy simultaneously $\delta(\cdot) \ge 0$ and a desired nominal performance, in particular if a fault occurred. Therefore, it is necessary to accept some degree of performance degradation after the occurrence of the fault in order to satisfy the safety. Some ideas about implementing DSM in controller design are stated in [15] and [18] .

The DSM value can be used as a performance index to adapt parameters of a certain controller, select a controller among different controllers or combine both methods.

Since, PID controller is one of the most popular controllers, particularly, for SISO systems, adapting PID controller parameters based on DSM is highlighted as an example of controller design based on DSM. For MIMO systems, MPC is successfully used in process control due to its ability to handle explicitly hard constraints on control and states. MPC design based on DSM is addressed as another example for controller design based on DSM for SISO and MIMO systems as well

3.1 Adapting controller parameters based on DSM

DSM can be used as a performance index instead of output error to tune the controller parameters in order to maintain the safety requirements in addition to the output performance. Based on the MIT rule ([20] ,[15]), the controller parameters can be updated by using the following equation:

$$k_i(k) = k_i(k) + \alpha_i \frac{\partial}{\partial k_i} \left| \delta(k+1) \right| \qquad (7)$$

where k_i is the controller parameter number i, α_i is the adaptation parameter, and $\delta(k)$ is the time-discrete form of DSM. This equation can be applied either for $\delta \ge 0$ or $\delta < 0$. In case of $\delta \ge 0$, applying (7) moves the system state far away from the safety boundary. Contrarily, the system state is led to the safety boundary when $\delta < 0$. $\delta(.)$ is a nonlinear and non-differentiable function (c.f. (6)) and it depends on $\mathbf{d}(.)$. Therefore, $\partial\delta(k+1)/\partial k_i$ can be replaced with a function $f_i(\partial\mathbf{d}(k+1)/\partial k_i)$ i.e.

$$k_i(k+1) = k_i(k) + \alpha_i \, f_i\left(\frac{\partial}{\partial k_i}\mathbf{d}(k+1)\right) \qquad (8)$$

If $\mathbf{d}$ has only one negative element, i.e. only one constraint of Φ is violated, then

$$\frac{\partial}{\partial k_i}\delta(k+1) = \frac{\partial}{\partial k_i}\delta_m(k+1). \qquad (9)$$

δ_m is the distance between current state and the violated constraint $m \in \{1,2,q\}$, where q is the total number of constraints.

If more than one constraints are violated, then the infinity norm

$$\frac{\partial}{\partial k_i}\delta(k+1) = \left\| \frac{\partial}{\partial k_i}\mathbf{d}_v(k+1) \right\|_\infty \qquad (10)$$

is used. It corresponds to the maximum effect of k_i on violated constraints and $\mathbf{d}_v \subseteq \mathbf{d}$ is the distances vector between the current state and violated constraints $v \le q$.

3.1.1 Adapting PID controller parameter

The PID controller is one of the popular controllers used in more than 80% of industrial SISO process. It has dominated industrial control for half a century, and there has been a great deal of research interest into the implementation of the advanced controllers. The reason is that the PID control has a simple structure, which is easy to be understood by field engineers, and it is robust to disturbance and system uncertainty [21] .

The control signal $u \in \Re$ at any instant k, using a discreet PID controller, is defined as

$$u(k) = K_P e(k) + K_I \sum_{j=1}^{k} e(j) + K_D \frac{e(k) - e(k-1)}{T} \qquad (11)$$

where K_P, K_I, and K_D are the controller proportional; integral; and derivative gains respectively.

Substituting by the state model and control input equation of PID controller then

$$\mathbf{d}(k+1) = \mathbf{d}_c - \mathbf{D}_a \mathbf{x}(k+1)$$

$$\mathbf{d}(k+1) = \mathbf{d}_c - \mathbf{D}_a(\mathbf{A}\mathbf{x}(k) + \mathbf{b}(K_P e(k) + K_I \sum_{j=1}^{k} e(j) + K_D \frac{e(k) - e(k-1)}{T}))$$

then $\mathbf{d}_v(k+1) = \mathbf{d}_a^v - \mathbf{D}_a^v \mathbf{x}(k+1)$, where $\mathbf{D}_a^v \in \Re^{vxn} \subseteq \mathbf{D}_a \in \Re^{qxn}$ and $\mathbf{d}_a^v \in \Re^{vx1} \subseteq \mathbf{d}_a \in \Re^{qx1}$. The updated parameters are

$$\left.\begin{aligned} k_P(k+1) &= k_P(k) + \alpha_P \left\| (-\mathbf{D}_a^{\nu} \mathbf{b} e(k)) \right\|_{\infty} \\ k_I(k+1) &= k_I(k) + \alpha_I \left\| (-\mathbf{D}_a^{\nu} (\mathbf{b} \sum_{j=1}^{k} e(j))) \right\|_{\infty} \\ k_D(k+1) &= k_D(k) + \alpha_D \left\| (-\mathbf{D}_a^{\nu} (\mathbf{b} \frac{e(k) - e(k-1)}{T})) \right\|_{\infty} \end{aligned}\right\} \quad (12)$$

The initial values of the controller parameters are designed in order to satisfy the output performance in normal operation.

3.2 *Model predictive control Design and adapting*

Model predictive Control (MPC) is a form of control in which the current control action is obtained by solving on-line, at each sampling instance, a finite horizon optimal control problem, using the current state of the plant as the initial state. The internal model is used to obtain prediction of system behavior over the finite horizon ([11] -[13]). The optimization yields an optimal control sequence but only the first control of the sequence is applied to the plant and in the next sampling time, the complete calculation is repeated. This is the main difference from conventional control, which uses a pre-computed control law. It naturally handles the control of multivariable plant and takes into account the information on constraints arising from equipment limitations, safety requirements, etc. The control law of predictive controllers, for a system defined by the state-space model, can be obtained by minimizing the 2-norm measure of the predicted performance [12] given by

$$J = \sum_{i=N_1}^{N} \left\| \hat{\mathbf{e}}(i+k|k) \right\|_{Q_i}^2 + \sum_{i=0}^{N_u-1} \left\| \mathbf{u}(i+k) \right\|_{R_i}^2 \quad (13)$$

subject to

$$\left.\begin{aligned} &\mathbf{x}(k+1) = \mathbf{A}\,\mathbf{x}(k) + \mathbf{B}\,\mathbf{u}(k) \\ &\mathbf{y}(k) = \mathbf{C}\,\mathbf{x}(k) + \mathbf{D}\,\mathbf{u}(k) \\ &\mathbf{x}(k+i|k) \in \mathbf{X}_s \\ &\mathbf{u}_{\min} \le \mathbf{u}(k+i) \le \mathbf{u}_{\max} \end{aligned}\right\} \quad (14)$$

where

$$\underset{\rightarrow}{\mathbf{u}} = [\mathbf{u}(k)\ \mathbf{u}(k+1) \cdots \mathbf{u}(k+N_u-1)]^{\mathrm{T}} \in \Re^{r.N_u},$$

$$\hat{\mathbf{e}}(k+i|k) = \mathbf{y}_d(k+i) - \hat{\mathbf{y}}(k+i|k) \text{ and}$$

$$\|\mathbf{e}\|_Q^2 = \mathbf{e}^{\mathrm{T}} \mathbf{Q}\, \mathbf{e}.$$

$\hat{\mathbf{e}}(k+i|k) \in \Re^m$ is the predicted error between the desired and predicted response. $\mathbf{x} \in \Re^n$ is the system state vector, $\mathbf{y}_d \in \Re^m$ is the reference output vector. $\hat{\mathbf{x}}(k+i|k)$ is the prediction of $\mathbf{x}(k+i)$ made at instance k, $X_s \subseteq X$ is the set of state vectors that satisfies all state constraints. **A**, **B**, **C** and **D** are the system parameter matrices of adequate dimensions. $\mathbf{Q}_i$ are error weighting matrices, $\mathbf{R}_i$ are input weighting matrices. N, N_1 and N_u are the maximum, minimum and control horizons, respectively. Notice that **Q**, **S**, **R**, N, N_1 and N_u are free design parameters.

The design of MPC based on DSM can be handled by replacing X_s by the safety region Φ. Hence, the state constraints can be written in the form

$$\hat{\delta}(k+1|k) \ge 0 \text{ or } \hat{\mathbf{d}}(k+1|k) \ge 0 \quad (15)$$

where $\hat{\delta}(k+1|k) \in \Re$ and $\hat{\mathbf{d}}(k+1|k) \in \Re^q$ are the prediction of DSM and distance vector, between the predicted state and the boundaries of Φ, made at instance k, respectively.

The solution of MPC based and adaptation on DSM are discussed in details in [24] [17] and [25]

Example 1: Consider a state-space model of SISO system defined as

$$\mathbf{x}(t) = \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u(t)$$
$$y(t) = \begin{bmatrix} 1 & 0 \end{bmatrix} \mathbf{x}(t) \quad (16)$$

$u(t) \in [0,5]$. The safe operation region Φ is defined by

$x_1(t)-(x_2(t)+0.5) < 0$; $x_1(t) - x_2(t) > 0$; $x_1 < 4$ and $x_2 < 4$

Figure 2 shows the system (27) response using PID controller with fixed and adapting parameters and state trajectory for step input equal 2. Figure 2-a shows the state responses and trajectories using fixed PID parameters with k_P, k_D and k_I are 4, 1 and 1 respectively. It is shown that the output response, transient and steady state, is accepted while state trajectory lies outside the safe boundaries, i.e. DSM <0 in this period. The state trajectory is forced to be inside the safe region using an adapted PID controller based on DSM as shown Figure 2-b, while the rise time is increased.

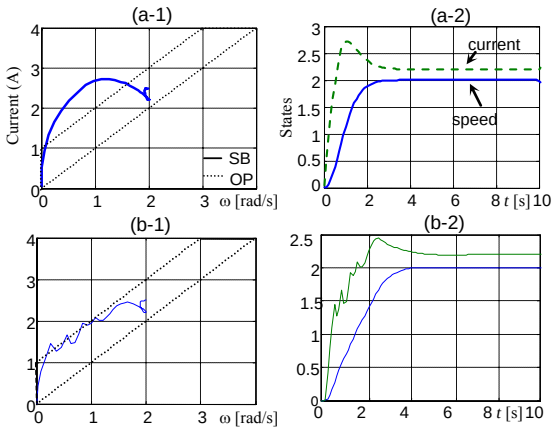


Figure 2: PID response and state trajectory with and without adaptation based on DSM

Although the previous example is a SISO system, it illustrates the effectiveness of each controller design method. Figure 3 shows the response using an MPC. Figure 3a shows MPC response without considering DSM with the following parameters: Q=70, R=0.01, N_1=1, N_u=6, and N= 10.

The response of MPC controller without considering DSM (Figure 3a-2) is accepted w.r.t. the error and rise-time

but the state trajectory lies outside the safe boundaries at transient ((Figure 3a-1)) i.e. DSM is negative. The response is almost the same as in case of fixed parameters PID (Figure 2a-2)). To improve DSM at transient time, the controller should be redesigned according to DSM.

Figure 3b shows the response using MPC with adapted weight based on DSM [25] . The DSM is improved and the response is faster than the adapted PID. The controller parameters are, $\mathbf{Q}_i$=[70], $\mathbf{R}_i$=[0.01], N=10, N_1=1, N_u=6.

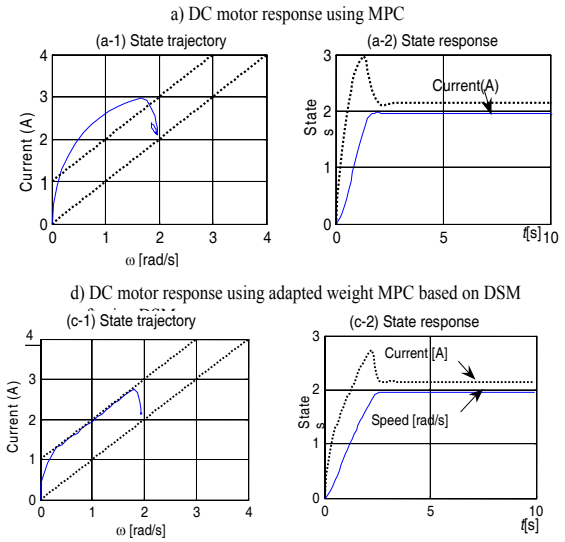


Figure 3: Responses using MPC with and without DSM constraints (SB: Boundary and OP: Trajectory)

4 FTC SYSTEM SCHEME BASED ON DSM

According to the definition of DSM, Controllers design based on DSM constraints satisfy the safety requirements of the system and the accepted degraded performance. In addition, a control system, whose design is based on DSM, can compensate faults when it is difficult or just not possible to find an FDI system that provides full and exact information about the fault. Moreover, not all faults can be anticipated. In such situation, a DSM based FTC system could be very useful to overcome this problem, because controllers based on DSM can maintain a safety operation with acceptable degraded performance even in some cases of unanticipated faults. On the other hand, the proposed FTC system can be applied to active as well as passive FTC.

Three controllers are configured according to the proposed FTC design and used for the following scenarios:

- Under normal operating conditions, a nominal controller is designed to guarantee the system's stability and robust tracking performance in the presence of the modelling uncertainty.
- When a fault occurs, the nominal controller should guarantee the system signal boundary by checking DSM until the fault is detected.
- After a fault is detected (DSM < 0), the nominal controller is replaced by a controller based on DSM using the nominal system model to compensate the effect of the (yet unknown) fault. This controller may recover some control performances (e.g., tracking of reference signals). This new controller should guarantee the boundedness of safety requirements and physical limitation of the components even in the presence of the fault.
- If the fault is isolated, then the controller with DSM is reconfigured again using fault information by selecting the suitable faulty model to improve the control performances.

Remark 1: In the case of PFTC, no FDI system is used, the controller is reconfigured according to the value of DSM. i.e., there are two control configurations; nominal controller and controller based on DSM using the nominal model.

Remark 2: It is possible that, in some cases, the fault that has occurred cannot be isolated, for instance a fault whose functional structure is completely unknown a priori (i.e., does not belong to the fault set). Then, the first fault-tolerant controller guarantees some minimal performance (e.g., closed-loop stability). In this case, the third FTC cannot be activated.

In this approach, the fault is isolated using Multi-model FDI scheme [22] ,[7] , the reconfigurable controller is designed using MPC based on DSM and new faulty model selected according to FDI algorithm information. Figure 5 shows the general structure for the proposed reconfigurable control scheme, which includes a set of reference models, controller using safe region constraints, a Multi-Model FDI system employing parameters and state estimation and a supervisor.

4.1 Multi-reference model and command control block

As mentioned above, the degree of capability of the other system components could significantly be reduced because of a faulty part. If the design objective is to maintain the original system performance, the remaining parts will be forced to work beyond the nominal duty in order to compensate the handicaps caused by the fault. Thus, it is necessary to reduce the overall system performance to an acceptable degraded performance. Moreover, in some faulty situation, the system cannot be able to follow the command input and therefore, it should be changed in order to maintain an adequate system operation. The performance change can be achieved by modifying the objective function of MPC [14] or by selecting a predesigned reference model [7] . A combination of both methods is proposed here. The objective function is changed according to DSM value in order to find a feasible solution of a constrained MPC. The multi-reference and command control block (see Figure 5) is dedicated to select an acceptable degraded performance in case of a specified fault. In case of a specified fault, a new command input is selected in order to maintain the

system availability. More investigation about reference model and command signal is discussed in this section

4.1.1 Degraded reference model design

In FTC dynamic and steady state, performance should be considered as well. The idea of using degraded reference model to satisfy the specified degraded performance is stated in [13].

Assume that the desired closed loop reference model of the system with no fault is represented by

$$\left.\begin{aligned}\dot{\mathbf{x}}(t) &= \mathbf{A}_r\mathbf{x}(t) + \mathbf{B}_r\mathbf{r}(t)\\ \mathbf{y}(t) &= \mathbf{C}_r\mathbf{x}(k) + \mathbf{D}_r\mathbf{r}(t)\end{aligned}\right\} \quad (17)$$

The corresponding transfer function matrix of the desired reference model is then:

$$\mathbf{T}_r(s) = \mathbf{C}_r(s\mathbf{I} - \mathbf{A}_r)^{-1}\mathbf{B}_r + \mathbf{D}_r . \quad (18)$$

Let's assume that the eignvalues of the closed-loop system are represented as

$$\mathbf{\Gamma}_r = diag\left[\lambda_1 \quad \lambda_2 \quad \cdots \quad \lambda_n\right] \quad (19)$$

After a fault has occurred, it is expected that the closed-loop system eignvalues of the degraded reference model will move towards the imaginary boundary of s-plane to reflect the loss of dynamic performance of the system as will as the reduction in stability margin.

Suppose that the eignvalues of the degraded reference model are represented as

$$\mathbf{\Gamma}_d = \Sigma^{-1}\,\mathbf{\Gamma}_r \quad (20)$$

where

$$\mathbf{\Sigma} = diag\left[\beta_1 \quad \beta_2 \quad \cdots \quad \beta_n\right],$$

$$\beta_i \geq 1, \ \forall \quad i = 1,\cdots,n.$$

The transfer function matrix of the reference model of the degraded system then becomes

$$\mathbf{T}_d(s) = \mathbf{C}_d(s\mathbf{I} - \mathbf{A}_d)^{-1}\mathbf{B}_d + \mathbf{D}_d \quad (21)$$

Assume that $\mathbf{A}_d$ is diagonal then

$$\mathbf{A}_d = \Sigma^{-1}\,\mathbf{\Gamma}_r$$

It is important to note that the desired and degraded reference models should have steady-state gain for the purpose of commend input tracing. Therefore,

$$\lim_{s\to 1}\left(\mathbf{C}_d(s\mathbf{I} - \mathbf{A}_d)^{-1}\mathbf{B}_d + \mathbf{D}_d\right) = \lim_{s\to 1}\left(\mathbf{C}_r(s\mathbf{I} - \mathbf{A}_r)^{-1}\mathbf{B}_r + \mathbf{D}_r\right)$$

and

$$\mathbf{C}_d(\mathbf{A}_d)^{-1}\mathbf{B}_d + \mathbf{D}_d = \mathbf{C}_r(\mathbf{A}_r)^{-1}\mathbf{B}_r + \mathbf{D}_r$$

If it is assumed that $\mathbf{C}_d$=$\mathbf{C}_r$ and $\mathbf{D}_d$=$\mathbf{D}_r$, then

$$\mathbf{B}_d = \mathbf{\Sigma}^{-1}\mathbf{\Gamma}_r\mathbf{A}_r^{-1}\mathbf{B}_r \quad (22)$$

Hence the degraded reference model can be represented as

$$\left.\begin{aligned}\dot{\mathbf{x}}(t) &= \mathbf{A}_d\mathbf{x}(t) + \mathbf{B}_d\mathbf{u}(t)\\ \mathbf{y}(t) &= \mathbf{C}_d\mathbf{x}(t) + \mathbf{D}_d\mathbf{u}(t)\end{aligned}\right\}$$

4.1.2 Command input control

In some faulty situations, the system cannot follow the command input and therefore, it should be changed in order to maintain system availability. A set of different command input for different fault modes can be previously designed and selected on line based on the detected fault. To avoid the transient effect due to the switching between the pre-fault and post fault command input, it is important to change the command input gradually (smooth change). Thus, based on smooth command input switching described in [7] , the following modified command input $\mathbf{r}_m$ will be generated based on the selected command input $\mathbf{r}$ as

$$\mathbf{r}_m(k) = \mathbf{r}_m(k-1) + (1-\mu\, e^{-\tau(k-k_D)})(\mathbf{r}(k) - \mathbf{r}_m(k-1)), \qquad k \geq k_D$$

where

$$\mathbf{r}(k) = \begin{cases}\mathbf{r}_n(k) & k < k_D\\ \mathbf{r}_f(k) & k \geq k_D\end{cases} \quad (23)$$

and $\mu\,(0 \leq \mu \leq 1)$ and $\tau > 0$

are designed parameters to provide smooth switching between $\mathbf{r}_n$ and $\mathbf{r}_f$; $\mathbf{r}_n$ and $\mathbf{r}_f$ are the command inputs before and after the fault detection. For large k, $\mathbf{r}_m \to \mathbf{r}_f$. In fact, the command input $\mathbf{r}_m(k)$ is an interpolation between $\mathbf{r}(k)$ and $\mathbf{r}_m(k\text{-}1)$.

Special case

In some situations, it is difficult to find controller parameters, which can track the command input and achieve and the safety performance in addition to the stability. If the highest priority is given to the safety i.e. DSM should be positive, then the DSM index is used to determine the new command input as follows:

When the DSM is negative, at each instant there exists at least one constraint from the constraints set of safe region is violated. In this case, DSM is the distance between the current state and the nearest boundary constraint to the current state, i.e.

$$\left|\delta(k)\right| = \left|\delta_i(k)\right| = \left\|v_{io} - \mathbf{x}(k)\right\|_2 \quad (24)$$

Assume that the violated constraint number $i \in \{1,2,\ldots,q\}$ is taken as the reference target to the system, and assume that D=0, then the new command will be

$$\mathbf{r}_c(k) = \mathbf{C}v_{io} \quad (25)$$

where

$$v_{io} = arg\left(\min_{\mathbf{v}_i}\left\|(\mathbf{x} - v_i)\right\|_2^2\right)$$

subject to

$$\mathbf{v}_i \in \left\{\mathbf{v}\middle|\phi_i(\mathbf{v}) = 0\right\}$$

and ϕ_i is the nearest violated boundary constraint.

For a SISO system and linear safety constraints, the command input can be calculated by another way without solving (4.41). The DSM can be defined for the violated constraint i according to (2.12) as

$$\delta_i(k) = c_{1i} - \mathbf{a}_{1i}^T \mathbf{x}(k) \qquad (26)$$

each vector a1i can be written as

$$\mathbf{a}_{1i}^T = \mathbf{c} + \mathbf{c}_{is}$$

then

$$\delta_i(k) = c_{1i} - (\mathbf{c} + \mathbf{c}_{is})\mathbf{x}(k)$$
$$= r_c - y(k)$$

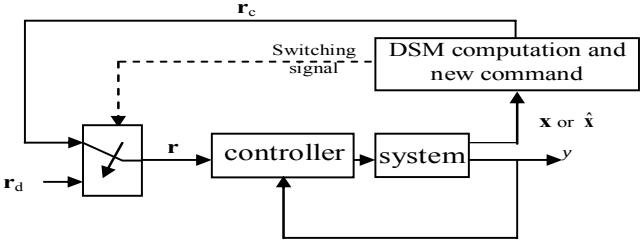
Therefore,

$$r_c(k) = c_i - \mathbf{c}_{is}\mathbf{x}(k) \qquad (27)$$

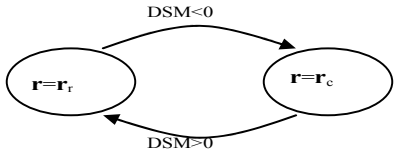
where $r_c(k)$ is the new reference which depends on the current state of the system, y is the output, $\mathbf{a}_{1i}^T \in \Re n$ and $c_{1i} \in \Re$.

It is clear that the reference is changed or adapted based on the system state location with respect to the safe region until the state reaches the safe region.

Figure 4-1 shows the block diagram of command input selection and adjusting based on DSM.



a) Block diagram of system with different command input



b) Supervisor automata

Figure 4-1: Block diagram of command input selection based on DSM

4.2 Controller employing DSM block

MPC with constraints provides a suitable architecture for the implementation of fault tolerant control systems, as it was stated before. The degraded accepted performance is obtained using MPC by changing the objective function or by using a multi-objective function. Therefore, the MPC with DSM constraints is used as a reconfigurable controller in the proposed scheme. According to the definition of DSM, MPC based on DSM constraints satisfies the safety requirements of the system and the accepted degraded performance. In most faulty system, the information from FDI is not accurate and sufficient to complete the fault description. Hence, an MPC complemented by DSM will insure a safe operation of the system and can compensate the missed information about the fault and uncertainties in the faulty model. The DSM index is used to specify the priority of the constraints that can be relaxed in order to find a feasible solution and to change the objective function parameters (weights).

4.3 Multi-model FDI and state and/or parameter estimation

Most of the model based fault diagnosis systems in the literature compare either the actual signals or the identified system parameters, according to the fault type, with the estimated from faulty models to generate the residual ([23]). The design of a residual generation system, which is insensitive to model parameter variations and external disturbances, is a very difficult task and it is called a robust FDI system. In [17] , it is explained, how DSM can be helpful in designing a robust FDI system. A complete analysis of the approach in [16] is discussed in more details in [26] This method for fault isolation depends on the generation of DSM from a set of models of the system under consideration defined as $M = \{M_0, M_1, \ldots, M_z\}$ (analytical redundancy of DSM) and compares the generated DSM with the actual value calculated from the measured state. Each one of these models simulates one fault of the faults set, which should be isolated in addition to the nominal fault free model. Multi-model FDI systems were addressed in different work (see for example [22] ,[23] and [7]). The main difference between [26] and the other works is the use of DSM in the comparison between the faulty model and the actual model instead of the state directly. The model is described in general as

$$M_i \begin{cases} \mathbf{x}_i(k+1) = \mathbf{G}_i(\boldsymbol{\theta}_i, \mathbf{x}_i(k), \mathbf{u}(k), \mathbf{f}(k)) \\ \mathbf{y}_i(k) = \mathbf{C}\mathbf{x}_i(k) \end{cases} ; i=0,1,...,z \quad (28)$$

where $\mathbf{x}_i \in \Re^n$ is the state vector of the system model i, $\mathbf{u} \in \Re^m$ the input vector; $\mathbf{y}_i \in \Re^p$ output vector; $\mathbf{f} \in \Re^l$ unknown additive fault signal vector, $\mathbf{G}_i$ is a mapping $\mathbf{G}_i: \Re^n \times \Re^m \times \Re^l \rightarrow \Re^n$, $\boldsymbol{\theta}_i$ system parameters for faulty model I, $\mathbf{C} \in \Re^{n \times p}$ constant matrix; and z number of anticipated fault. $i = 0$ means fault free case, nominal model.

The fault diagnosis and isolation subsystem is activated when $\delta(t) < 0$ and/or $d\delta(t)/dt < 0$. $d\delta(t)/dt < 0$ means that the state trajectory moves in the direction of unsafe operation. In general, faults can be divided into two types: additive faults, which can be simulated as an unknown external signal, and multiplicative faults, which represent the change in the parameters of the system. In both cases, it is necessary to estimate the unknown external input or new system

parameters, according to the fault type, in order to obtain information about the fault. Therefore, parameters and state estimation are considered as a subsection of the FDI system. The output of this block is the estimated state and faulty model parameters, which are submitted to the MPC block. It also sends a status signal to the supervisory block.

4.4 Supervisory block

Based on the results of FDI block, the fault information can be positive or negative. Positive information means that one of the faulty models can describe the fault. Negative information signifies that it is difficult to represent the fault by one model of the set. Thus, positive information is treated according to the scenario of fault recovery described before and the reference model and command signal can be selected easily according to the history of the system operation and the operation experience. Contrarily, negative information is not easy to be handled and therefore the supervisory controller should select the command input as well as the reference model and/or reconfigure the system in order to maintain the system availability. The supervisor receives the data γ from the FDI block, which contains fault type, output performance index and DSM value and it sends the signal ν to FDI in order to select the new model, which has to be used in the MPC. DSM plays an important role in supervisory control. It can be considered as a safety index for the recovery control performance, which is described by MPC. It is used to adapt the command input signal and to configure the reference models.

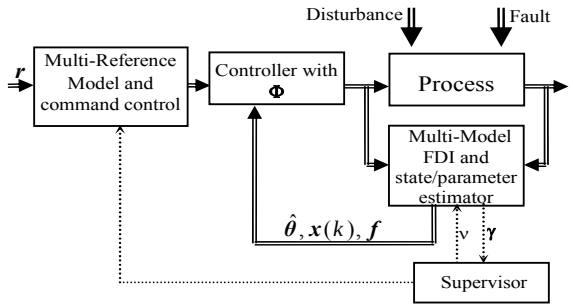


Figure 5: Overall structure of proposed FTC system

VI EXPERIMENTAL RESULTS

The above algorithms are tested in real-time operation on an experimental laboratory process described in [16] . The process, shown in Figure 3, consists of two-tanks 100l filling a sink tank 300l. Each tank has a control valve at the output line in order to control its level. In the current experiment the interconnecting valve was fully opened, the leakage valve (control valve of 2nd tank) was adjusted manually to simulate the leakage and the valve, of the left tank, was used to control the level. The two-tank system was fed at constant flow of 1 l/s in the first tank. The output h is the level in the tank [m] and the input is the valve opening.

Consider that the variables relevant to system safety are the tank level rate (dh/dt) and v_i [m], the valve limb movement, which simulates the valve opening. The safe operation region $\mathbf{\Phi}$ is given by:

$$dh/dt + 0.8\ \text{vi} - 0.08 < 0;\ dh/dt + 0.75\ v_i + 0.14 > 0;$$
$$-0.4 < dh/dt < 0.4;\ -0.5 < v_i < 0.5, \qquad (35)$$

where the valve opening is normalized within [-0.5, 0.5] i.e. 0.5 means fully opened and -0.5 completely closed. The level rate change (dh/dt) is in [mm/s].

Note that, firstly the state vector $\mathbf{x}= [h_1\ h_2\ v_i]$T in case of two tank system and $\mathbf{x}= [h_1\ v_i]$T in case of one tank system; secondary one of the safety variable is $dh/dt = f(\mathbf{x})$ not the state directly and $f:\Re^n \rightarrow \Re$ is a nonlinear function of $\mathbf{x}$ therefore dh/dt is taken as an independent variable which can be easily computed from h_1 in order to have a linear constraints.

The input flow is not fixed at 1 l/s but it varies within [0.92 1.05] l/s. Therefore, there are uncertainties in the linearized model parameters. In addition, the cross section areas of the tanks are not constant, but it varies with the level height.

The proposed FTC approach, discussed in the previous section, is implemented on the experimental setup in case of actuator fault. A model predictive controller, corresponding to Section 3, is used with and without DSM to regulate the level of the left tank at the set point of 0.3 m in case of actuator fault. Figure 4 shows real-time results of the above FTC algorithm for the two-tank system in case of bias fault of 20% in the control valve from 320s until 480s (fault scenario). Three controllers are used: MPC without DSM in normal operation until DSM<0 (0-370s), MPC with DSM constraints when DSM<0 until fault diagnosis (370s-400s), and MPC with DSM using faulty model (actuator fault model) after fault diagnosis (after 400s). The recovery time is short, the steady state error is small, and DSM is almost zero after the fault detection.

5 CONCLUSIONS

A new performance index called DSM is introduced. The controller design based on DSM improves safety-assessment of safety-critical systems. Design MPC and adapting PID controlled parameters based on DSM are introduced in this work. Simulation results demonstrates the advantage of adapting PID and MPC design based on DSM in order to improve system safety during transient. FDI and control design based on DSM are employed together in order to design a reliable FTC scheme based on DSM. The proposed FTC can compensate the effect of error in FDI subsystem, and can maintain the system output performance and stability within an acceptable rage until the fault is isolated for some fault set. Results of a real-time implementation on a two-tank process demonstrate the advantage of the proposed approach of FTC. There are some open topics in applying this approach, which should be covered in the future: For example, safe region determination methods and DSM measuring for large-scale system. Hence, all these topics will be undertaken in the future work as well as the problem of applying DSM to fault prognosis.

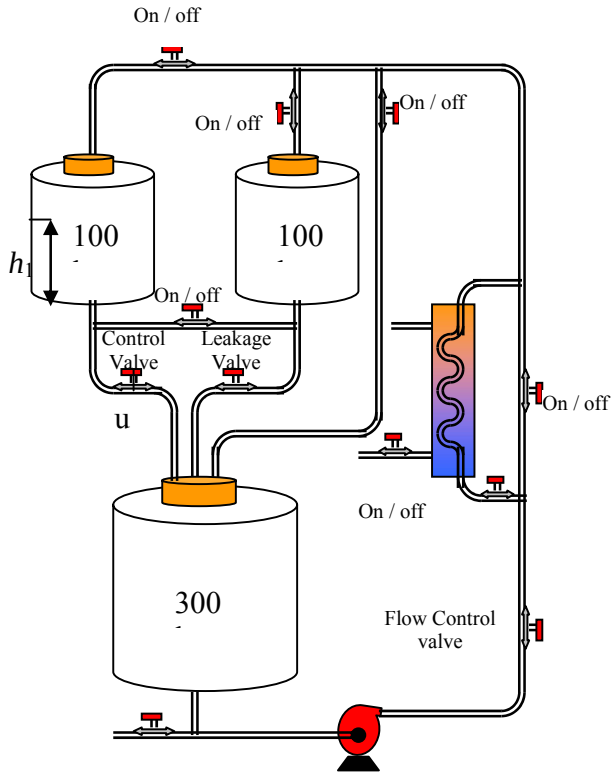


Figure 3: Schematic diagram of Two Tank system

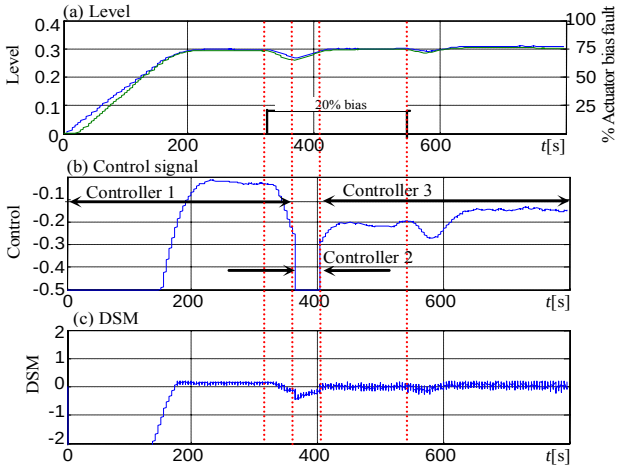


Figure 4: FTC response using three controllers

REFERENCES

[1] S. Persin, B. Tovarnik, N. Murkinja, and D. Vohl, "Increasing Process Safety using Analytical Redandancy", Electrotehniski vestnik, vol 69, No. 3-4, pp. 240-246, 2002.

[2] Morgens Blanke, "Enhanced Martine Safety through Diagnostic and Fault Tolerant Control", IFAC Proc. conference CAMS' 2001, UK. July 2001.

[3] Zaxin Diao and Kevin M. Passino, "Stable Fault-Tolerant Adaptive Fuzzy/Neural Control for Turbine Engine", IEEE Transaction on Control System Technology, Vol. 9, No. 3, May 2001.

[4] H. Noura, D Sauter, F. Hamelin, and D. Theilliol, "Fault Tollerant control in Dynamic System", IEEE Control System Magazine, PP. 33-49, February 2000.

[5] M. Blanke, M. Staroswieki and N. Eva Wu, "Concept and methods in fault-tolerant control", *Tutorial at American Control Conference*, June, 2000.

[6] M. Mahmoud, J. Jiang, and Y. Zhang, "*Active Fault Tolerant Control System.*" *Lecture Notes in Control and information Sciences*", Springer, 2003.

[7] Y. Zhang and J. Jiang, "Fault tolerant control system design with explicit consideration of performance degradation". *IEEE Trans. in Aerospace and electronic system*, vol. 39, June 2003.

[8] G.A. Murad, I. Posthethwaite, and D.W. Gu, "A Robust Design Approach to Integrated Control and Diagnostics", in proc. 13th IFAC Word Congress, San Francisco, CA, 1996, pp. 199-204.

[9] D. Sauter, F. Hamelin, and H. Noura, "Fault Tolerant Control in Dynamic System Using Convex Optimization", in Proc. IEEE ISIC/CIRA/ISAS Joint Conf.,Gaithersburg, MD, 1998, pp. 187-192

[10] G. Simon, G. Karsai, G. Biswas, s. Abdelwahed,N. Mahadevan, T. Szemeth, G. Peceli and T. Kovacshaz, "Model-Based fault-Adaptive control of Complex dynamic system", IMTC 2003- International and measurement Technology Conference, pp. 20-22, Vail, Co, USA, May 2003.

[11] J.A Rossiter, "Model-Based Predictive Control: Practical Approach", CRC, 2003.

[12] J.M. Maciejowski, "Predictive Control with Constrained", Prentice Hall, 2001.

[13] D. Q. Mayne, J. B. Rawlings, C. V. Rao and Po. M. Scokaert, "Constrained model predictive control: Stability and optimality", Automatica, 36, pp 789-814, 2000.

[14] J. M. Maciejowskiand C.N. jones, "MPC fault-tolerant flight control case study: Flight 1862". IFAC Safe Process Conference, Washington DC, pp 9-11, June 2003

[15] E. Badreddin and M. Abdel-Geliel. "Dynamic safety margin principle and application in control of safety critical system" IEEE International Conference of Control Application (CCA 2004) Conference, September 2-4, 2004, Taiwan. pp 689-695

[16] M. Abdel-Geliel and E. Badreddin, "Adaptive controller using dynamic safety margin for hybrid laboratory plant". Accepted to be presented in American Control Conference 2005, Portland, Oregon, USA.

[17] M. Abdel-Geliel, E. Badreddin and A. Gambier, "Dynamic safety margin in fault tolerant model predictive controller". IEEE International Conference of Control *Application* (CCA 2005), September, 2005, Canada.

[18] M. Abdel-Geliel and E. Badreddin, "Dynamic safety margin in fault diagnosis and isolation". *Accepted to be presented in European Safety and Reliability (ESREL) conference,* June 27-30, 2005, Tri city Poland.

[19] F. Blanchini, "Set invariance in control", Automatica, Vol. 35, pp. 1747-1767, 1999.

[20] Karl J. Astrom and B. Wittenmark, " Adaptive Control",2nd Edition, Addison-wesley, 1995.

[21] Ding-Li Yu; T. K. Chang and Ding-Wen Yu "Fault tolerant control of multivariable processes using auto-tuning PID controller" IEEE Tran. Man, and Cybernetics, PartB: cybernetics, Vol. 35, no. 1: 32-43, Feb. 2005.

[22] Y. Zhang and X Z. Rong Li, "Detection and Diagnosis of sensor and Actuator failures Using IMM Estimator", *IEEE Tran. In Aerospace and electronic system*, vol 34, no 4, 1998

[23] J. Patton, P. Frank, R. Clark, *Issues of Fault Diagnosis for Dynamic System*, Springer, 2000

[24] M. Abdel-Geliel, E. Badreddin and A. Gambier, "Application of model predictive control for fault tolerant system using dynamic safety margin," in Proc. American Control Conf., Minneapolis, Minnesota, USA, June 2006, pp. 5493-5498.

[25] M. Abdel-Geliel, A. Gambier and E. Badreddin, "Adaptive model predictive control based on dynamic safety margin for fault tolerant system," in Proc. 6th Asian Control Conf., Bali, Indonesia, July 2006, pp. 375-383.

[26] M. Abdel-Geliel, E. Badreddin and A. Gambier, "Robust fault detection based on dynamic safety margin," in Proc. 6th Asian Control Conf., Bali, Indonesia, July 2006, pp. 367-374.