Proceedings of the 2004 IEEE
International Conference on Control Applications
Taipei, Taiwan, September 2-4, 2004

Dynamic Safety Margin Principle and Application in Control of Safety Critical Systems

E. Badreddin and M. Abdel-geliel
badreddin@ti.uni-mannheim.de , elgeliel@ti.uni-mannheim.de
Automation Laboratory, University of Mannheim, Germany

Abstract— **Control systems are designed in general to meet a given performance requirement. 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 especially important for safety-critical systems to maintain a predefined margin of safety during the transient and in the presence of large disturbances. In this paper, the idea of DSM is explained and applied in controller design for fluid level in two-tank system. Simulation examples and results of a real-time implementation on the actual process demonstrate the fruitfulness of this design.**

Keywords: DSM, Performance index, safety boundary, safety-critical systems

I. INTRODUCTION

The main goal of control system design is to achieve a desired performance of the controlled system, which can be specified e.g. according to the stability, rise and settling times or a general norm of the controlled variable. The evaluation of the control system depends mainly on a comparison between the desired performance and the actual performance. The selection of the controller also depends on the available information (quantitative or qualitative) about the controlled system. A quantitative controller is based on the accurate model of the system (model based), while the qualitative controller depends on the information of the system behaviour (knowledge based) in case that a system model is not available or difficult to obtain [1].

In this contribution, we propose a new performance index for the control system design, which we call "Dynamic Safety Margin" (DSM). This index could also be considered as an additional term in a more general cost functional. This index measures how far is the system trajectory to a predefined safety boundary in the state space at any time and answers the following questions:

Does the system operate in a safe area all the time even during the transient phase? If so, how far is the current state from a predefined safety boundary? Hence, if we can measure the DSM of the controlled system, we can take it as a measure for the quality of the controller in this respect. We call it dynamic because the magnitude of DSM changes with time as the system trajectory evolves in the state.

Safety margin-based design, of any controlled system, is a signal based method and the boundary of the safe operation area is determined according to the amount of experience about the controlled process.

Designing a controller based on DSM is important to maintain a predefined margin of safety during transient and disturbance actions. Moreover it can help speeding up performance recovery in some cases of system faults. These are some of the applications of DSM, which will be discussed in this work.

Most of the work related to system safety use fault diagnostic 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 [2]-[6]. A fault is any kind of malfunction or degradation in the plant that can lead to a performance reduction or loss of important functions, impairing safety. 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 [7]-[10]. There are many methods of performance recovery in the literature [4],[6],[10] and all of them depend on the diagnostic of the system and readjustment of the plant controller.

According to our best knowledge, the idea of defining a "Dynamic safety margin" and its application to improve the system performance has not been reported in literature and it constitutes the main contribution of this paper. There is an alternative concept that is close to DSM stated in [5] called on line safety control. In [5] the authors try to define all safe states (safe region) of the system, explore the nearest safe states to the current states up to a specified depth and design a supervisor that can drive the system from the current states to safe states in a finite time using a finite sequence of inputs. This approach is conceptually similar to the model predictive control approach [11] in which a limited time forecast of the process behaviour at each state is optimized according to given criteria.

However, there are significant differences between the approach described in [5] and the DSM approach introduced here. These differences will become clear later.

Controller design based on DSM can be implemented as an optimal control problem with special constrains but in this case the system model and safety boundary model must

be well known. A variable structure supervisory controller can use the DSM value to switch between different controllers in order to increase operation safety. DSM can be introduced in the control design in several other forms some of which are stated in this work.

We shall illustrate the idea and its implementation through few examples in section 2. The importance of determining the DSM and its application "mainly in improving safety during the transient phase, disturbance suppression, and speeding up performance recovery in case of faults" are discussed in section 3. Experimental results of applying DSM are discussed in section 4. Conclusions and future work are discussed in the last section.

II. DYNAMIC SAFETY MARGIN (DSM)

To explain the idea of Dynamic Safety Margin (DSM), let's consider a "fictive" boiler which is designed to withstand a certain pressure and temperature (Fig.1). The safe operation region $\Phi \subseteq X$ can be given by $\phi(x_1, x_2) < 0$ [1] while $\phi(x_1, x_2) > 0$ indicates unsafe operation. We shall further assume that the system is stable -in the sense of Lyapunov- with its stability region fully contained in the safe region. Starting with the initial condition $\mathbf{x_o}$, the system trajectory will evolve to the operating point **a** traversing the state space with varying distance to the safety boundary. DSM in this case is defined as the shortest distance, $\delta(t)$, between the fluid state of interest, e.g., pressure $x_1(t)$ and temperature $x_2(t)$, and a predefined boundary $\phi(x_1, x_2)=0$ in this subspace of the state variables. At the operating point $d\delta(t)/dt=0$ and $\delta(.)$ reaches a constant value indicating the Stationary Safety Margin (SSM). Most –industrial- designs are made to satisfy SSM of specified values. However, systems, very often, fail in the transient phase which emphasis the importance of the DSM. In addition, the rate of change $d\delta(t)/dt$ of DSM can be used to predict possible system failure.

In other words, if the system state variables (Temperature, Pressure) at time t are $(x_1(t),x_2(t))$ then the DSM at this time will be the minimum distance between the current states and safety boundary $\phi(x_1, x_2)$ according to the following equation.

$$\delta(t) = s(t) \cdot \left\| \phi(x_1, x_2) - (x_1(t), x_2(t)) \right\|_{\min} \qquad (1)$$

Where $s(t)=$ +1 for **x inside** the safe operation region; -1 for **x outside** the safe operation region

$\|\cdot\|_{\min} \triangleq$ shortest distance from **x**(t) to ϕ

$$\Phi = \{\phi_i(x) < 0 | i = 1,..., k\} \qquad (2)$$

[1] $\phi(x_1, x_2) < 0$ represents an open safe-operation region, i.e. the boiler is assumed not to "implode" at very low pressures and will not "freeze" at very low temperatures.

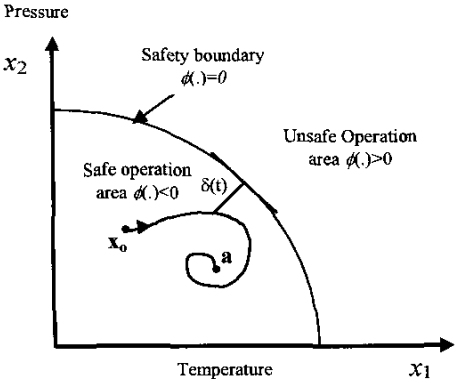


Fig. 1 Safety margin and DSM for a fictive boiler

and DSM is given by

$$\delta^*(t) = \min_i \{\delta_i(t)\} \qquad (3)$$

$$\delta_i(t) = s(t) \cdot \left\| \phi_i(\mathbf{x}) - \mathbf{x} \right\|_{\min}, \mathbf{x} = (x_1, x_2, ..., x_m)$$

where k is the number of defined inequalities and m the number of state variables relevant to safety. Notice that m ≤ n the dimension of the state-space.

I.e. DSM: is the minimization of the minimization of the function $\delta_i(t)$.

If Φ is convex LMI (linear matrix inequalities) can be applied to solve the optimization problem to determine $\delta^*(t)$.

The following simple example should further illustrate the DSM concept.

Example 1

The state space model of a separately exited dc motor (Fig. 2a) is given by

$$\dot{\mathbf{x}} = \begin{bmatrix} \frac{-f}{J} & \frac{k_t}{J} \\ \frac{-k_t}{L} & \frac{-R}{L} \end{bmatrix} \mathbf{x} + \begin{bmatrix} 0 & \frac{-f}{J} \\ \frac{1}{L} & 0 \end{bmatrix} \mathbf{u}$$
$$y = \begin{bmatrix} 1 & 0 \end{bmatrix} \mathbf{x} \qquad (4)$$

where $\mathbf{x} = \begin{bmatrix} w \\ i \end{bmatrix}$; $\mathbf{u} = \begin{bmatrix} v_i \\ T_l \end{bmatrix}$

w is the motor speed (angular velocity), i armature current, f friction coefficient of the motor, J moment of inertia, k_t torque constant of the motor, L Motor armature inductance, R Motor armature resistance, v_i input voltage and T_l load torque

At steady state the relation between armature current and motor speed will be

$$i=(w*f+T_l)/k_t \qquad (5)$$

If we assumed that

1- The safety state variables are speed and current;
2- For simplicity all motor parameters (R, L, ...) are unity;
3- The maximum speed is 3 rad/s and armature current 3 A;
4- The load torque varies from 0 to 0.5 Nm.

In other words, Φ, the safe operation region is given by:

$i-(w*f+0.5)/k_t<0$

$i-w*f/k_t>0$

$i<4$ and $w<4$

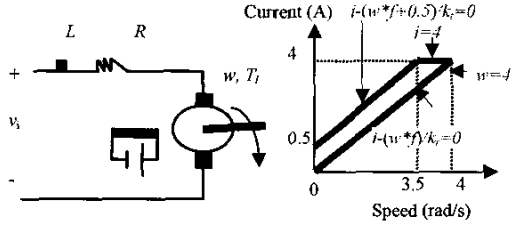
This region is depicted in Fig. 2b. In this example, Φ is defined in the first quadrant only for simplicity.

The open loop response of this motor and DSM variations for a step input of 4v are shown in Fig. 3. Note that d1, d2, d3 and d4 are the minimum distances between motor trajectory and safety region boundaries (b1, b2, b3 and b4). It is clear that DSM at any time t is the minimum value of d_i for i=1,...,4.

At this point we can discuss the differences between the DSM approach and the approach described in [5]:

1. The approach in [5] defines the safe values of each state individually while DSM relies on the definition of a safe operating region in subspace of the state-space.
2. In [5], it's necessary to explore all combination of safe states to find the nearest safe state employing a specified tree depth. The computation complexity can, therefore, become prohibitively high for large trees particularly in real time implementation.
3. The distance between current states and safe states is defined as

D = 0 if $\mathbf{x} \in X_s$ and D>0 if $\mathbf{x} \notin X_s$



a) Separately excited dc motor b) Safety region of the dc motor

Fig. 2 DC motor and safety operation region

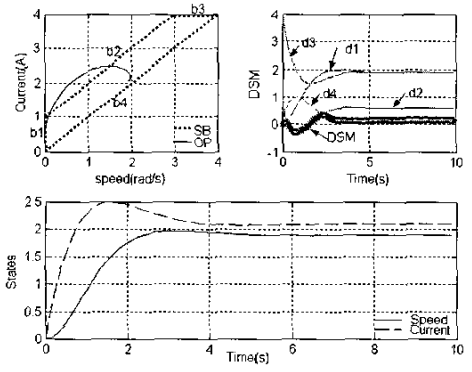


Fig. 3 Open loop response of the dc motor
SB : safety boundary
OP : system trajectory

Where x is the current state vector, and X_s all safe state vectors. This means that system behaviour inside the safe region is not taken into consideration. On the other hand, DSM has a positive value inside safe region and otherwise negative. The value of DSM indicates, therefore, the safety state more precisely.

III. DSM APPLICATION

DSM is an indication to system safety. Hence, controller design based on DSM is important for safety-critical system to maintain a predefined margin of safety during transient and in the presence of large disturbance. Also it is useful in fault diagnostics, system performance recovery and controller evaluation.

The benefits of employing DSM will be clear in the response of the dc motor (example 1). The block diagram of the motor with PID controller employing analogical gates [12] for anti-reset wind-up is shown in Fig. 4, where the input voltage to the motor is limited to ±5 V. The Strategy of employing analogical gates for anti-reset wind-up is implemented using a single analogical-gate namely the XOR-gate as follows:

$$K_i = K_{io}[((u-u_o)/u_o) \oplus (u/u_o)] \qquad (6)$$

where K_i and K_{io} are the current and the initial integral-gain respectively. The unsaturated and saturated control commends are u_o and u respectively.

Fig. 5 shows the motor speed response and DSM variation of the motor for step reference speed of 2 rad/s using PID controller with tuned parameter K_p=4, K_i=2 and K_d=2 and load torque 0.2 N.m. Note that the transient and steady state response of the motor speed is satisfactory but, the motor state trajectory lies in the transient period outside the safe operation region (DSM negative). In order to improve the DSM during the transient period the PID controller parameter must be retuned. There is no a systematic way to retune the controller to improve DSM rather than trial and error tuning procedure. Thus, to handle this problem the controller must be redesigned.

In the next section we shall explain how we can apply DSM to improve the system performance during transient and in steady state, in the presence of disturbance and as "faults" occur.

A. Effect of DSM design during transients and in the presence of disturbances and faults

Consider that the motor was suddenly exposed to a load torque disturbance from 0.2 to 0.5 Nm after 10s from the motor start. Three controller including DSM action are tested in this section.

1)*Multi-controller with supervisor*: Fig. 6 shows the block diagram of dc motor with two PID controllers (with different parameter) and switching controller between them. If DSM is positive then the switch moves toward PID1 and the input to the controller is the error. Otherwise

it moves to PID2 as shown in the supervisor automata in Fig. 6b. The input to the second controller (PID2) is the DSM and it is not necessary in this case to follow the reference but the priority is given to improving DSM. Figure 7 shows the dc motor response using switching controller. Note that DSM is improved in the transient period and the disturbance effect is decreased.

2)*Optimal control*: Optimal control can be used to improve system performance and DSM. In this case, the control problem can be solved as a linear quadratic tracking problem (LQT) [13] to find state feedback gain. The objective functional will be:

$$J = \sum_{k=0}^{\infty} \mathbf{u}(k)^T R\, \mathbf{u}(k) + \mathbf{e}(k)^T Q\, \mathbf{e}(k) + d(k)^T P\, d(k)$$

$$= \sum_{k=0}^{\infty} \mathbf{u}(k)^T R\, u(k) + [\mathbf{e}(k)\ \mathbf{d}(k)]^T \begin{bmatrix} Q & 0 \\ 0 & P \end{bmatrix} \begin{bmatrix} \mathbf{e}(k) \\ \mathbf{d}(k) \end{bmatrix} \quad (7)$$

subject to

$$\mathbf{x}(k+1) = A\,\mathbf{x}(k) + B\,\mathbf{u}(k)$$

$$\mathbf{y}(k) = C\,\mathbf{x}(k)$$

$$\mathbf{d}(k) = [\delta_1(k)\ \delta_2(k) \cdots \delta q(k)]^T$$

$$\mathbf{e}(k) = \mathbf{y}_d(k) - \mathbf{y}(k)$$

$$\delta(k) = \min_{1 \le i \le q}(\delta_i(k))$$

here $\delta_i(k)$ is the minimum distance to each boundary of the safety operation region Φ (equation 2), $\delta(k)$ is the DSM at instance k, i number of inequality constrains, u the control signal vector, **e** the error vector between actual response and desired response and Q,P,R the weighting matrices.

The control low will be

$\mathbf{u}(k) = \mathbf{r}(k) - \mathbf{k}_f^* \mathbf{x}(k)$

where $\mathbf{k}_f$ is the state feedback gain and **r** is the reference inputs.

Fig. 8 shows the dc motor response and DSM variations using optimization algorithm with the following parameters:

$R = [2],\quad Q = [11.5],\quad P = \mathbf{I},\quad \mathbf{k}_f = [0.457\ 0.5739],$

Note that the DSM values are positive for the whole operation period, i.e. the motor operates safely.

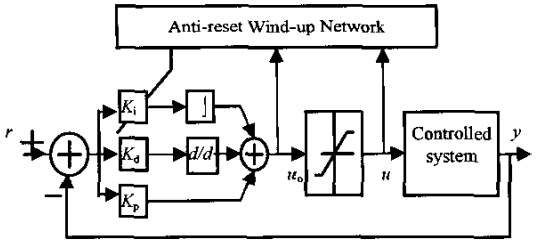


Fig. 4 PID-controller with saturation empoying Analogical-gates for anti-rest wind-up

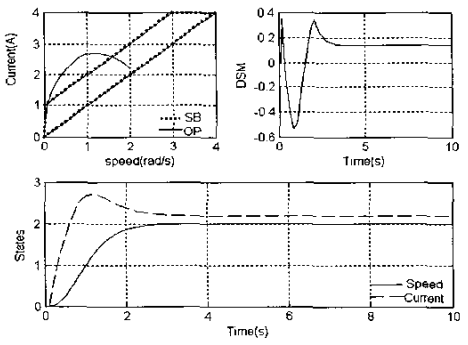
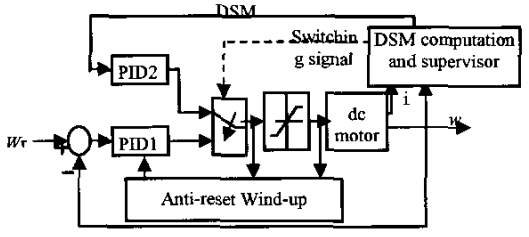
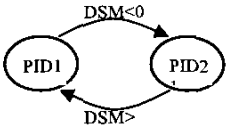


Fig. 5 dc Motor response and DSM variation using fixed parameter PID-controller



a) Block diagram of switching controller



b) Supervisor automata

Fig. 6 Block diagram of dc motor with two controller and supervisor

3) Adapted PID controller: If the controller parameters are defined as a function of DSM, they will be adapted online according to DSM value. We adapt the proportional gain of PID according to the value of DSM and the adapted value is calculated from the following equations

$$K_p(k+1) = K_o * K_g(k+1)$$

$$K_g(k+1) = K_g(k) + \alpha * DSM(k) \quad (8)$$

Where α is the adaptation factor, $K_p(k)$ the proportional gain at any instance k, K_o the nominal value of proportional gain and K_g the adapted gain.

The complete block diagram of the adapted proportional gain of PID controller with anti-reset wind-up network is shown in Fig. 9. Fig. 10 shows the dc motor response using adapted proportional gain. It is clear that the transient and DSM are improved and the torque disturbance effect is reduced.

The different responses of the dc motor show that the system operates in safe mode at transient as well as at steady state and/or system disturbance when DSM is considered in the controller design. Thus, using DSM in adapting controller parameters helps speeding up performance recovery due to disturbances or some faults..

B. Implementation of DSM for System Performance Recovery

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 [6],[8],[10]. Most of the methods, used to performance recovery, depend on the diagnostic of the plant and readjust the controller. Online controller adapting based on the value of DSM helps speeding up the performance recovery close to the nominal performance before the diagnostic of the system has been completed or changes in the model parameters are identified. Adapted PID controller based on DSM is tested in the next section to recover level performance of two-tank system close to the nominal performance due to tank leakage. The experimental results in the next section illustrate the effect of DSM in speeding up performance recovery.

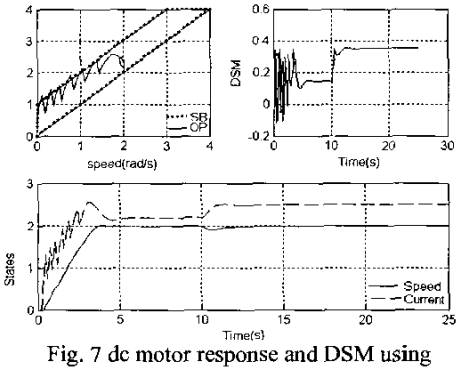


Fig. 7 dc motor response and DSM using switching controller
PID1: K_p=4; K_i=1; K_d=1.1
PID2: K_p=2; K_i=2; K_d=2.0

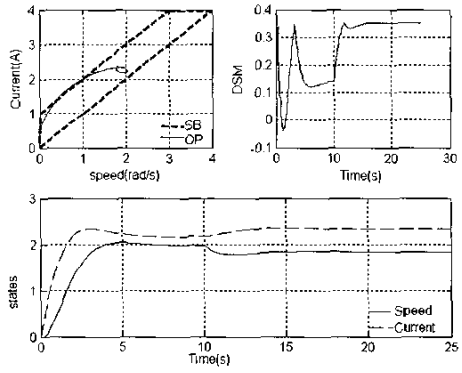


Fig. 8 dc motor response and DSM using LRT controller

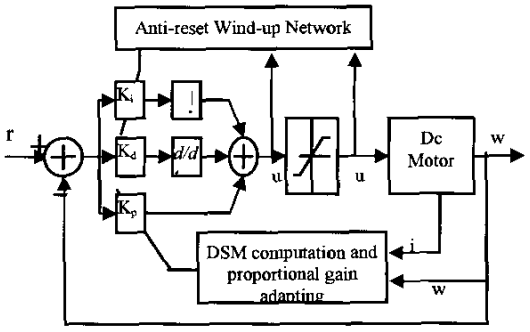


Fig. 9 PID-controller with saturation empoying Analogical-gates for anti-rest wind-up and DSM improving

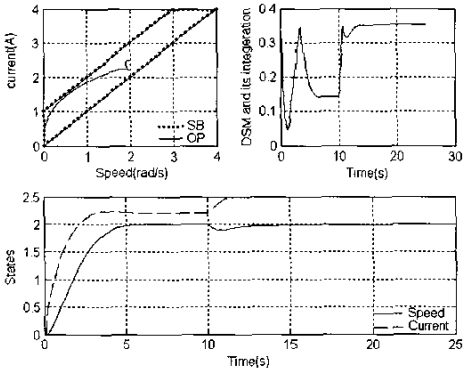


Fig. 10 dc motor response and DSM using adapted PID controller

IV EXPERIMENTAL RESULLS

Real implementation of the above algorithm, adapted PID controller (8), was applied on a laboratory two-tank system (Fig. 11a) [14],15]. Each tank has a control valve at the output line to control the level in the tank. In our experiment the interconnecting valve is fully opened, the leakage valve (control valve of 2nd tank) was adjusted manually to simulate the leakage from both tanks and the level adjusted in both tanks through the control valve of the first one. The two-tank system is fed by constant flow 1 l/s in the first tank. The safety operation region (Φ) of each tank (Fig. 11b) is given by:

$$\begin{aligned} &dh/dt+0.8\,v_i<0 \\ &dh/dt+0.8\,v_i-0.16>0 \\ &-0.4<dh/dt<0.4 \\ &-0.5<v_i<0.5 \end{aligned} \qquad (10)$$

where dh/dt is the tank level rate and v_i control signal which simulate the valve limb movement (m).

Fig. 12 and 13 show the experiment results using PID controllers with and without employing DSM for different opening of the leakage valve. It is clear that the system response, when the desired level 0.3m, has improved due to employing DSM in controller and the system performance recovered closer to the nominal performance.

V. CONCLUSION

In this paper, we have presented a new concept (DSM) to indicate how far the system trajectory from a predefined safety boundary is. Advantages of controller design based on DSM are discussed as well. DSM can control the safety of the system during transient and steady state operation, decrease disturbance effect, and help speeding up performance recovery in case of some system faults. Adaptive PID controller, LQT optimization and switching controller based on DSM are tested in this work. Practical implementation of DSM in adapting proportional gain of PID controller for laboratory plant gives a good result with respect to the fixed parameter PID controller.

The main drawbacks of DSM are: firstly, until now there is no systematic way to determine safety region, where it is knowledge base. Finally, some times it is not easy to find a mathematical formulation for the DSM. In this case a knowledge based model (fuzzy, neural...etc.) can be used. We shall generalize this idea and extend the area of using DSM in control engineering especially in FDI, FTC and performance recovery in the future work.

REFERENCES

[1] R. R. Leitch, Q. Shen, G.M. Coghill and M.j. Chantler, "Choosing the Right Model", *IEE Proc. Control theory Appl.*, vol. 146, No. 5, september 1999.

[2] 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.

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

[4] 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.

[5] S. Abdelwahed, G. Karsai and G. Biswas, "Online Safety Control of a Class of Hybrid Systems", *IEEE 2002 Conference on Decesion and Contro*", pp. 1988-1990, Las Vages,USA, December 2002.

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

[7] 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.

[8] 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

[9] D. Sauter and F. Hamelin, "Frequency-Domain Optimization for Robust Fault Detection and Isolation Dynamic System", *IEEE Trans. Automat. Cont.*, vol. 44. no. 4, pp. 878-883, 1999

[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.

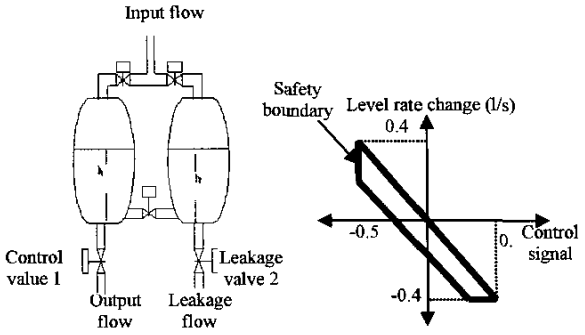
[11] M. Morari and J. lee, "Model Predictive Control: Past Present and Future", *Computers and chemical engineering*, vol. 23, pp. 667-682, 1999

[12] E. Badreddin, "Analogical gates:A Network Logical Gates: A Network Approach to Fuzzy Control with Applications to a Non-holonomic Autonomous Mobile Robot", *International Journal of Intelligent Automation and Soft Computing*, 1997

[13] Frank L. Lewis, Vassilis L. Syrmos, *Optimal Control*, 2nd ed., New York, John Wiley, 1995.

[14] T. Miksch, *Modeling and Implementation of Experimental Plant*, Diploma thesis, Mannheim University, July 2003

[15] A. Gambier, t. Miksch, E. Badreddin, "A control Laboratory Plant to Experiment with Hybrid System", *in Proc. American Control Conference 2003*, Denver, USA.



a) Schematic diagram of two-tank process b) Safety region for one tank

Fig. 11 Schematic diagram of experimental process and safe region

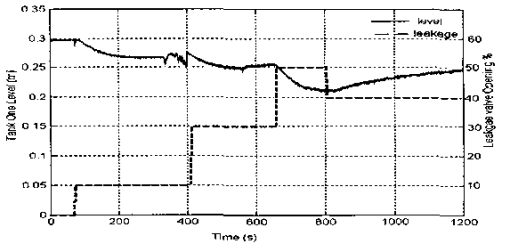


Fig. 12 Level response of experimental two-tank system using PID

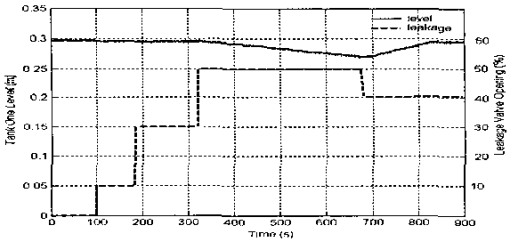


Fig. 13 Level response of experimental two-tank system using PID adapted by DSM