Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnline CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 51-24 (2018) 500–507

A Robust Fault Detection Method using a Zonotopic Kaucher Set-membership Approach

Stefan Schwab * **Vicenç Puig** ** **Soeren Hohmann** ***

* *Institute of Control Systems, Karlsruhe Institute of Technology, Karlsruhe, Germany (e-mail: stefan.schwab@kit.edu)*
** *Automatic Control Department, Universitat Politècnica de Catalunya, Barcelona, Spain (e-mail: vicenc.puig@upc.edu)*
*** *Institute of Control Systems, Karlsruhe Institute of Technology, Karlsruhe, Germany (e-mail: soeren.hohmann@kit.edu).*

Abstract: This paper presents a robust fault detection method using a zonotopic Kaucher set-membership method. The fault detection approach is based on checking the consistency between the model and the data. Consistency is given if there is an intersection between the feasible parameter set and the nominal parameter set. To allow efficient computation the feasible set is approximated by a zonotope. Due to the usage of Kaucher interval arithmetic the results are mathematically guaranteed. The proposed approach is assessed using an illustrative application based on a well-known four-tank case study. The study shows that it is possible to detect even small errors in a noisy setting.

Keywords: Robust fault detection, set-membership approach, Kaucher arithmetic.

1. INTRODUCTION

The principle of model-based fault detection is to test whether the measured system inputs and outputs are consistent with the system behavior described by a faultless model. If the measurements are inconsistent with the model of the faultless system, the existence of a fault is proved. The residual vector usually describes the result of the consistency check between the predicted and the real behavior. Ideally, the residuals should only be affected by the faults. However, the presence of disturbances, noise and modelling errors causes the residuals to become nonzero even in the nominal case and thus interferes with the detection of faults. Therefore, the fault detection procedure must be robust against these undesired effects (Chen and Patton, 1999). In case that modelling errors are taken into account in the form of parametric uncertainties, the healthy system model should include a vector of uncertain parameters bounded by sets that contain all possible parameter values when the system operates normally. So far, in the robust fault detection literature, parameters have been bounded using intervals and the resulting model is known as an interval model. This approach has received a lot of attention in the context of robust fault detection, see among others: Armengol et al. (2000); Fagarasan et al. (2004); Ploix and Adrot (2006); Puig (2010); Seydou et al. (2012); Combastel (2016). Generally in these publications the uncertainty interval for residuals (or predicted outputs) is computed by propagating the effect of the parameter uncertainty using a direct image of an interval function. Then, the model is invalidated if the measured variable for which the interval is calculated leaves the predicted interval. This approach will be referred to as a direct image test in what follows. Alternatively, following the idea proposed by Ingimundarson et al. (2009), a passive robust method based on the inverse image of the interval model (in case the system is linear or non-linear but linear with respect to the parameters) expressed in regressor form can be used to check whether there exists a member in the family of models, described by an interval model, that can explain the measured data. This inverse image test has already been suggested in Puig et al. (2006) using subpavings and SIVIA algorithm (see Jaulin et al. (2001)). However, such implementation is computationally expensive but it can be made very efficient using zonotope representation and arithmetic as shown in Ingimundarson et al. (2009).

This paper will address how models and their uncertainty parameter bounds are obtained. Standard system identification methods provide only an estimation of the nominal model but do not provide a reliable means for bounding the uncertainty associated with the model. This problem has been stated in many papers coming from robust control field (Reinelt et al., 2002). Recently some methodologies that provide a model with its uncertainty have been developed but thinking always in its application to control (Reinelt et al., 2002; Krebs et al., 2016b,a). In fact in this community, robust system identification is used to describe the new methodologies of system identification that provide not only a nominal model but also a reliable estimate of the uncertainty associated with the model. See for example the set-membership parameter estimation algorithms proposed by Milanese et al. (1996), that produces a set of parameters that are consistent with the model structure that has been selected and assumed noise bounds. Alternatively, in the Fault Detection and Identification (FDI) community, (Bravo et al., 2006; Blesa et al., 2011; Wang et al., 2017) have suggested an adaptation of classical system identifications methods in order to provide the nominal model plus the uncertainty bounds for parameters that guarantee that all collected data from the system in non-faulty scenarios will be included in the model prediction interval (worst-case parameter estimation).

However, in the setting of safety critical systems (e.g. automated driving, aviation, medical devices, process control) the worst-case view needs to be complemented by regarding also type II errors to guarantee correct functional behavior. A

2405-8963
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2018.09.623

method that will only verify a system if the real behavior is given by parameters within the nominal parameter set was presented in Schwab et al. (2017). The main difference to (Bravo et al., 2006; Blesa et al., 2011; Wang et al., 2017) is that an inner approximation of the feasible set is used instead of an outer approximation. The new approach uses Kaucher interval arithmetic to enclose measurement noise with known properties leading to guaranteed verification of behavioral conformance. The obtained guarantees represent a new quality of the verification results which is of increasing importance especially for such safety critical systems.

The main contribution of this paper is to present a robust fault detection method by combining previous work of the authors. The new method uses Kaucher arithmetic to define the feasible solution set as introduced in Schwab et al. (2017). This set is bounded by a zonotopic outer inclusion which is then shrunken to achieve a zonotopic inner inclusion as proposed by Blesa et al. (2011). The shrinking is done here by interpreting the Kaucher representation of the measurement data as constraints of an optimization problem. The feasibility of a zonotope with respect to all constraints can be checked efficiently by using the Prager-Oettli theorem (as shown in Schwab et al. (2017)) now applied to all vertices of the zonotope. The proposed approach is assessed and an illustrative application based on a well-known four-tank case study is given.

The paper is organized in the following manner. In Section 2, the problem of fault detection using a parameter consistency test is introduced and a conceptual algorithm is proposed. In Section 3, the proposed approach to implement the fault detection algorithm based on a parameter consistency test are introduced. In Section 4, an example based on a four tanks system is given that allows to show the fault detection performance. Conclusions are presented in Section 5.

2. PROBLEM FORMULATION

2.1 Problem set-up

The principle of *model-based fault detection using consistency tests* relies on checking whether the measured sequence of system inputs U and outputs Y available for N points, at every time instant k lies within the behavior described by a model of the faultless system (Blanke et al., 2006). If the measurements are inconsistent with the model of the faultless system, the existence of a fault is possible concluding the fault detection task.

In this paper it is assumed that the system output can be described by

$$y(k) = \varphi^T(k)\theta(k) + e(k) + f_y(k) \tag{1}$$
$$\theta(k+1) = \theta(k) + \theta_f(k) + w(k) \tag{2}$$
$$\theta(0) \in \Theta \tag{3}$$

where $\theta(k) \in \mathbb{R}^n$ is the parameter vector whose values are assumed to be unknown but belong to a compact bounded nominal set Θ, $\varphi(k) \in \mathbb{R}^n$ is the regressor vector which can contain any function of inputs $u(k)$ and outputs $y(k)$, $f_y(k)$ is the sensor fault signal added to the regressor equation and $\theta_f(k)$ is the parametric fault signal, both are zero in the fault-free case. The noise $e(k)$ and parameter variation $w(k)$ are limited as

$$|e(k)| \leq \sigma \quad \text{and} \quad |w(k)| \leq \lambda \tag{4}$$

As the parameter vector is assumed to belong to $\mathbb{R}^n$ so does λ and the last inequality is an element wise inequality. Notice that this system description includes any system linear in the parameters. Parameter uncertainty comes from physical modeling or from the set-membership parameter estimation algorithms applied in a non-faulty situation.

Note that Eq. (2) specifies the allowed range of uncertain parameters θ.

2.2 Fault detection algorithm

From the model description above the following sequences are defined:

$$\Phi_N = \{\varphi(k)\}_{k=0,\ldots,N-1} \qquad Y_N = \{y(k)\}_{k=0,\ldots,N-1}. \tag{5}$$

Based on the measurement data and the sensor fault assumption in (1) it is possible to define intervals $\mathbf{y}(k)$ and $\mathbf{u}(k)$ that are guaranteed to include the true (undisturbed / noiseless) system values $u_{true}(k)$ and $y_{true}(k)$ using

$$y_{true}(k) \in \mathbf{y}(k) = [y(k)-\sigma,\ y(k)+\sigma] = \left[\underline{y}(k),\ \overline{y}(k)\right] \tag{6}$$
$$u_{true}(k) \in \mathbf{u}(k) = [u(k)-\sigma,\ u(k)+\sigma] = \left[\underline{u}(k),\ \overline{u}(k)\right]. \tag{7}$$

This interval inclusions lead to an interval regressor vector φ that is used to set up the interval valued regressor matrices

$$\mathbf{A} = \{\varphi(k)\}_{k=0,\ldots,N-1} \qquad \mathbf{B} = \{\mathbf{y}\}_{k=0,\ldots,N-1}. \tag{8}$$

To define what constitutes a fault, the feasible solution set at time N is defined as follows.

Definition 1. Given the data sequences Φ_N and Y_N, the parameter θ is said to belong to the **Feasible Solution Set** at time N, (denoted FSS_N), if there exist $\theta(0), \theta(1), \ldots, \theta(N-1)$ such that:

$$|y(k) - \varphi^T(k)\theta(k)| \leq \sigma \quad k = 0,\ldots,N-1 \tag{9}$$
$$|\theta(k) - \theta(k-1)| \leq \lambda \quad k = 1,\ldots,N-1 \tag{10}$$
$$\theta(0) \in \Theta \tag{11}$$

A complementary and even stricter definition can be obtained if the identification problem is expressed in Kaucher interval arithmetic as proposed in Schwab et al. (2017).

Definition 2. The so called **United Solution Set** $\sum_{\exists\exists}$ contains all parameters that are able to map the regressor values to the output measurement values:

$$\sum_{\exists\exists}(\mathbf{A},\ \mathbf{B}) := \left\{\tilde{\theta} \in \mathbb{R}^n \mid (\exists A \in \mathbf{A}),\ (\exists B \in \mathbf{B}),\ \left(A\tilde{\theta} = B\right)\right\}. \tag{12}$$

Throughout this paper it is assumed that all specifications and measurements lead to an interval regressor matrix $\mathbf{A}$ that has full rank. This can be checked using the sufficient conditions given in Shary (2014) and it is assumed that at least one sufficient condition is fulfilled.
Using Definition 1, a fault is now defined for the sequences Φ_N and Y_N.

Definition 3. Given the data sequences Φ_N and Y_N, a **fault** is said to have occurred if the set FSS_N is empty.

Complementary consistency can be defined using definition 2:

Definition 4. The measurement is guaranteed to be **consistent** with the nominal parameters as long as, given the interval regressor matrices $\mathbf{A}$ and $\mathbf{B}$, the intersection of the united solution set $\sum_{\exists\exists}$ with the nominal parameter set Θ is non-empty i.e. $\sum_{\exists\exists} \cap \Theta \neq \emptyset$.

Each new measurement defines a set of consistent parameters defined by

$$F_k = \{\theta(k) \in \mathbb{R}^n : -\sigma \leq y(k) - \varphi(k)^T\theta(k) \leq \sigma\} \tag{13}$$

F_k is the region between two hyperplanes. The normalized form of this strip is written as

$$F_k = \{\theta \in \mathbb{R}^n : \left| \frac{y(k)}{\sigma} - \frac{\varphi(k)^T}{\sigma} \theta(k) \right| \leq 1\}$$
$$= \{\theta \in \mathbb{R}^n : \left| d(k) - c(k)^T \theta(k) \right| \leq 1\}. \quad (14)$$

The strip F_k available at time k allows to iteratively refine the feasible parameter set FSS_k:

$$FSS_{k+1} = FSS_k \cap F_k \quad (15)$$

and to detect the presence of a fault if its intersection with the feasible parameter set FSS_k is empty:

$$FSS_k \cap F_k = \emptyset \quad (16)$$

In practice, the computation of FSS_k is difficult. The fault detection algorithm presented in this paper is based on using a zonotope to upper bound the feasible solution set, creating an approximate feasible solution set denoted $AFSS_k$, that fulfills $FSS_k \subseteq AFSS_k$ and for which consistency is checked. In the case when $\lambda > 0$, the set $AFSS_k$ is expanded to take the allowed parameter range into account in the next sample. The expanded set is denoted $\overline{AFSS}_{k+1}$.

Algorithm 1 provides a general conceptual form of the suggested fault detection strategy based on the use of parameter consistency test. The basic idea of this algorithm is the following: at every time instant, input/output system measurements obtained from sensors are used to build the regressor $\varphi(k)$ and strip F_k according to Eqs. (5) and (14), respectively. Then, the consistent set between strip and the zonotope $AFSS_k$ is calculated. The algorithm proceeds to refine the current zonotope by its intersection with the strip F_k and the resulting zonotope is expanded by the allowed parameter range λ. This zonotope is now used as initial point for the optimization calculating the inner inclusion. If the intersection between the inner inclusion and the nominal set is non-empty there is consistency between measurement data and nominal system. Otherwise, if an inconsistency is detected, a fault is considered to be present.

Algorithm 1 Fault detection using a parameter consistency test

1: $k \leftarrow 0$
2: $\overline{AFSS}_k \leftarrow \Theta$
3: **while** $k < N$ **do**
4: Obtain input-output data $\{u(k), y(k)\}$ at time instant k, build regressor $\varphi(k)$ and strip F_k according to Eqs. (5) and (14).
5: Calculate **outer** inclusion $\overline{AFSS}_k$ by intersecting the strips given by the measurement
6: Set initial zonotope parameters P_k and H_k, given by the **outer** inclusion $\overline{AFSS}_k$
7: Solve optimization problem (22)-(26) to calculate α, now defining an **inner** inclusion $\sum_Z^O$
8: **if** $\sum_Z^O \cap \Theta \neq \emptyset$
9: Consistency between measurement and nominal parameter set is proven
10: **else** A fault might be existent
11: **endif**
12: $k \leftarrow k + 1$
13: **end while**

3. PROPOSED APPROACH

The approach presented in this paper is based on the verification method first presented in Schwab et al. (2017). The basic idea is appended by using a zonotope to bound the resulting solution set.

Any parameter vector $\tilde{\theta} \in \Theta$ within the nominal set can be interpreted as solution candidate for the identification equation

$$\mathbf{A}\tilde{\theta} = \mathbf{B} \quad (17)$$

with the regressor matrix $\mathbf{A}$, the measurement vector $\mathbf{B}$ and the parameter vector $\tilde{\theta} = \left[a_1^*, \cdots, a_{n_a}^*, c_1^*, \cdots, c_{n_c}^*\right]$. It is thus sufficient to show that $\tilde{\theta}$ is within the parameter region solving (17) and within the nominal parameter set Θ. Thus there is consistency between the measurement and the specification.

Proposition 1. If a given candidate parameter $\tilde{\theta}$ is part of the feasible parameter set $\sum_{\exists\exists}$, as restricted by the measurement data, and part of the nominal set Θ the system is called consistent.

- The candidate parameter $\tilde{\theta} = \left[a_1^*, \cdots, a_{n_a}^*, c_1^*, \cdots, c_{n_c}^*\right]^T \in \Theta$ is consistent with the measurement data $[\Phi_N,\ Y_N]$ of a system under test (SUT) iff
$$\tilde{\theta} \in \sum_{\exists\exists}(\mathbf{A}, \mathbf{B}), \quad (18)$$
i.e. the specified parameter vector is part of the united solution set of the measurement data.
- Whether a solution candidate $\tilde{\theta}$ is part of the united solution set $\sum_{\exists\exists}(\mathbf{A}, \mathbf{B})$ can be calculated using the criterion
$$\left| A_c\tilde{\theta} - B_c \right| \leq A_\Delta \left|\tilde{\theta}\right| + B_\Delta \quad (19)$$
given in Hladík (2014).

Proposition 1 uses the center matrix

$$A_c = \frac{1}{2}\left(\underline{A} + \overline{A}\right) \quad (20)$$

and the radius matrix

$$A_\Delta = \frac{1}{2}\left(\overline{A} - \underline{A}\right) \quad (21)$$

and applies the $\leq$-operator element-wise. A detailed proof of the proposition is given in Schwab et al. (2017), a brief sketch of the proof is as follows: If both, the nominal parameter $\tilde{\theta}$ and the current real system parameter $\tilde{\theta}_{true}$, are in the same united solution set, both are able to explain the measurement. Hence the SUT is consistent with the specification.
If (18) does not hold, $\tilde{\theta}$ cannot map a single $A \in \mathbf{A}$ onto any $B \in \mathbf{B}$. Thus this parameter does not explain the measurements and is therefore inconsistent with the current SUT.
Criterion (19) holds if and only if a solution candidate $\tilde{\theta}$ is part of the united solution set. The calculation uses the connection between the assignment of the quantors and the Kaucher interval arithmetic as explained in Schwab et al. (2017) based on Shary (2002).
Condition (19) can be used for the verification of a specific parameter $\tilde{\theta}$. The verification result for this parameter is thus available after the evaluation of one simple condition.
To solve this problem for a set of parameters $\sum$, this property can be used when the problem is reformulated as an optimization problem as follows: The identification problem (17) can be transformed into an optimization problem by interpreting the Prager-Oettli Theorem (19) as nonlinear constraint on each element $\tilde{\theta}$ of a feasible parameter region $\sum$:

$$c(\sum) := \left| A_c\tilde{\theta} - B_c \right| \leq A_\Delta \left| \tilde{\theta} \right| + B_\Delta,\ \forall \tilde{\theta} \in \sum \qquad (22)$$

with the center and radius matrix of the regressor matrix $A_c, A_\Delta \in \mathbb{R}^{N\times n}$, the center and radius vector of the measurement vector $B_c, B_\Delta \in \mathbb{R}^{N\times 1}$ the number of parameters $j = 1,\ldots,n$ and the number of used measurement points $k = 1,2,\ldots,N$. This setting restricts the feasible region to the united solution set $\sum_{\exists\exists}$. The constraints can be appended to include also the condition that the solution has to be located within the area given by the known nominal parameter set $\Theta = \left[\mathbf{a}_1^*, \cdots, \mathbf{a}_{n_a}^*, \mathbf{c}_1^*, \cdots, \mathbf{c}_{n_c}^*\right]^T = \left[\left[\underline{\Theta}^{(1)}, \overline{\Theta}^{(1)}\right], \cdots, \left[\underline{\Theta}^{(n)}, \overline{\Theta}^{(n)}\right]\right]^T$ given by the nominal system:

$$c^{(j)}(\sum) := \underline{\Theta}^{(j)} - \tilde{\theta}^{(j)} \leq 0,\ \forall \tilde{\theta} \in \sum \qquad (23)$$

$$c^{(n+j)}(\sum) := -\overline{\Theta}^{(j)} + \tilde{\theta}^{(j)} \leq 0,\ \forall \tilde{\theta} \in \sum. \qquad (24)$$

The used objective function is based on a zonotopic approximation $\sum_Z$ of the united solution $\sum_{\exists\exists}$ defined as follows:

$$\sum_Z = P_0 \oplus \alpha \boldsymbol{H_0} \boldsymbol{K}^V = \left\{ P_0 + \alpha \boldsymbol{H_0} z : z \in \boldsymbol{K}^V \right\} \in \sum_{\exists\exists} \qquad (25)$$

thereby $\sum_Z$ is exhaustively defined by the set of $v = 1,2,\ldots,V$ vertices of the zonotope, $P_0 \in \mathbb{R}^{(n\times 1)}$ the center of the zonotope, $\boldsymbol{H_0} \in \mathbb{R}^{(n\times V)}$ the radius matrix and $\boldsymbol{K}^V$ a unitary box composed of V unitary interval vectors $\boldsymbol{K} = [-1,1]$. The V vertices of the zonotope are thus defined by a given center P_0 and radius matrix H_0 and an arbitrary scaling parameter $\alpha > 0$. Each vertex v represents a solution candidate vector $\tilde{\theta}^{(v)}$ that needs to be checked using (19). The initial values of P_0 and H_0 are determined by calculating the outer inclusion as in Blesa et al. (2011), given in Eq. (13)-(16) appended to Kaucher arithmetic. The nominal set Θ is expressed as initial zonotope $P_0 = \Theta_c$ and $H_0 = I\Theta_\Delta$. Each measurement interval is iteratively interpreted as a strip containing the possible parameters. The intersection between the strip and the zonotope is calculated and the common region is used to calculate the new radius matrix. This procedure leads to a zonotopic outer inclusion of the feasible parameter set.

The idea of maximal possible parameter variability within the zonotope leads to the most general predicates if the area of the zonotope is maximal. Therefore an objective function is used to maximize the scaling parameter α of the zonotope definition (25):

$$J(\sum_Z) := -\alpha. \qquad (26)$$

The negative sign is needed to convert the maximization problem into a minimization problem that can be handled by standard optimization tools. The resulting zonotopic solution set that solves the optimization problem is denoted as solution set $\sum_Z^O$.
Additional assumptions on the optimization problem are:

- The interval solution has to be bounded to one orthant.
- All values of the input signal need to have the same sign, either all positive or all negative.

This is due to the fact that intervals containing zero can erroneously be interpreted as inverse elements and thus cancel the influence of some parameters. The all positive or all negative input signal is necessary to prevent increasing intervals that may arise even when Kaucher interval arithmetic is used.

Every solution of the optimization algorithm is guaranteed to be a solution of the identification problem, hence the conditions based on the optimization procedure are sufficient.

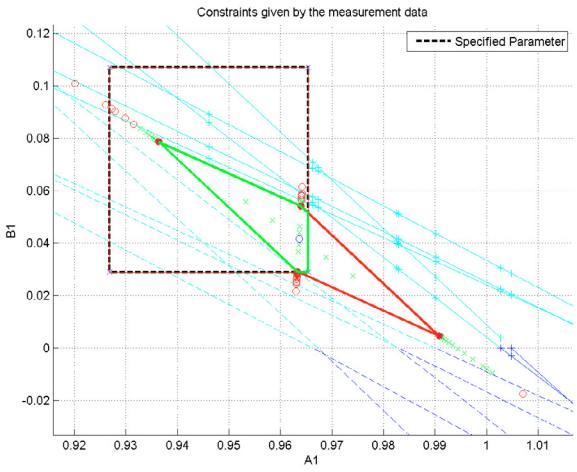


Fig. 1. Feasible set bounded by a zonotope. Initial zonotope shape and orientation given by outer approxiation, fitting is done by shrinking. Constraints given by five measurement points.

Fig. 1 shows a snapshot of an exemplary time step during the calculations. The blue lines depict the constraints given by the measurement data. Lines marked with a plus are upper borders, dashed lines are lower borders. The area between all lower and all upper borders is the feasible region. The nominal set Θ is given by the dashed black rectangle. The vertices of the initial outer zonotopic approximation are given by the outmost red circles. Each zonotope vertex that was evaluated during the optimization is given by a red circle if the Prager-Oettli theorem (19) was not fulfilled and with a green cross if it was satisfied. It is thus possible to observe the different values of α that were used by the optimization algorithm. The final zonotope is given in bold red. All vertices of the final zonotope are within the nominal set. The intersection of the final zonotope and the nominal set is given as the green polytope. As the intersection of the feasible set and the nominal set is non-empty the setting depicts measurement data that is consistent with the given specification.

4. APPLICATION EXAMPLE

The well known example of a four-tank process as proposed by Johansson (2000) is used to illustrate the results. The example setting is depicted in Fig. 2. For symmetry reasons the setting can be reduced to the tanks 1 and 3. The heights h_1 and h_3 of both tanks are measured, as well as the on/off signal of the pump v_1. All simplifications and the resulting model equations are based on the considerations of Blesa et al. (2011).
The flow exiting the tanks is governed by the formula of Torricelli which is well known to be dependent on the current height. Therefore are the nominal parameters of the tank system also depending on the height which renders them time variant. The time variant parameters can be interpreted as an interval set that includes all possible feasible parameters as well as some spurious solutions. The feasible parameter set is the bounding box of the time variant parameters. The dynamics of the first tank are given as:

$$\frac{\mathrm{d}h_1}{\mathrm{d}t} = -\underbrace{\frac{a_1}{A_1}\sqrt{2gh_1}}_{\text{outflow}} + \underbrace{\frac{a_3}{A_1}\sqrt{2gh_3}}_{\text{inflow from tank 3}} + \underbrace{\frac{\gamma_1 k_1}{A_1} v_1}_{\text{inflow by pump 1}} . \qquad (27)$$

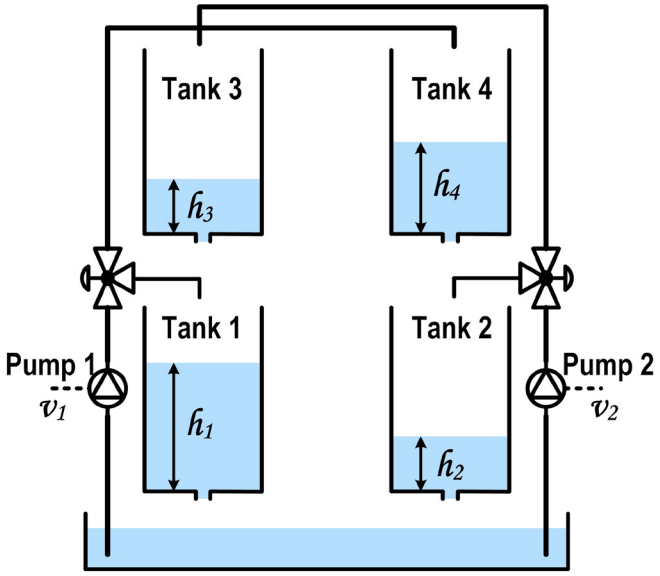


Fig. 2. Schematic view of the used 4 tank system example.

with pipe diameter $a_1 = a_3 = 0.071\text{cm}^2$, tank diameter $A_1 = 28\text{cm}^2$, gravitational force $g = 981\text{cm/s}^2$ and constants $k_1 = 3.33\text{cm}^3/\text{Vs}$ and $\gamma = 0.7$. The model is discretized using the Euler method and $\Delta t = 1\text{s}$ leading to:

$$h_1(k) = h_1(k-1) - \frac{a_1}{A_1}\sqrt{2gh_1(k-1)} + \frac{a_3}{A_1}\sqrt{2gh_3(k-1)} + \frac{\gamma_1 k_1}{A_1}v_1(k-1) + e_1(k) \tag{28}$$

where $e_1(k)$ is the additive error including sensor and discretization fault. It is considered to be bounded by

$$|e_1(k)| \leq \sigma = 0.05\text{cm}. \tag{29}$$

The measurement data is enclosed by interval bounds such that the true noiseless measurement data is guaranteed to be included in the interval.
The problem is reduced to a 2D setting to make it possible to plot the feasible parameter region:

$$y(k) = h_1(k) - \frac{\gamma_1 k_1}{A_1}v_1(k-1) \tag{30}$$

$$\varphi(k) = [h_1(k-1)\ h_3(k-1)] \tag{31}$$

$$\theta(k) = [A1\ B1]^T \tag{32}$$

with the time variant parameters

$$A1(k) = 1 - \frac{a_1}{A_1}\sqrt{\frac{2g}{h_1(k-1)}} \tag{33}$$

$$B1(k) = \frac{a_3}{A_1}\sqrt{\frac{2g}{h_3(k-1)}}. \tag{34}$$

It is assumed that the operation range of the tank system is

$$h_1 \in [2,\ 11] \quad \text{and} \quad h_3 \in [1,\ 15] \tag{35}$$

which leads to

$$A1 \in [0.920,\ 0.966] \quad \text{and} \quad B1 \in [0.029,\ 0.112] \tag{36}$$

using (33) and (34). The midpoint radius expression of the parameters is

$$A1_c = 0.943 \quad \text{and} \quad B1_c = 0.070 \tag{37}$$

$$A1_\Delta = 0.022 \quad B1_\Delta = 0.041. \tag{38}$$

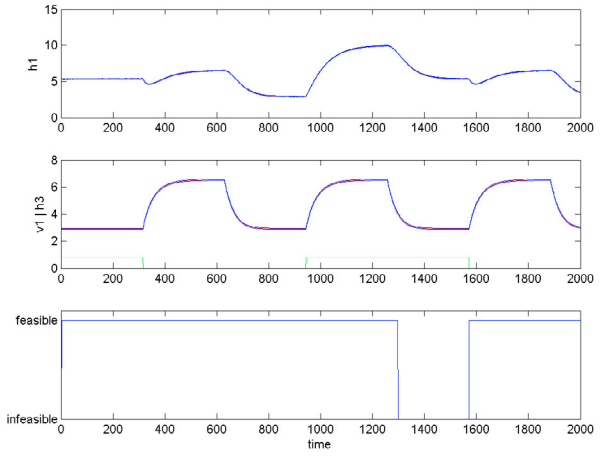


Fig. 3. The depicted error free setting is verified by the proposed method.

To use the optimization based approach given in (22)-(26) the given measurement data $[\Phi_N\ Y_N]$ and the nominal parameter set Θ are used to set up the constraints of the optimization problem. The initial zonotope is given by the nominal feasible parameter interval:

$$P_0 = [A1_c\ B1_c]^T \tag{39}$$

$$H_0 = \begin{bmatrix} A1_\Delta & 0 \\ 0 & B1_\Delta \end{bmatrix}. \tag{40}$$

Afterwards the outer inclusion of the intersection between initial zonotope and measurement data is calculated by using (13)-(16). This initial zonotope is used as starting point of the optimization problem. The solution of the optimization problem is thus a zonotopic approximation of the united solution set. The solution is given by the set $\sum_Z^O$ which is a zonotope. All parameter vectors included in the optimal solution set $\sum_Z^O$ are solutions of the identification equation (17). If the intersection of specification and measurement is non-empty, the algorithm calculates an feasible set in this area.

The results of the proposed method are demonstrated using several different settings.

4.1 Fault free setting

First a fault free scenario is given as depicted in Fig. 3. The chosen scenario includes parts with pump on and off and thus shows a variety of different water level dynamics both in h_1 and h_3. The measurement data of h_1 and h_3 are enclosed using intervals with radius $\sigma = 0.05$ which is suitable to include the used noise signal. The optimization based zonotopic method is able to calculate a feasible set of parameters that are suitable for all measurement points at $k = 2000$.
During the operation of the algorithm there are times where temporarily no feasible set was found, i.e. within $k_i \in [1298, \ldots, 1571]$. A detailed view on this region is given in Table 1 which displays the change from "feasible" to "infeasible" and back. For $k = 1297$ the measurement data are proven to be consistent with the specification (Table 1(a)). When the result turns "infeasible" in Table 1(b) there is still a feasible region within the nominal parameter set (which is proven by the green crosses, depicting vertices that fulfill (19)) but no intersection is found anymore. Nevertheless the resulting zonotope

would be able to form an intersection if it was "longer" or if the center point moved. However, the basic assumption in the proposed approach is to use the center and shape P and H of the outer inclusion and only change the scaling parameter α. Based on this theory the depicted behavior was expected to happen. The optimization based method calculates an inner inclusion (under approximation) of the parameters that are able to explain the measurement. A basic property of the inner inclusion is that some parameters might be missed which is exactly what happens within k_i. We call this effect "Center MisPlacement" (CMP) and it is a reversible phenomenon as can be seen in Table 1(d). With additional constraints from the measurement data the center and shape of the outer inclusion is moved such that it is possible to calculate an intersection with the nominal set again. As those later results are calculated based on all measurement data (including k_i) the CMP effect is "healed" and the system behavior can be verified successfully for $k > 1571$.

4.2 Additive faults

Additive faults can be located to occur in the sensors. A possible sensor error is a so called "freeze" where the sensor will return a fixed constant value. Another common sensor error is "bias" where the sensor will add a constant value to the true measurement value. The third sensor property is the specific sensor noise. Noise is not regarded a failure to be detected here. Nevertheless it is crucial to know the sensor noise precisely to choose the error bound for the interval inclusion correctly.

Given the correct faultless but noisy sensor data $s_{cor}(k)$ a sensor freeze occurring at k_{err} can be expressed as follows:

$$s_{err}(k) = s_{cor}(k_{err}) + f_f,\ \forall k \in [k_{err}, \ldots, N]\,. \tag{41}$$

The setting for an additive failure at $k_{err} = 650$ of $f_f = 0.3$ is depicted in Fig. 4. It can be seen, that the detection time k_{det} of the error is the moment of its occurrence at $k_{err} = 650$.
The failure value of $f_f = 0.3$ was chosen as a benchmark as it is also used in Blesa et al. (2011). The results given in this previous paper were obtained using the outer approximation which is used as initial zonotope in the approach proposed in this paper. To show the improvement given by the new Kaucher based zonotopic method several different failure amplitudes and the respective failure detection times k_{det} are given in Table 2. All detected failures were checked in detail to differentiate between real inconsistencies as defined in (12) and inconsistencies caused by CMP. If an inconsistency is detected in a CMP condition it can be concluded that a failure of this magnitude can not be found reliably. The values of the failures are chosen based in the benchmarks given in Blesa et al. (2011) and appended by additional suitable values. For very small values of f_f the failure can be detected but due to CMP occurrence the invalidation is not formally valid.

The second regarded failure is sensor offset. A constant sensor offset will not fix the sensor value but add a specific value to each measurement:

$$s_{err}(k) = s_{cor}(k) + f_o,\ \forall k \in [k_{err}, \ldots, N]\,. \tag{42}$$

The results for a sensor offset of $f_o = 0.7$ are depicted in Fig. 5. The inconsistency is detected right at the instant the failure occurs up to a failure amplitude of $f_o = 0.15$. Note that the measurement noise is included using $\sigma = 0.05$ which leads to an interval width of $2\sigma = 0.1$ what is very close to the failure amplitude. Further results for different failure amplitudes are

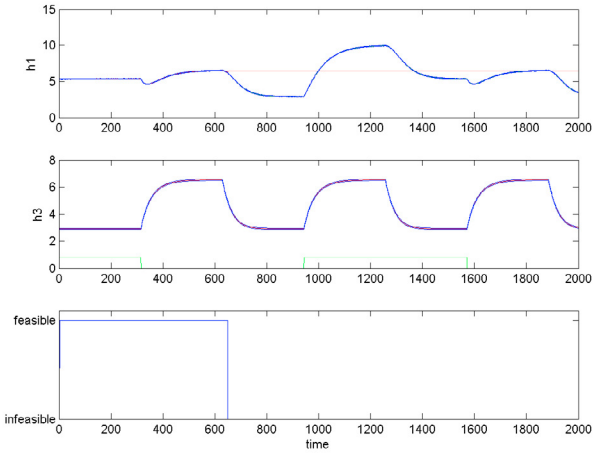


Fig. 4. Verification results for additive failure of $f_f = 0.3$ at $k_{err} = 650$.

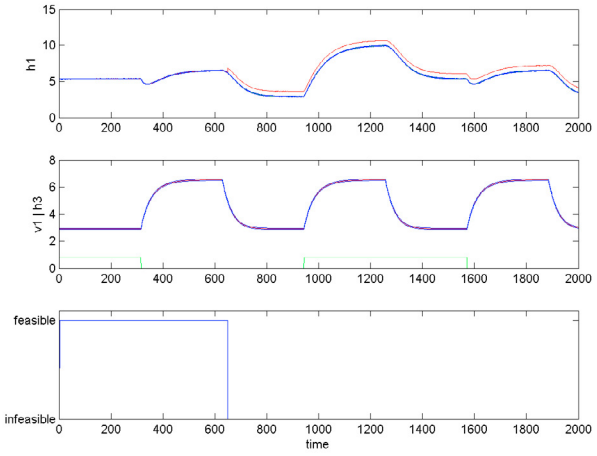


Fig. 5. Verification results for offset failure of $f_o = 0.7$ at $k_{err} = 650$.

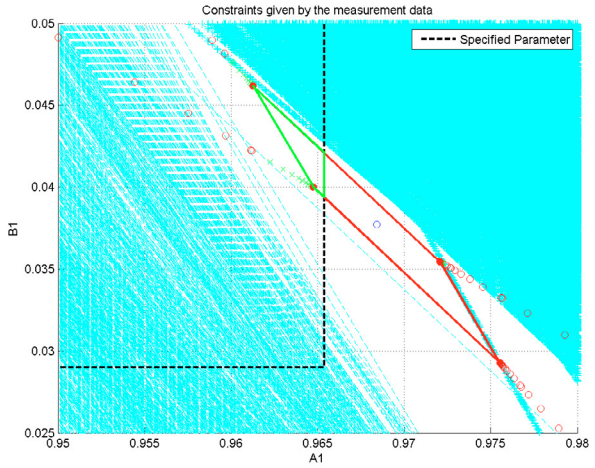
given in Table 3. There is no benchmark for the offset setting as it is newly introduced in this paper. When using $f_o = 0.1$ - which is exactly the interval width - a formal failure detection is not possible anymore as the CMP effect occurs.

4.3 Multiplicative faults

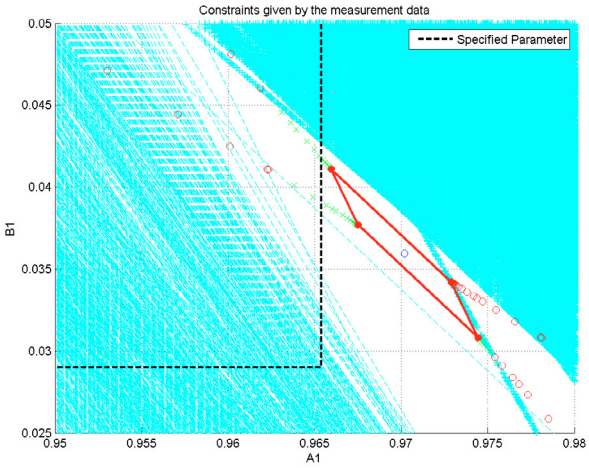
Multplicative faults can be related to faults in the system components i.e. a congested or leaking pipe or decreasing pump performance. Such a multiplicative fault e.g. $\theta_f(k) = [f_{A1}\ \ 0]^T$ directly influences the parameter of the system:

$$A1_{err}(k) = A1(k) + f_{A1},\ \forall k \in [k_{err}, \ldots, N]\,. \tag{43}$$

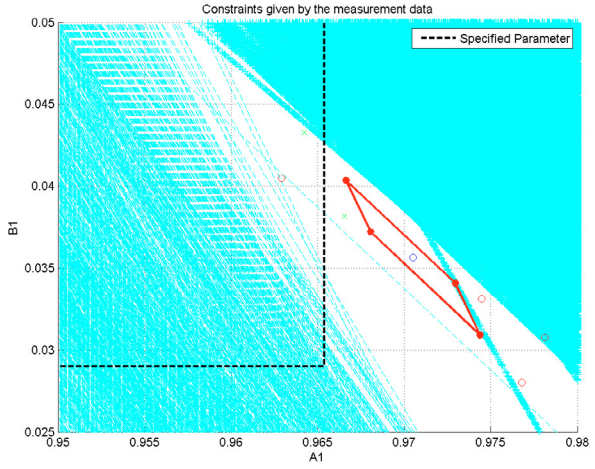
If there is a parametric fault within the measurement data, the optimization based zonotopic method is able to detect the inconsistency. The according measurement data and the resulting feasibility signal for $f_{A1} = 0.035$ is depicted in Fig. 6. Further results are given in Table 4. The values of the failures are chosen based in the benchmarks given in Blesa et al. (2011) and appended by additional suitable values. The minimum detectable fault of $f_{A1} = 0.022$ from Blesa et al. (2011) was reduced by the factor 2 to $f_{A1} = 0.01$ with this new approach.



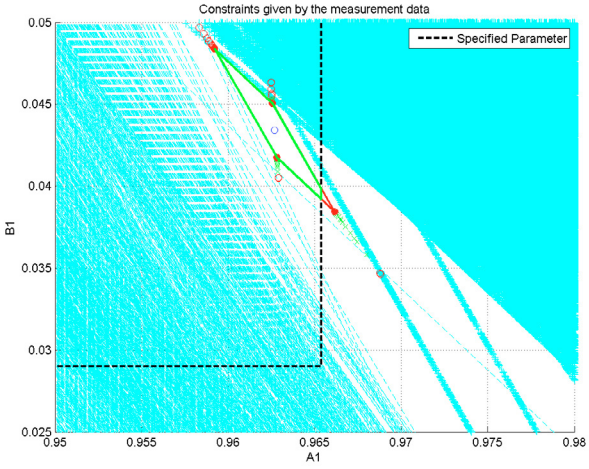
(a) $k = 1297$



(b) $k = 1298$



(c) $k = 1571$



(d) $k = 1572$

Table 1. Zoom on the CMP effect within k_i.

Failure f_f	Failure time k_{err}	Detection time k_{det}	Quality
0.70	650	650	no CMP
0.30	650	650	no CMP
0.11	650	650	CMP occured
0.05	650	691	CMP occured

Table 2. Different failure amplitudes and resulting detection times for sensor freeze

Failure f_o	Failure time k_{err}	Detection time k_{det}	Quality
0.70	650	650	no CMP
0.30	650	650	no CMP
0.20	650	650	no CMP
0.15	650	650	no CMP
0.10	650	1300	CMP occurred

Table 3. Different failure amplitudes and resulting detection times for sensor offset

Nevertheless the detection was only possible after the failure was active for quite some time. If short detection times are necessary the minimum possible failure amplitudes are within the same range. All detected inconsistencies were checked in detail and CMP occurred only in the case of $f_y = 0.005$. Note that this is a very small value with respect to the nominal parameter variability $A1_\Delta = 0.025$.

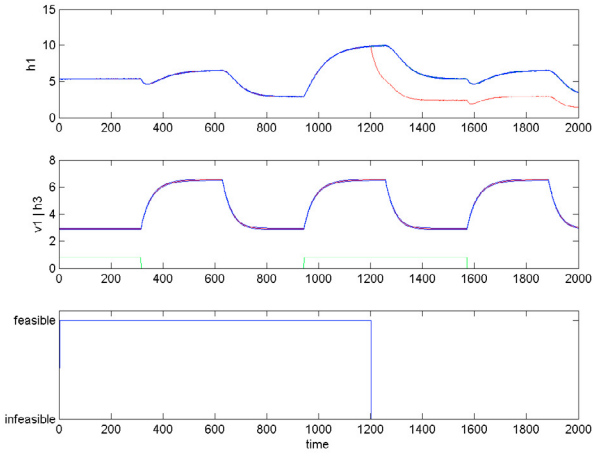


Fig. 6. Verification results for multiplicative failure of $f_{A1} = 0.035$ at $k_{err} = 1200$.

5. CONCLUSION

This paper has presented a robust fault detection method using a zonotopic Kaucher set-membership method. Robust-

Failure f_{A1}	Failure time k_{err}	Detection time k_{det}	Quality
0.035	1200	1200	no CMP
0.022	1200	1215	no CMP
0.020	1200	1227	no CMP
0.010	1200	1572	no CMP
0.005	1200	1638	CMP occurred

Table 4. Different failure amplitudes and resulting detection times for parameter failure

ness is achieved by considering uncertainty in a deterministic way by assuming an unknown but bounded description. Using input/output measurements, the model and the uncertainty bounds, a set of feasible parameters can be obtained in a non-faulty situation. The fault detection is based on checking the consistency between the model and the data by checking if the parameter feasible set is empty. The proposed approach is assessed using an illustrative application based on a well-known four-tank case study.

The examples showed that it is possible to verify the correct behavior of a dynamic system based on the input and output measurement data. The main difference to the benchmark method is that here the whole past measurement data is used to calculate a parameter set that is feasible for all times. Also the new method uses Kaucher based constraints and calculates the inner inclusion instead of the outer inclusion. This leads to the possibility to detect even very small failure amplitudes of additive and multiplicative failures. The new method is especially suitable for parametric (multiplicative) faults. In this setting very small failures can be recognized after they were persistent for a sufficient time. Large failures can be detected instantaneously. The method shows a specific property called CMP effect which was explained and examined in the paper.

The results can be improved if the initial zonotope is calculated differently and thus the CMP effect is avoided. This will be implemented in future works. Further the proposed approach should be extended to deal with non-linear systems that can be represented by means of linear parameter varying models.

ACKNOWLEDGEMENTS

This work has been partially funded by the Spanish Government and FEDER through the projects CICYT ECOCIS (ref. DPI2013- 48243-C2-1-R), CICYT DEOCS (ref. DPI2016-76493-C3-3-R) and CICYT HARCRICS (ref. DPI2014-58104-R).

REFERENCES

Armengol, J., Trave-Massuyes, L., Vehi, J., and de la Rosa, J.L. (2000). A survey on interval model simulators and their properties related to fault detection. *Annual Reviews in Control*, 24, 31–39.

Blanke, M., Kinnaert, M., Lunze, J., and Staroswiecki, M. (2006). *Diagnosis and Fault-Tolerant Control*. Springer-Verlag Berlin Heidelberg.

Blesa, J., Puig, V., and Saludes, J. (2011). Identification for passive robust fault detection using zonotope-based set-membership approaches. *International Journal of Adaptive Control and Signal Processing*, 25(9), 788–812.

Bravo, J.M., Alamo, T., and Camacho, E.F. (2006). Bounded error identification of systems with time-varying parameters. *IEEE Transactions on Automatic Control*, 51(7), 1144–1150.

Chen, J. and Patton, R. (1999). *Robust Model-Based Fault Diagnosis for Dynamic Systems*. Kluwer Academic Publishers.

Combastel, C. (2016). Kalman filtering and zonotopic state bounding for robust fault detection. In *3rd Conference on Control and Fault-Tolerant Systems (SysTol)*, 99–104.

Fagarasan, I., Ploix, S., and Gentil, S. (2004). Causal fault detection and isolation based on a set-membership approach. *Automatica*, 40, 2099–2110.

Hladík, M. (2014). AE solutions and AE solvability to general interval linear systems. *ArXiv e-prints*.

Ingimundarson, A., Bravo, J.M., Puig, V., Alamo, T., and Guerra, P. (2009). Robust fault detection using zonotope-based set-membership consistency test. *International Journal of Adaptive Control and Signal Processing*, 23(4), 311–330.

Jaulin, L., Kieffer, M., Didrit, O., and Walter, E. (2001). *Applied Interval Analysis, with Examples in Parameter and State Estimation, Robust Control and Robotics*. Springer-Verlag, London.

Johansson, K.H. (2000). The quadruple-tank process: a multivariable laboratory process with an adjustable zero. *IEEE Transactions on Control Systems Technology*, 8(3), 456–465. doi:10.1109/87.845876.

Krebs, S., Köhrer, L., and Hohmann, S. (2016a). Interval modelling of a voltage source inverter. In *IET International Conference on Power Electronics, Machines and Drives*.

Krebs, S., Schnurr, C., Pfeifer, M., Weigold, J., and Hohmann, S. (2016b). Reduced-order hybrid interval observer for verified state estimation of an induction machine. *Control Engineering Practice*, 57, 157 – 168.

Milanese, M., Norton, J., Piet-Lahanier, H., and Walter, E. (1996). *Bounding Approaches to System Identification*. Plenum Press.

Ploix, S. and Adrot, O. (2006). Parity relations for linear uncertain dynamic systems. *Automatica*, 42, 1553–1562.

Puig, V. (2010). Fault diagnosis and fault tolerant control using set-membership approaches: Application to real case studies. *International Journal of Applied Mathematics and Computer Science*, 20(4), 619–635.

Puig, V., Ingimundarson, A., , and Tornil, S. (2006). Robust fault detection using inverse images of interval functions. In *IFAC SAFEPROCESS 2006*. Beijing, China.

Reinelt, W., Garulli, A., and Ljung, L. (2002). Comparing different approaches to model error modeling in robust identification. *Automatica*, 38(5), 787 – 803.

Schwab, S., Stark, O., and Hohmann, S. (2017). Verified diagnosis of safety critical dynamic systems based on kaucher interval arithmetic. *Proceedings of the 20th IFAC World Congress*.

Seydou, R., Raissi, T., Zolghadri, A., Efimov, D., and Combastel, C. (2012). Robust fault diagnosis based on constraint satisfaction and interval continuous-time parity equations. *IFAC Proceedings Volumes*, 45(20), 1293 – 1298. 8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes.

Shary, S. (2002). A new technique in systems analysis under interval uncertainty and ambiguity. *Reliable Computing*, 8, 321–418.

Shary, S. (2014). On full-rank interval matrices. *Numerical Analysis and Applications*, 7(3), 241–254.

Wang, H., Kolmanovsky, I., and Sun, J. (2017). Zonotope-based set-membership parameter identification of linear systems with additive and multiplicative uncertainties: A new algorithm. In *2017 American Control Conference (ACC)*, 1481–1486.