Threshold design for fault detection with first order sliding mode observers

Keijzer, Twan; Ferrari, Riccardo M.G.

DOI
10.1016/j.automatica.2022.110600

Publication date
2022

Document Version
Final published version

Published in
Automatica

Automatica 146 (2022) 110600

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Brief paper

Threshold design for fault detection with first order sliding mode observers☆

Twan Keijzer, Riccardo M.G. Ferrari *

Delft University of Technology, Mekelweg 2, 2628 CD, Delft, The Netherlands

ARTICLE INFO

Article history:
Received 7 February 2021
Received in revised form 17 June 2022
Accepted 25 July 2022
Available online xxxx

ABSTRACT

Sliding Mode Observer (SMO) based methods have been extensively used for Fault Estimation (FE). However, the fault detection (FD) problem for these SMO based FE methods has not been completely solved. In this paper a robust threshold on the so-called Equivalent Output Injection (EOI) is presented which enables FD for systems with measurement noise and unmatched uncertainties. This threshold is applicable to a large class of existing SMO based FE methods, and its applicability can easily be verified. Theoretical guarantees on the detection performance of this threshold are provided, and further demonstrated via a simulation study.

1. Introduction

Following the ever growing adoption of automation technologies, also safety critical systems, such as industrial processes and autonomous vehicles, are gaining increasing autonomy. Such development calls for robust fault detection, identification, and estimation (FDIE), in order to sustain system autonomy also in the presence of faults, without requiring intervention by a supervisor.

Unknown Input Observers (UIOs) have been applied extensively for this purpose, allowing for fault estimation (FE) and detection (FD) (Chen & Zhang, 1991; Koenig, 2005; Lan & Patton, 2017; Odgaard & Stoustrup, 2012) for a class of systems as defined in Saif and Guan (1993). More recently, also sliding mode observers (SMOs) were adopted for this purpose (Alwi, Edwards, & Tan, 2008; Edwards, Spurgeon, & Patton, 2000; Fridman, Davila, & Levant, 2008; Hermans & Zarrop, 1996; Tan & Edwards, 2003). These SMO-based FE methods are applicable to a larger class of systems and have, in certain applications, better performance (Edwards & Tan, 2006).

SMO-based FE methods have furthermore been developed to allow for even broader applicability. Methods have been proposed to achieve this using higher order exact differentiators (de Loza, Henry, Cieslak, Zolghadri, & Davila, 2015; Floquet, Edwards, & Spurgeon, 2007; Fridman, Levant, & Davila, 2007; Ríos, Davila, Fridman, & Edwards, 2015) or by using multiple cascaded SMOs (Tan & Edwards, 2010). However, also methods exist where a single first order SMO (FOSMO) is used, while still relaxing the matching condition (Keijzer, Jarmolowitz, & Ferrari, 2021; Raoufi, Marquez, & Zinober, 2010; Tan, Crusca, & Aldeen, 2008; Tan & Edwards, 2003), non-minimum phase condition (Bejarano, 2011; Zhang, Swain, & Nguang, 2013), or both (Hmidi, Brahim, Hmida, & Sellami, 2020; Wang, Tan, & Zhou, 2017; Zhirabok, Zuev and Shumsky, 2021).

Nevertheless, a challenge that still needs to be addressed is the design of SMO-based FD methods when measurement noise is present. Such noise prevents ideal sliding motion to be reached: this causes the FE results to no longer be exact, and thus existing methods that use them for FD cannot lead to robust detection. In this work, we will address the FD problem for systems with measurement noise and (un)matched uncertainties, by developing a robust detection threshold. Some works consider the effects of measurement noise on SMO-based state and fault estimation using higher order SMOs, giving time-averaged/order bounds on the accuracy (de Loza et al., 2015; Fridman et al., 2007; Levant, 2003; Poznyak, 2003). However, the works considering the effect of measurement noise on FOSMO-based FE are very limited. In Zhirabok, Shumsky and Zuev (2021) it is required that measurement errors directly affect the state equation, whereas (Yang, Zhu, & Zhang, 2013) assumes the measurement noise derivatives to be bounded. Both these noise representations are restrictive and may limit the practical applicability.

In this work the FD problem for SMO based FDIE is addressed by designing a robust and deterministic FD threshold, applicable to a large class of FOSMOs, such as Alwi et al. (2008),

☆ The material in this paper was partially presented at the 58th IEEE Conference on Decision and Control, December 11–13, 2019, Nice, France. , and the 7th IFAC Workshop on Distributed Estimation and Control in Networked Systems, NecSys 2018, August 27–28, 2018, Groningen, The Netherlands. This paper was recommended for publication in revised form by Associate Editor Hernan Haimovich under the direction of Editor Sophie Tarbouriech.

* Corresponding author.
E-mail addresses: t.keijzer@tudelft.nl (T. Keijzer), r.ferrari@tudelft.nl (R.M.G. Ferrari).

https://doi.org/10.1016/j.automatica.2022.110600

Edwards et al. (2000), Keijzer et al. (2021), Tan and Edwards (2001, 2002, 2003) and Wang et al. (2017). Specifically, it will be proven that the threshold is applicable to the SMOs from Keijzer et al. (2021) and Tan and Edwards (2003). The designed threshold allows for robust FD on systems with measurement noise and (un)matched uncertainties. Furthermore, sufficient conditions will be presented (1) for which there exists a realisation of the uncertainty and measurement noise such that detection occurs and (2) for which detection is guaranteed for all uncertainty and noise realisations.

In Section 2 the threshold design problem is formulated. In Section 3 a time response of the so-called Equivalent Output Injection (EOI) is presented, such that it can be used as the basis of the fault detection threshold design in Section 4. In Section 5, guarantees on the detection performance are presented. In Section 6 it will be proven that the designed threshold is applicable to a large class of SMOs. Lastly, a simulation example of a collaborative vehicle platoon is used to demonstrate the threshold performance in Section 7.

1.1. Notation

For a vector x, $x_{(i)}$ denotes the ith element of x. Inequalities for vectors are evaluated element-wise. $\bar{x}$ and $\underset{\sim}{x}$ denote the true, possibly unknown bounds on x which are defined element-wise as $\bar{x}_{(i)} \triangleq \max_t(|x_{(i)}|)$ and $\underset{\sim}{x}_{(i)} \triangleq \min_t(|x_{(i)}|)$. $\tilde{x}$ and $\underline{x}$ denote known bounds such that $\tilde{x} \geq \bar{x}$ and $\underline{x} \leq \underset{\sim}{x}$ always hold. Superscript ^{0} denotes healthy behaviour, and superscripts u and l denote the variable is related to the so-called upper and lower thresholds respectively. $\mathrm{diag}(X)$ denotes a column vector containing the diagonal elements of a square matrix X. $|x|$ denotes the element-wise absolute value of a matrix or vector x. Lastly, when $x = 0$, it is considered $\mathrm{sign}(x) = -\mathrm{sign}(x^{nz})$ where x^{nz} is the last non-zero x.

2. Problem formulation

The aim of this paper is to present a design for a robust detection threshold that is applicable to a large class of FOSMO based fault estimation schemes. The class of systems to which the threshold is applicable will be characterised in this section using three propositions. Such statements are not restrictive, as they can be proven to hold for many existing SMOs. In Section 6, due to space constraints, the proofs will be presented only for two selected SMOs. Furthermore, in this section, the threshold design problem is formalised by introducing suitable design criteria.

2.1. System description

Let us consider a dynamical system with the form

$$\begin{cases} \dot{x}_1 = A_{11}x_1 + A^s_{12}x_2 + h_1(y,u) + E_{11}\zeta_1 + E^s_{12}\zeta_2 + N_1 f \\ \dot{x}_2 = A_{21}x_1 + A^s_{22}x_2 + h_2(y,u) + E_{21}\zeta_1 + E^s_{22}\zeta_2 + N_2 f \\ y = C_2 x_2 + F\zeta_2 \,, \end{cases}$$

where $x_1 \in \mathbb{R}^{n-p}$ and $x_2 \in \mathbb{R}^p$ are partitions of the system state; $y \in \mathbb{R}^p$ is the system output; $u \in \mathbb{R}^w$ is the system input; $f \in \mathbb{R}^r$ is a time varying term representing the fault to be detected; $\zeta_1 \in \mathbb{R}^{q_1}$ is the system uncertainty; $\zeta_2 \in \mathbb{R}^{q_2}$ is the measurement noise; and $h_1 : \mathbb{R}^{p\times w} \to \mathbb{R}^{n-p}$ and $h_2 : \mathbb{R}^{p\times w} \to \mathbb{R}^p$ are known, possibly nonlinear functions. The following, common assumptions characterise the fault and the uncertainties.

Assumption 1. $f(t) = 0$, while $t < T_f$.

Assumption 2. ζ_1, ζ_2, and f are bounded as $\bar{\zeta}_1 \geq \tilde{\zeta}_1 \triangleq \max_t(|\zeta_1|)$, $\bar{\zeta}_2 \geq \tilde{\zeta}_2 \triangleq \max_t(|\zeta_2|)$, and $\bar{f} \geq \tilde{f} \triangleq \max_t(|f|)$. Using the notation defined in Section 1.1, $\bar{\zeta}_1$, $\bar{\zeta}_2$ and $\bar{f}$ are assumed to be known, deterministic values.

We will consider an SMO of the general form

$$\begin{cases} \dot{\hat{x}}_1 = A_{11}\hat{x}_1 + A^s_{12}\hat{x}_2 + h_1(y,u) - (A^s_{12} - A_{12})C_2^{-1}e_y - K_1\nu \,, \\ \dot{\hat{x}}_2 = A_{21}\hat{x}_1 + A^s_{22}\hat{x}_2 + h_2(y,u) - (A^s_{22} - A_{22})C_2^{-1}e_y - K_2\nu \,, \\ \nu \triangleq -\mathrm{sign}(Pe_y) \\ \hat{y} = C_2\hat{x}_2 \,, \end{cases}$$

where $\hat{x}_1 \in \mathbb{R}^{n-p}$, $\hat{x}_2 \in \mathbb{R}^p$ and $\hat{y} \in \mathbb{R}^p$ are the state and output estimates; $e_y \triangleq y - \hat{y}$; and $\nu \in \mathbb{R}^p$ is the switching output feedback. The error dynamics then becomes

$$\begin{cases} \dot{e}_1 = A_{11}e_1 + A_{12}e_2 + E_{11}\zeta_1 + E_{12}\zeta_2 + N_1 f + K_1\nu \,, \\ \dot{e}_2 = A_{21}e_1 + A_{22}e_2 + E_{21}\zeta_1 + E_{22}\zeta_2 + N_2 f + K_2\nu \,, \\ e_y = C_2 e_2 + F\zeta_2 \,, \end{cases} \tag{1}$$

where $e_1 \triangleq x_1 - \hat{x}_1 \in \mathbb{R}^{n-p}$ and $e_2 \triangleq x_2 - \hat{x}_2 \in \mathbb{R}^p$ are the state estimation errors, $E_{12} = E^s_{12} - (A^s_{12} - A_{12})C_2^{-1}F$, and $E_{22} = E^s_{22} - (A^s_{22} - A_{22})C_2^{-1}F$. The fault is then estimated by $\hat{f}$ based on the switching term ν via

$$\begin{aligned} \dot{\nu}_{\mathrm{eq}} &= -K_\nu(\nu_{\mathrm{eq}} - \nu) \\ \hat{f} &= g(\nu_{\mathrm{eq}}) \end{aligned} \tag{2}$$

where $K_\nu \succ 0 \in \mathbb{R}^{p\times p}$ is the gain matrix of a stable filter, ν_{eq} is the so-called Equivalent Output Injection (EOI), and $g : \mathbb{R}^p \to \mathbb{R}^r$ is the *fault estimation function*.

Remark 1. The function $g(\nu_{\mathrm{eq}})$ can vary and depends on the specific SMO which is used. However its definition does not affect the applicability of the threshold derived in the present work.

2.2. Threshold applicability propositions

Based on the error dynamics, Propositions 1–3 together provide a sufficient condition for the threshold to be applicable. As an exemplification, in Section 6 we will prove that they hold for the SMOs from Keijzer et al. (2021) and Tan and Edwards (2003).

Proposition 1. *In Eq. (1), A_{11} is Hurwitz, $K_\nu \succ 0$ is a diagonal matrix, C_2 is invertible, and $K_2 \neq 0$.*

Proposition 2. *The following conditions on e_2 hold.*

$$\begin{cases} |e_2| \leq \tilde{e}_2 \leq \bar{e}_2 \\ sign(\dot{e}_2) = -sign(Pe_y) \\ if\ \dot{e}_2 > 0: \quad \underset{\sim}{\dot{e}}^+_2 \leq \dot{e}^+_2 \leq |\dot{e}_2| \leq \tilde{\dot{e}}^+_2 \leq \bar{\dot{e}}^+_2 \\ if\ \dot{e}_2 < 0: \quad \underset{\sim}{\dot{e}}^-_2 \leq \dot{e}^-_2 \leq |\dot{e}_2| \leq \tilde{\dot{e}}^-_2 \leq \bar{\dot{e}}^-_2 \end{cases} \tag{3}$$

where $\tilde{e}_2$, $\underset{\sim}{\dot{e}}^+_2$, $\underset{\sim}{\dot{e}}^-_2$, and $\tilde{\dot{e}}^-_2$ are the unknown true bounds, and $\bar{e}_2$, $\bar{\dot{e}}^+_2$, $\dot{e}^+_2$, $\bar{\dot{e}}^-_2$, and $\dot{e}^-_2$, are the known bounds on e_2. Furthermore, equivalent bounds for the healthy system can be obtained, denoted with superscript ^{0}.

Remark 2. The unknown bounds on e_2 introduced in Proposition 2 may not admit an algebraic closed form, albeit they can still be computed numerically from Eq. (1) and the true bounds introduced in Assumption 2. The known bounds, instead, need only to satisfy relations (3) and can be freely defined by the user in any form.

The relation between true-faulty and known-healthy bounds can thus be conveniently written as

$$\begin{aligned}
&\tilde{e}_2 + \delta_e = \bar{e}_2^0 + \delta_f(f)\,,\\
&\dot{\tilde{e}}_2^+ + \delta_{\dot{e}} = \dot{\bar{e}}_2^{0,+} + \delta_{\dot{f}}^+(f)\,;\ \dot{\underline{e}}_2^+ - \delta_{\dot{e}} = \dot{\underline{e}}_2^{0,+} + \delta_{\dot{f}}^+(f)\,,\\
&\dot{\tilde{e}}_2^- + \delta_{\dot{e}} = \dot{\bar{e}}_2^{0,-} - \delta_{\dot{f}}^-(f)\,;\ \dot{\underline{e}}_2^- - \delta_{\dot{e}} = \dot{\underline{e}}_2^{0,-} - \delta_{\dot{f}}^-(f)\,,
\end{aligned} \tag{4}$$

where $\delta_e > 0$ and $\delta_{\dot{e}} > 0$ represent the difference between the true and known bound, and $\delta_f : \mathbb{R}^r \to \mathbb{R}^p$, $\delta_{\dot{f}}^+ : \mathbb{R}^r \to \mathbb{R}^p$, and $\delta_{\dot{f}}^- : \mathbb{R}^r \to \mathbb{R}^p$ represent the effect of a fault. Here, and in the following, the superscripts $^+$ and $^-$ denote a variable relates to time periods during which the sign of $\dot{e}_2$ is, respectively, positive or negative.

Proposition 3. *For any j and d_f such that $|f_{(j)}| \geq d_f$, there exists a $\gamma > 0$ and an index i such that either of the following holds.*

I. $\delta_{f,(i)}(f) \geq 0$, $\delta_{\dot{f},(i)}^+(f) \leq -\gamma d_f$ *and* $\delta_{\dot{f},(i)}^-(f) \leq 0$.

II. $\delta_{f,(i)}(f) \geq 0$, $\delta_{\dot{f},(i)}^+(f) \geq 0$ *and* $\delta_{\dot{f},(i)}^-(f) \geq \gamma d_f$.

Remark 3. Proposition 1 presents some requirements on the observer matrices which are common for SMOs. Furthermore, Proposition 2 bounds the area around the ideal sliding surface to which the observer error is attracted. These conditions will form the basis of the threshold design. Lastly, Proposition 3 requires the fault to affect the system, which is needed for the fault to be detected.

2.3. Threshold design problem

In this paper a threshold is designed on the EOI, ν_{eq}. The lower and upper thresholds are denoted as $\bar{\nu}_{\text{eq}}$ and $\underline{\nu}_{\text{eq}}$ respectively. Detection occurs if $\nu_{\text{eq}} > \bar{\nu}_{\text{eq}}$ or $\nu_{\text{eq}} < \underline{\nu}_{\text{eq}}$. The thresholds $\bar{\nu}_{\text{eq}}$ and $\underline{\nu}_{\text{eq}}$ are designed such that:

1. The threshold is applicable to all systems and SMOs which fit the general error dynamics of (1) and for which Propositions 1–3 hold.
2. The threshold is deterministic and robust to uncertainties, i.e. there are no false positives.
3. If $\delta_e = 0$ and $\delta_{\dot{e}} = 0$, for any non-zero fault there exists a realisation of the uncertainty and noise such that detection occurs.
4. Any fault of sufficient magnitude, which is sustained for a sufficient duration, is detected for all realisations of the uncertainty and noise. Here the sufficient magnitude and duration are specified in Theorem 3.

3. Equivalent output injection dynamics

The detection logic which will be used in this paper is based on comparing the EOI, ν_{eq}, to the detection threshold. Therefore, in this section we will first derive the time response of the EOI. Then in Section 4 this will be used for threshold design.

Recall the definition of the EOI in Eq. (2). As ν is piecewise constant, the time response of each element of the EOI, $\nu_{\text{eq},(i)}$, can be written in closed form. To simplify notation, for each element $\nu_{\text{eq},(i)}$, let us denote $k_i = K_{\nu,(i,i)}$. Furthermore, we define the so-called *switching times*, $\{t_j\}_i$, as the sequence of times at which $\nu_{(i)}$ changes sign. Note that the switching times are not equally spaced, but depend on the system dynamics. In the following, wherever possible, derivations will be shown for one element $\nu_{\text{fil},(i)}$ and the subscript i will be dropped to ease notation. Furthermore, without loss of generality, it is assumed that $\nu_{(i)}$ is positive during each period $[t_{2j}\ \ t_{2j+1}]$, and $\nu_{(i)}$ is negative during each period $[t_{2j+1}\ \ t_{2j+2}]$. With this, the EOI response over any period $[t_{2j}\ \ t]$ where $t_{2j} \leq t \leq t_{2j+1}$, can be written as

$$\nu_{\text{eq},(i)}(t) = e^{-k(t-t_{2j})}\nu_{\text{eq},(i)}(t_{2j}) + (1 - e^{-k(t-t_{2j})})\,. \tag{5}$$

During the next period $[t_{2j+1}\ \ t_{2j+2}]$, $\nu_{(i)} = -1$, so the EOI response over any period $[t_{2j+1}\ \ t]$, where $t_{2j+1} \leq t \leq t_{2j+2}$, can be written as

$$\nu_{\text{eq},(i)}(t) = e^{-k(t-t_{2j+1})}\nu_{\text{eq},(i)}(t_{2j+1}) - (1 - e^{-k(t-t_{2j+1})})\,. \tag{6}$$

Substituting Eq. (5), with $t = t_{2j+1}$, into Eq. (6) gives

$$\nu_{\text{eq},(i)}(t) = e^{-k(t-t_{2j})}\nu_{\text{eq},(i)}(t_{2j}) - e^{-k(t-t_{2j})} + 2e^{-k(t-t_{2j+1})} - 1\,, \tag{7}$$

for $t_{2j+1} \leq t \leq t_{2j+2}$. Substituting Eq. (7), with $t = t_{2j+2}$, into itself, and repeating this process N times, the EOI at t_{2N} for any $N \in \mathbb{Z}^+$ can be calculated as

$$\begin{aligned}
\nu_{\text{eq},(i)}(t_{2N}) =& e^{-k(t_{2N}-t_0)}\nu_{\text{eq},(i)}(t_0)\\
&- e^{-k(t_{2N}-t_0)} + 2\sum_{j=1}^{2N-1}\left((-1)^{j+1}e^{-k(t_{2N}-t_j)}\right) - 1\,.
\end{aligned} \tag{8}$$

An example of a healthy EOI response, with the corresponding behaviour of e_2 is shown on the left in Fig. 1.

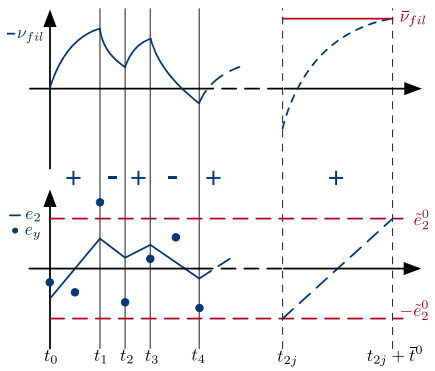

Fig. 1. Example healthy EOI response - $t_0 \leq t \leq t_4$; Worst-case EOI response for the peak threshold design - $t_{2j} \leq t \leq t_{2j} + \bar{t}^0$. Both with corresponding e_2 behaviour.

4. Fault detection threshold

In this section the detection threshold is designed as an upper bound on the healthy EOI response. This way, by construction, the threshold is guaranteed to have no false positives, i.e. design criterion 2 is satisfied. The resulting threshold consists of two parts. First, a threshold is designed bounding the EOI response considering only one period between switches. This threshold is called the *peak threshold*. However, for this threshold no sufficient conditions guaranteeing detection exist. Therefore, a so-called *sustained condition* is designed to serve as an initial condition for the peak threshold. The resulting threshold will be called the *combined threshold*. Sufficient conditions for fault detection using the combined threshold are presented in Section 5.

Because the threshold is modelled as a bound on the healthy EOI, first recall the EOI responses in Eqs. (5) and (8). From these EOI responses, a particular observation can be made, which will form the basis of the whole threshold design: *the EOI can be determined by the knowledge of its initial value and by the duration of the periods between switches, $t_j - t_{j-1}$*. These periods between switches can be bound based on the known limits on e_2 from Proposition 2. Bounding the duration of these periods in healthy conditions will thus form the core of the threshold design.

Remark 4. In the following the design procedure will only be shown for the upper threshold. The lower one can be derived similarly and only the end result will be stated.

4.1. Peak threshold

The peak threshold considers the worst-case behaviour of the healthy EOI over one period between switches. As can be seen in Eq. (5), this occurs for the maximum duration of a period between switches, which we will denote $\tilde{t}^{0,u}$. $\tilde{t}^{0,u}$ occurs for the hypothetical behaviour of e_2 where e_2 moves from its minimum, $-\tilde{e}_2^0$, to its maximum, $\tilde{e}_2^0$, with the minimum rate, $\dot{e}_2^{0,+} = \underline{\dot{e}}_2^{0,+}$, as illustrated in the right part of Fig. 1, leading to the definition below. Similarly also the known bound $\bar{t}_i^{0,u}$ is defined below, based on the known bounds on e_2.

$$\tilde{t}_i^{0,u} \triangleq \frac{2\tilde{e}_{2,(i)}^0}{\underline{\dot{e}}_{2,(i)}^{0,+}} \; ; \; \bar{t}_i^{0,u} \triangleq \frac{2\bar{e}_{2,(i)}^0}{\underline{\dot{e}}_{2,(i)}^{0,+}},$$

where we will drop the subscript i to ease notation. With these definitions, by Proposition 2, $\bar{t}_i^{0,u} \geq \tilde{t}_i^{0,u}$. Substituting $t - t_{2j} = \bar{t}^{0,u}$ in Eq. (5), gives the bound on the healthy EOI

$$\bar{\nu}_{\text{eq},(i)}^{\text{peak}}(t_{2j}) \triangleq e^{-k\bar{t}^{0,u}} \nu_{\text{eq},(i)}(t_{2j}) + 1 - e^{-k\bar{t}^{0,u}},$$

which is the so-called peak threshold. Here the argument t_{2j} denotes the time at which the threshold is calculated, or reset based on the current value of the EOI, $\nu_{\text{eq},(i)}(t_{2j})$. The resulting threshold is constant until a new peak threshold is calculated at $t_{2(j+1)}$. This threshold is used with the fault detection logic

$$\exists\, i,j \text{ s.t. } \nu_{\text{eq},(i)}(t) > \bar{\nu}_{\text{eq},(i)}^{\text{peak}}(t_{2j}) \text{ for } t \in [t_{2j}\; t_{2(j+1)}]\,. \tag{9}$$

A lower peak threshold can be designed similarly as

$$\underline{\nu}_{\text{eq},(i)}^{\text{peak}}(t_{2j+1}) = e^{-k\bar{t}^{0,l}} \nu_{\text{eq},(i)}(t_{2j+1}) - 1 + e^{-k\bar{t}^{0,l}},$$

$$\bar{t}^{0,l} \triangleq \frac{2\bar{e}_{2,(i)}^0}{\underline{\dot{e}}_{2,(i)}^{0,-}},$$

for which the fault detection logic is

$$\exists\, i,j \text{ s.t. } \nu_{\text{eq},(i)}(t) < \underline{\nu}_{\text{eq},(i)}^{\text{peak}}(t_{2j+1}) \text{ for } t \in [t_{2j+1}\; t_{2j+3}]\,. \tag{10}$$

This lower threshold has to be calculated, or reset, at every t_{2j+1} based on the current value of the EOI $\nu_{\text{eq},(i)}(t_{2j+1})$, and holds until t_{2j+3}. The peak thresholds, as presented above, are applicable to the considered SMOs, and are deterministic, i.e. design criteria 1 and 2 hold.[1] However, its detection capabilities are not consistent, thus failing to meet criterion 4. This issue is formalised by the following theorem.

Theorem 1. *If $\tilde{e}_2 \leq \max_t(C_2^{-1}F\zeta_2(t))$, no sufficient condition on f exists guaranteeing fault detection using the peak thresholds. That is, regardless of f there always exists a realisation of $\zeta_2(t)$ such that neither of the detection conditions are satisfied.*

Proof. From (3) and the hypothesis, $|e_2| \leq \tilde{e}_2 \leq \max_t(C_2^{-1}F\zeta_2)$, implying there always exists a ζ_2 such that $C_2^{-1}F\zeta_2 = e_2$. Substituting this ζ_2 in the definition of e_y from (1) gives $e_y = 0$. Thus there always exists a ζ_2 such that $e_y = 0$. By the definition of the sign function (see Section 1.1), a switch occurs when $e_y = 0$, thus there always exists a realisation of ζ_2 that makes the time between switches arbitrarily small. Detection with the peak threshold occurs only if the time between two switches is sufficiently large, specifically if $t_{2j+1} - t_{2j} > \min(\bar{t}^{0,u}, \bar{t}^{0,l})$. Therefore, detection with the peak threshold can never be guaranteed. □

[1] Design criterion 3 also holds for the peak thresholds, however due to space constraints the proof will not be provided.

Remark 5. In Section 6 it will be proven that $\tilde{e}_2 \leq \max_t(C_2^{-1}F\zeta_2)$ holds for the two selected SMOs.

To satisfy design criterion 4, the threshold design needs to be changed. In particular, we no longer want to use $\nu_{\text{eq}}(t_{2j})$ and $\nu_{\text{eq}}(t_{2j+1})$ as reset conditions for the peak thresholds. This will allow to decouple the detection performances from the actual trajectory of ν_{eq}, which depends on the uncertainty realisation and not only on the fault f. To achieve this, in the following section global bounds on $\nu_{\text{eq}}(t_{2j})$ and $\nu_{\text{eq}}(t_{2j+1})$ will be designed.

4.2. Sustained condition & combined threshold

In this section the so-called sustained condition, denoted by $\bar{\nu}_{\text{eq},0,(i)}$, is introduced as an initial condition for the peak threshold. The sustained condition replaces the reset to $\nu_{\text{eq},(i)}(t_{2j})$, which was used for the upper peak threshold. The sustained condition will be defined later. Using the sustained condition as initial condition for the peak threshold gives the so-called combined threshold as

$$\bar{\nu}_{\text{eq},(i)}(t_{2j}) = e^{-k\bar{t}^{0,u}} \bar{\nu}_{\text{eq},0,(i)}(t_{2j}) + 1 - e^{-k\bar{t}^{0,u}}\,. \tag{11}$$

To guarantee that the combined threshold does not result in any false detection, for healthy behaviour the sustained condition should globally upper-bound $\nu_{\text{eq},(i)}(t_{2j})$. By doing so the combined threshold can globally bound the healthy EOI without requiring the resets previously needed for the peak threshold. Furthermore, $\nu_{\text{eq},0}$ should be an initial condition for the peak threshold. Therefore, the hypothetical behaviour of e_2 leading to $\nu_{\text{eq},0}$ should also be an initial condition for the behaviour of e_2 leading to the peak threshold. Therefore, as the hypothetical behaviour leading to the peak threshold starts at $e_2 = -\tilde{e}_2$, for the design of $\bar{\nu}_{\text{eq},0}$, e_2 needs to be constrained as $e_2(t_{2j}) = -\tilde{e}_2\ \forall j$, as can be seen in Fig. 2. Now we will use the bounds on e_2 from Proposition 2, together with the newly found constraint $e_2(t_{2j}) = -\tilde{e}_2\ \forall j$ to bound the time between switches as

$$\begin{aligned} e_{2,(i)}(t_{2j+2}) - e_{2,(i)}(t_{2j}) = 0 &= \int_{t_{2j}}^{t_{2j+2}} \dot{e}_{2,(i)}^0 \mathrm{d}t \\ &= \int_{t_{2j}}^{t_{2j+1}} |\dot{e}_{2,(i)}^0| \mathrm{d}t - \int_{t_{2j+1}}^{t_{2j+2}} |\dot{e}_{2,(i)}^0| \mathrm{d}t \\ = \dot{e}_{2,(i)}^{0,+}(t_{2j+1} - t_{2j}) - \dot{e}_{2,(i)}^{0,-}(t_{2j+2} - t_{2j+1}) &= 0 \\ \rightarrow \frac{t_{2j+1} - t_{2j}}{t_{2j+2} - t_{2j+1}} &= \frac{\dot{e}_{2,(i)}^{0,-}}{\dot{e}_{2,(i)}^{0,+}}, \end{aligned} \tag{12}$$

where $\dot{e}_{2,(i)}^{0,+}$ and $\dot{e}_{2,(i)}^{-,0}$ are the average of $|\dot{e}_{2,(i)}^0|$ over periods $[t_{2j}\; t_{2j+1}]$, and $[t_{2j+1}\; t_{2j+2}]$, respectively. These averages, $\dot{e}_{2,(i)}^{0,+}$ and $\dot{e}_{2,(i)}^{-,0}$, can be bound in the same way as $|\dot{e}_2^0|$ is bound by Proposition 2. Using these bounds, the ratio between switching times defined in Eq. (12) can be bound for healthy behaviour as

$$\frac{t_{2j+1} - t_{2j}}{t_{2j+2} - t_{2j+1}} \leq \frac{\bar{\dot{e}}_{2,(i)}^{0,-}}{\underline{\dot{e}}_{2,(i)}^{0,+}}.$$

Now we will use this bound on the duration between switches to bound the EOI. Let us define $r_e^{0,u} = \frac{\bar{\dot{e}}_{2,(i)}^{0,-}}{\underline{\dot{e}}_{2,(i)}^{0,+}}$, and $t_{j-} = t_{2j} - t_{2j-1}$, such that we can write $t_{2j+1} - t_{2j} \leq r_e^{0,u} t_{j-}$. Using this bound in the EOI response from Eq. (8) gives the upper sustained condition as

$$\begin{aligned} \bar{\nu}_{\text{eq},0,(i)}(t_{2j}) = e^{-k(1+r_e^{0,u})\sum_{\ell=0}^{j} t_{\ell-}} \nu_{\text{eq},(i)}(t_0) - e^{-k(1+r_e^{0,u})\sum_{\ell=0}^{j} t_{\ell-}} \\ - 1 + 2\sum_{\ell=1}^{2j-1} \left((-1)^{\ell+1} e^{-k\left(\sum_{q=1}^{\left\lceil \frac{\ell}{2} \right\rceil} t_{q-} + r_e^{0,u} \sum_{q=1}^{\left\lfloor \frac{\ell}{2} \right\rfloor} t_{q-}\right)} \right). \end{aligned} \tag{13}$$

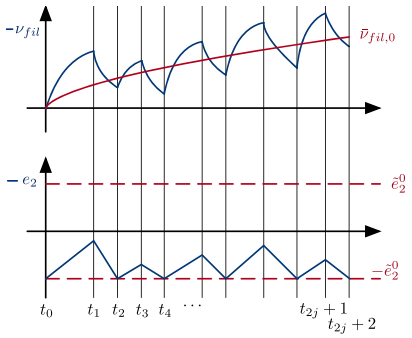

Fig. 2. Worst-case EOI response for the sustained condition design with corresponding hypothetical e_2 behaviour.

which can be calculated at time t_{2j}, for each $j \in \mathbb{Z}^+$, and is valid over the period $[t_{2j}\, t_{2j+2}]$. Substituting this sustained condition in Eq. (11) gives the combined threshold. Note that, by construction, this combined threshold satisfies design criteria 1 and 2. The corresponding detection logic is given in Eq. (9).

Remark 6. The sustained condition from Eq. (13) can be calculated recursively as

$$\begin{aligned}\bar{\nu}_{\text{eq},0,(i)}(t_{2j}) =& e^{-k(1+r_e^{0,u})t_{j-}}\nu_{\text{eq},0,(i)}(t_{2j-2}) \\ &- e^{-k(1+r_e^{0,u})t_{j-}} + 2e^{-kt_{j-}} - 1\,,\end{aligned} \tag{14}$$

to reduce the computational load.

A lower combined threshold can be designed similarly as

$$\underline{\nu}_{\text{eq},(i)}(t_{2j+1}) = e^{-k\bar{t}^{0,l}}\underline{\nu}_{\text{eq},0,(i)}(t_{2j+1}) - 1 + e^{-k\bar{t}^{0,l}}, \tag{15}$$

$$\begin{aligned}\underline{\nu}_{\text{eq},0,(i)}(t_{2j+1}) =& e^{-k(1+r_e^{0,l})\sum_{\ell=0}^{j} t_{\ell+}}\nu_{\text{eq},(i)}(t_1) + e^{-k(1+r_e^{0,l})\sum_{\ell=0}^{j} t_{\ell+}} \\ &+ 1 - 2\sum_{\ell=1}^{2j-1}\left((-1)^{\ell+1}e^{-k\left(\sum_{q=1}^{\lceil \frac{\ell}{2} \rceil} t_{q+} + r_e^{0,l}\sum_{q=1}^{\lfloor \frac{\ell}{2} \rfloor} t_{q+}\right)}\right),\end{aligned}$$

with $t_{j+} = t_{2j+1} - t_{2j}$, $t_{2j+2} - t_{2j+1} \leq r_e^{0,l} t_{j+}$, $r_e^{0,l} = \frac{\bar{\dot{e}}_{2,(i)}^{0,+}}{\underline{\dot{e}}_{2,(i)}^{0,-}}$, and the detection logic as in Eq. (10).

Even though this combined threshold is not reset at every switch, like the peak threshold was, it still requires to be recalculated at every switch, as t_{j-} and t_{j+} are actual durations between switches. Furthermore, as t_{j-} and t_{j+} are also influenced by the system uncertainty and measurement noise, the combined threshold is different for each realisation. Therefore, in the next section a constant upper-bound to the combined threshold will be designed, which can be calculated off-line.

4.3. Constant combined threshold

In this section a constant upper-bound to the combined threshold is designed. This threshold will be called the *constant combined threshold*. A constant threshold reduces the computational burden to a single off-line calculation. To calculate the constant threshold, first, without loss of generality, assume $t_{j-} = t_-$ for all j. This allows us to rewrite Eq. (13) as

$$\begin{aligned}\bar{\nu}_{\text{eq},0,(i)} =& e^{-k(1+r_e^{0,u})Nt_-}\nu_{\text{eq},(i)}(t_0) + 2(e^{-kt_-} - 1)\sum_{i=0}^{N} e^{-ki(1+r_e^{0,u})t_-} \\ &+ 1 + e^{-kN(1+r_e^{0,u})t_-} - 2e^{-k(N+1+Nr_e^{0,u})t_-}\,.\end{aligned}$$

Considering the effect of N alone, this bound will always increase for increasing N. Therefore, take $N \to \infty$ to get a simplified constant threshold.

$$\begin{aligned}\lim_{N\to\infty}\bar{\nu}_{\text{eq},0,(i)} &= 1 + 2(e^{-kt_-} - 1)\lim_{N\to\infty}\sum_{i=0}^{N} e^{-ki(1+r_e^{0,u})t_-} \\ &= 1 - 2\frac{e^{-kt_-} - 1}{e^{-k(1+r_e^{0,u})t_-} - 1}\,.\end{aligned}$$

Only considering the effect of t_-, this expression is maximised for minimal t_-. So, by taking the limit for $t_- \to 0$, once again a simplified upper-bound on the time-varying threshold is obtained. Using L'Hospital's rule this gives

$$\bar{\nu}_{\text{eq},0,(i)}^{\text{const}} = 1 - 2\frac{-k}{-k(1+r_e^{0,u})} = \frac{r_e^{0,u} - 1}{1 + r_e^{0,u}}\,.$$

Substituting the definition of $r_e^{0,u}$ this gives

$$\bar{\nu}_{\text{eq},0,(i)}^{\text{const}} = \frac{\bar{\dot{e}}_{2,(i)}^{0,-} - \underline{\dot{e}}_{2,(i)}^{0,+}}{\bar{\dot{e}}_{2,(i)}^{0,-} + \underline{\dot{e}}_{2,(i)}^{0,+}}\,. \tag{16}$$

Substituting this expression in Eq. (11) gives the constant combined threshold as

$$\bar{\nu}_{\text{eq},(i)}^{\text{const}} = e^{-k\bar{t}^{0,u}}\bar{\nu}_{\text{eq},0,(i)}^{\text{const}} + 1 - e^{-k\bar{t}^{0,u}}\,. \tag{17}$$

The used detection logic can be found in Eq. (9). A lower combined constant threshold can be designed similarly, resulting in

$$\underline{\nu}_{\text{eq},(i)}^{\text{const}} = e^{-k\bar{t}^{0,l}}\underline{\nu}_{\text{eq},0,(i)}^{\text{const}} - 1 + e^{-k\bar{t}^{0,l}}\,,$$

$$\underline{\nu}_{\text{eq},0,(i)}^{\text{const}} = -\frac{\bar{\dot{e}}_{2,(i)}^{0,+} - \underline{\dot{e}}_{2,(i)}^{0,-}}{\bar{\dot{e}}_{2,(i)}^{0,+} + \underline{\dot{e}}_{2,(i)}^{0,-}}\,,$$

with detection logic as in Eq. (10).

To summarise, in this section, first the so-called *peak threshold* $\bar{\nu}_{\text{eq}}^{\text{peak}}$ has been designed in Section 4.1. This threshold does allow for fault detection, but, detection can never be guaranteed. To address this sensitivity to measurement noise, the *sustained condition*, $\bar{\nu}_{\text{eq},0}$, was introduced in Section 4.2 as a global initial condition from which the combined threshold, $\bar{\nu}_{\text{eq}}$, can be calculated. For this combined threshold fault detection can be guaranteed, as will be proven in Section 5. However, it still has to be recalculated online at every switch of ν. To reduce the computational burden, in Section 4.3, a *constant combined threshold* $\bar{\nu}_{\text{eq}}^{\text{const}}$ has been designed which over-bounds the combined threshold.

Remark 7. The derived detection thresholds are based on a novel approach to bound ν_{eq}. As such, a full analytical derivation and a suitable notation were required. However, this does not lead to a high computational cost. $\bar{\nu}_{\text{eq}}$ can be obtained online by Eqs. (11) and (14); $\bar{\nu}_{\text{eq}}^{\text{const}}$ can be obtained offline by Eqs. (16) and (17).

5. Detectability analysis

In this section the performance of the combined threshold is analysed. In doing so it will be proven that the threshold satisfies design criteria 3 and 4. First, in Theorem 2 a condition will be presented for which there exists a realisation of the noise and uncertainty such that detection occurs. Then, in Corollary 1, it will be proven that without uncertainty the condition from Theorem 2 reduces to $f \neq 0$, proving design criterion 3 is satisfied.

Theorem 2. *If* $|\delta_f^+(f)\underline{\dot{e}}_2^{0,-} + \delta_{\dot{f}}^-(f)\bar{\dot{e}}_2^{0,+}| > \delta_{\dot{e}}(\bar{\dot{e}}_2^{0,+} + \underline{\dot{e}}_2^{0,-})$, *and* $\delta_f(f)\underline{\dot{e}}_2^{0,+} - \delta_{\dot{f}}^+(f)\bar{e}_2^0 > \delta_{\dot{e}}\bar{e}_2^0 + \delta_e\underline{\dot{e}}_2^{0,+}$ *or* $\delta_f(f)\underline{\dot{e}}_2^{0,-} + \delta_{\dot{f}}^-(f)\bar{e}_2^0 > \delta_{\dot{e}}\bar{e}_2^0 + \delta_e\underline{\dot{e}}_2^{0,+}$ *there exists a realisation of the uncertainty* ζ_1 *and noise* ζ_2 *such that detection occurs with the combined threshold.*

Proof. In order to prove that there exists a realisations of ζ_1 and ζ_2 such that detection occurs (using the upper threshold), we first design a function $\tilde{\nu}_{\text{eq}}$ such that $\exists t, \zeta_1, \zeta_2$ s.t. $\nu_{\text{eq}}(t) \geq \tilde{\nu}_{\text{eq}}$. Then, based on this function

$$\tilde{\nu}_{\text{eq}} > \bar{\nu}_{\text{eq}} \tag{18}$$

needs to hold to prove the theorem. The behaviour leading to the upper combined threshold is based on the realisations of ζ_1 and ζ_2 that maximise ν_{eq}. Therefore, with the same methodology, but using the faulty-true bounds instead of the healthy-known bounds, $\tilde{\nu}_{\text{eq}}$ is defined as

$$\tilde{\nu}_{\text{eq},(i)} = e^{-k\tilde{t}^u}\tilde{\nu}_{\text{eq},0,(i)} + (1 - e^{-k\tilde{t}^u}),$$

where $\tilde{t}^u = \frac{2\tilde{e}_2}{\dot{\tilde{e}}_2^+}$ and $\tilde{\nu}_{\text{eq},0,(i)}$ is defined as in Eq. (13) where we replace $r_e^{0,u} \leftarrow \tilde{r}_e^u = \frac{\tilde{e}_2^-}{\dot{\tilde{e}}_2^+}$. Satisfying relation (18) is now implied by $\tilde{t}^u > \bar{t}^{0,u}$ and $\tilde{r}_e^u > r_e^{0,u}$. Using Eq. (4) $\tilde{t}^u > \bar{t}^{0,u}$ can be written as

$$\delta_f(f)\dot{\underline{e}}_2^{0,+} - \delta_{\dot{f}}^+(f)\bar{e}_2^0 > \delta_{\dot{e}}\bar{e}_2^0 + \delta_e\dot{\underline{e}}_2^{0,+},$$

and $\tilde{r}_e^u > r_e^{0,u}$ can be written as

$$\delta_{\dot{f}}^+(f)\dot{\underline{e}}_2^{0,-} + \delta_{\dot{f}}^-(f)\dot{\bar{e}}_2^{0,+} < -\delta_{\dot{e}}(\bar{e}_2^{0,+} + \underline{e}_2^{0,-}).$$

Similarly, using the lower peak threshold, we obtain

$$\delta_f(f)\dot{\underline{e}}_2^{0,-} + \delta_{\dot{f}}^-(f)\bar{e}_2^0 > \delta_{\dot{e}}\bar{e}_2^0 + \delta_e\dot{\underline{e}}_2^{0,+},$$
$$\delta_{\dot{f}}^+(f)\dot{\underline{e}}_2^{0,-} + \delta_{\dot{f}}^-(f)\dot{\bar{e}}_2^{0,+} > \delta_{\dot{e}}(\dot{\bar{e}}_2^{0,+} + \dot{\underline{e}}_2^{0,-}). \quad \square$$

Corollary 1. *Assume $\delta_e = 0$ and $\delta_{\dot{e}} = 0$. If $f \neq 0$ there exists a realisation ζ_2 and ζ_1 for which detection occurs.*

Proof. Using the equalities in the theorem statement, the conditions on f in Theorem 2 reduce to $|\delta_{\dot{f}}^+(f)\dot{\underline{e}}_2^{0,-} + \delta_{\dot{f}}^-(f)\dot{\bar{e}}_2^{0,+}| > 0$, and $\delta_f(f)\dot{\underline{e}}_2^{0,+} - \delta_{\dot{f}}^+(f)\bar{e}_2^0 > 0$ or $\delta_f(f)\dot{\underline{e}}_2^{0,-} + \delta_{\dot{f}}^-(f)\bar{e}_2^0 > 0$. By Proposition 3 these conditions are implied by $f \neq 0$. $\square$

In the following, a sufficient condition will be presented guaranteeing fault detection in terms of a minimum fault magnitude, i.e. all faults continuously larger than this magnitude are guaranteed to be detected in finite time.

Theorem 3. *If*

$$\delta_{\dot{f}}^+(f) + \delta_{\dot{f}}^-(f) + (\delta_{\dot{f}}^+(f) - \delta_{\dot{f}}^-(f))\bar{\nu}_{eq} < -(\dot{\underline{e}}_2^{0,-} + \dot{\bar{e}}_2^{0,+})\bar{\nu}_{eq} + (\dot{\underline{e}}_2^{0,-} - \dot{\bar{e}}_2^{0,+} + 2\delta_{\dot{e}})$$

or

$$-\delta_{\dot{f}}^+(f) - \delta_{\dot{f}}^-(f) - (\delta_{\dot{f}}^+(f) - \delta_{\dot{f}}^-(f))\underline{\nu}_{eq} < (\dot{\underline{e}}_2^{0,-} + \dot{\bar{e}}_2^{0,+})\underline{\nu}_{eq} + (\dot{\underline{e}}_2^{0,+} - \dot{\bar{e}}_2^{0,-} + 2\delta_{\dot{e}}),$$

a fault is guaranteed to be detected within finite time.

Proof. To prove that detection is guaranteed for all realisations of ζ_1 and ζ_2, first define a function such that $\exists t$ s.t. $\nu_{\text{eq}}(t) \geq \underline{\nu}_{\text{eq}}$ $\forall \zeta_1, \zeta_2$. Then, based on this function, the relation

$$\underline{\nu}_{\text{eq}} > \bar{\nu}_{\text{eq}} \tag{19}$$

needs to hold to prove the theorem statement.

For the design of $\underline{\nu}_{\text{eq}}$, consider the behaviour leading to the lower sustained condition, $\underline{\nu}_{\text{eq},0}$. The lower sustained condition is designed such that for all realisations of ζ_1 and ζ_2, $\nu_{\text{eq}}(t_{2j+1}) \geq \underline{\nu}_{\text{eq},0}(t_{2j+1})$ if $e_2(t_{2j+3}) \geq e_2(t_{2j+1})$. Furthermore, as e_2 is bounded, $\exists t$ s.t. $e_2(t_{2j+3}) \geq e_2(t_{2j+1})$. Therefore, with the same methodology, but using the true-faulty bounds instead of the known-healthy bounds, $\underline{\nu}_{\text{eq}}$ can be defined as

$$\underline{\nu}_{\text{eq},(i)} = -\frac{\tilde{\dot{e}}_{2,(i)}^+ - \dot{\underline{e}}_{2,(i)}^-}{\tilde{\dot{e}}_{2,(i)}^+ + \dot{\underline{e}}_{2,(i)}^-}.$$

With this, detection can be guaranteed, according to Eq. (19), if

$$-\frac{\tilde{\dot{e}}_{2,(i)}^+ - \dot{\underline{e}}_{2,(i)}^-}{\tilde{\dot{e}}_{2,(i)}^+ + \dot{\underline{e}}_{2,(i)}^-} > \bar{\nu}_{\text{eq},(i)}$$

which can be simplified to

$$\delta_{\dot{f}}^+(f) + \delta_{\dot{f}}^-(f) + (\delta_{\dot{f}}^+(f) - \delta_{\dot{f}}^-(f))\bar{\nu}_{\text{eq}} < -(\dot{\underline{e}}_2^{0,-} + \dot{\bar{e}}_2^{0,+})\bar{\nu}_{\text{eq}} + (\dot{\underline{e}}_2^{0,-} - \dot{\bar{e}}_2^{0,+} + 2\delta_{\dot{e}}).$$

where subscript (i) is dropped to ease notation. Similarly considering detection by the lower threshold we obtain

$$-\delta_{\dot{f}}^+(f) - \delta_{\dot{f}}^-(f) - (\delta_{\dot{f}}^+(f) - \delta_{\dot{f}}^-(f))\underline{\nu}_{\text{eq}} < (\dot{\underline{e}}_2^{0,+} + \dot{\bar{e}}_2^{0,-})\underline{\nu}_{\text{eq}} + (\dot{\underline{e}}_2^{0,+} - \dot{\bar{e}}_2^{0,-} + 2\delta_{\dot{e}}). \quad \square$$

Corollary 2. *If $\tilde{f}$ is sufficiently large there always exists an f such that the conditions in Theorem 3 hold.*

Proof. By Assumption 2 and Proposition 3 there exists an f such that $\delta_{\dot{f},(i)}^+(f) < -\gamma d_f$ for any $0 < d_f < \tilde{f}$ and $\delta_{\dot{f},(i)}^-(f) \leq 0$. Substituting this in the first condition of Theorem 3 – for detection with the upper threshold – gives

$$\tilde{f} > \frac{(\dot{\underline{e}}_2^{0,-} + \dot{\bar{e}}_2^{0,+})\bar{\nu}_{\text{eq}} - (\dot{\underline{e}}_2^{0,-} - \dot{\bar{e}}_2^{0,+} + 2\delta_{\dot{e}})}{\gamma(1 + \bar{\nu}_{\text{eq}})}. \tag{20}$$

Similarly for detection with the lower threshold we get

$$\tilde{f} > \frac{(\dot{\underline{e}}_2^{0,-} + \dot{\bar{e}}_2^{0,+})\underline{\nu}_{\text{eq}} + (\dot{\underline{e}}_2^{0,+} - \dot{\bar{e}}_2^{0,-} + 2\delta_{\dot{e}})}{\gamma(\underline{\nu}_{\text{eq}} - 1)}. \tag{21}$$

Therefore, if $\tilde{f}$ satisfies Eqs. (20) or (21), there exists an f s.t. one of the conditions in Theorem 3 holds. $\square$

6. Proving the applicability propositions

In this section, Propositions 1–3 from Section 2 are proven for the SMOs proposed in Keijzer et al. (2021) and Tan and Edwards (2003). Similar proofs exist for many other existing SMOs such as Alwi et al. (2008), Edwards et al. (2000), Tan and Edwards (2001, 2002) and Wang et al. (2017). However, due to space constraints these proofs are omitted.

6.1. SMO from Keijzer et al. (2021)

The work by Keijzer et al. is one of the few which relaxes the matching condition for fault estimation while still only using a single FOSMO. By doing so, however, the state partition x_1 cannot be estimated. Furthermore, Keijzer et al. (2021) already considers system uncertainties and measurement noise, such that the threshold is applicable without any change to the observer. The SMO error dynamics in Keijzer et al. (2021) can be written as

$$\begin{cases} \dot{e}_1 = A_{11}e_1 + A_{12}e_2 + E_{11}\zeta_1 + E_{12}\zeta_2 + N_1 f \\ \dot{e}_2 = A_{21}e_1 + A_{22}e_2 + E_{21}\zeta_1 + E_{22}\zeta_2 + N_2 f + K_2\nu \\ e_y \triangleq \hat{y} - y = e_2 - \zeta_2 \\ \nu = -\text{sign}(e_y) \end{cases} \tag{22}$$

where ζ_1, ζ_2 and f are bounded (see Assumptions 2 and 3 in Keijzer et al. (2021)), such that Assumption 2 holds. Below we present proofs of Propositions 1–3 from Section 2.2.

Proof of Proposition 1. Assumption 4 and Proposition 1 of Keijzer et al. (2021). □

Proof of Proposition 2. Proof of these statements can be found in Proposition 1 in Keijzer et al. (2021), where known bounds $\bar{e}_2$, $\bar{\dot{e}}_2^+$, $\underline{\dot{e}}_2^+$, $\bar{\dot{e}}_2^-$, and $\underline{\dot{e}}_2^-$ have been derived directly. The true bounds $\tilde{e}_2$, $\tilde{\dot{e}}_2^+$, $\underline{\tilde{\dot{e}}}_2^+$, $\tilde{\dot{e}}_2^-$, and $\underline{\tilde{\dot{e}}}_2^-$ can be found following the same methodology. □

Proof of Proposition 3. From Proposition 1 in Keijzer et al. (2021) it can be seen that $\delta_f = 0$ and $\delta_{\dot{f}}^- = \delta_{\dot{f}}^+ = r(f)$, where in steady state $r(f) = (F_2 - A_{21}A_{11}^{\dagger}F_1)f$. By Assumption 5 in Keijzer et al. (2021) $F_2 - A_{21}A_{11}^{\dagger}F_1$ is full column-rank. □

6.2. SMO from Tan and Edwards (2003)

The SMO design by Tan and Edwards considers a system with model uncertainty to estimate both actuator and sensor faults. The work, however, does not consider measurement noise and requires the matching condition. Here, the SMO is applied on a system with measurement noise $F\zeta_2$. With the measurement noise, the observer error dynamics from equations (23) and (24) in Tan and Edwards (2003) can be written in the general form (1) as

$$\begin{cases} \dot{e}_1 = A_{11}e_1 + A_{12}e_2 + E_{11}\zeta_1 + E_{12}\zeta_2 \\ \dot{e}_2 = A_{21}e_1 + A_{22}e_2 + E_{21}\zeta_1 + E_{22}\zeta_2 + N_2 f + K_2\nu \\ e_y \triangleq \hat{y} - y = e_2 - F\zeta_2 \\ \nu = -\text{sign}(Pe_y) \end{cases}$$

where ζ_1, ζ_2 and f are bounded (see Eq. (3) and below in Tan and Edwards (2003)), such that Assumption 2 holds. Below we will present the proofs of Propositions 1–3, as introduced in Section 2.2.

Proof of Proposition 1. The proof can be found in Eq. (19), the Remark below Equation (21) and Equation (24) of Tan and Edwards (2003). □

Proof of Proposition 2. We extend Proposition 1 in Tan and Edwards (2003). Here statement (26) in Tan and Edwards (2003) depends on $e_2^{\top}P\nu < 0$[2], which is true trivially for a system without measurement noise. For a system with measurement noise this can be untrue if $-F\zeta_2 < e_2 < F\zeta_2$. Therefore, only practical convergence to an area $|e_2| \leq \max_t(F\zeta_2) = \bar{e}_2$ can be proven. This allows to define $\bar{e}_2 = |F|\bar{\zeta}_2$. By substituting ρ in the right hand side of Equation (24) in Tan and Edwards (2003) it can be proven that $\text{sign}(\dot{e}_2) = -\text{sign}(Pe_y)$. Furthermore, bounds on $\dot{e}_2$ can be obtained by bounding the right hand side of Equation (24) in Tan and Edwards (2003). □

Proof of Proposition 3. From the bounds on e_2 in Proposition 2 it can directly be found that $\delta_f = 0$ and $\delta_{\dot{f}}^- = \delta_{\dot{f}}^+ = N_2 f$, where N_2 is full column rank. □

7. Simulation example

As a simulation example, we consider a platoon of cooperative autonomous cars. Collaboration occurs by communication of the control input to the following car and only longitudinal dynamics are considered. The communicated control input is subject to Man-In-The-Middle attacks, which should be detected. Below, first, the considered system will be introduced. Then, the observer from Keijzer et al. (2021) will be applied to this system using two different sets of observer parameters. A discussion is presented on the effect of these parameter choices. The model used by the SMO for car i is taken from Keijzer and Ferrari (2021) and can be stated as

$$\begin{cases} \dot{x}_1 = A_{11}x_1 + A_{12}^s x_2 + E_{11}\zeta_1 + B_1 u + N_1 f \\ \dot{x}_2 = A_{21}x_1 + A_{22}^s x_2 + B_2 u \\ y = C_2 x_2 + F\zeta_2 \end{cases}$$

$$A_{11} = \begin{bmatrix} 0 & 0 \\ 0 & -\frac{1}{\hat{\tau}_{i-1}} \end{bmatrix}; A_{12}^s = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; A_{21} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix};$$

$$A_{22}^s = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -\frac{1}{\tau_i} \end{bmatrix}; B_1 = \begin{bmatrix} 0 & 0 \\ \frac{1}{\hat{\tau}_{i-1}} & 0 \end{bmatrix}; B_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & \frac{1}{\tau_i} \end{bmatrix};$$

$$N_1 = \begin{bmatrix} 0 \\ -\frac{1}{\hat{\tau}_{i-1}} \end{bmatrix}; E_{11} = \begin{bmatrix} 0 \\ \frac{1}{\hat{\tau}_{i-1}} \end{bmatrix}; F = I_4$$

where ζ_2 is white noise. To obtain this model, we assume $\Delta\tilde{y} = 0$ in Equation (3) in Keijzer and Ferrari (2021). Of the SMOs considered in Section 6, only the one from Keijzer et al. (2021) can be applied to this model as $N_1 \neq 0$. Furthermore, the detectors in Yang et al. (2013) and Zhirabok, Shumsky et al. (2021) are not applicable due to the measurement noise ζ_2. The noise is bounded as $\bar{\zeta}_2 = [15\ 30\ 3\ 15]^{\top} \cdot 10^{-2}$. Other model and observer parameters used in this section are presented in Table 1.

Table 1
Parameters used in simulation.

Param.	Value	Param.	Value	Param.	Value
τ_i	0.1 [s]	τ_{i-1}	0.11 [s]	$\hat{\tau}_{i-1}$	0.1 [s]
$\bar{\zeta}_1$	$1\ \left[\frac{\text{m}}{\text{s}^2}\right]$	$\bar{f}$	$10\ \left[\frac{\text{m}}{\text{s}^2}\right]$	A_{21}	0
A_{22}	$-0.1I_4$	P	I_4	K_1	0

7.1. Parameter study

In this section we will investigate the detection performance of the designed detection threshold for the system presented above. To this end we introduce two sets of design parameters which will be referred to as the *slow* and *fast* parameter sets. The slow parameter set is $K_2 = [2.35\ 3.3\ 2.2\ 3.6]$, $K_\nu = 0.1 \cdot I_4$; and the fast parameter set is $K_2 = [10.35\ 11.3\ 10.2\ 11.6]$, $K_\nu = 2 \cdot I_4$.

In Fig. 3 the detection time of a step attack with magnitude 2.8 [m/s^2] is presented for both parameter sets and for varying measurement noise bounds $\bar{\zeta}_2$. Note that for this parameter study the measurement noise bounds on each measurement are equal. One can see that for low noise bounds better detection results are obtained with the fast parameter set. However, for larger noise bounds the attack is no longer detected with the fast parameter set. This because for the same noise bound the threshold corresponding to the fast parameter set is higher than for the slow parameter set. Based on this result, the optimal parameter set for any application of the presented detection threshold depends on the system uncertainty, including measurement noise, and the expected fault/attack magnitude. Furthermore, the fault/attack shape is another factor that is not taken into consideration here. As the detector is guaranteed to have no false detections, it is possible to simultaneously use multiple detectors, without loss in accuracy. Each detector can then be designed for a specific type of fault.

[2] Tan and Edwards (2003) use e_y to denote e_2.

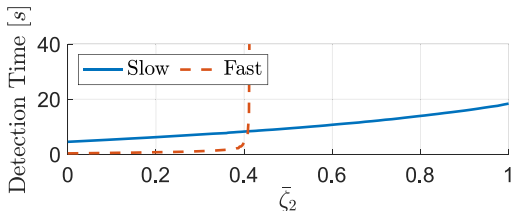

Fig. 3. Detection time of a step attack of 2.8 m/s^2 for different measurement noise bounds $\bar{\zeta}_2$. $\bar{\zeta}_1 = 1$ is kept constant.

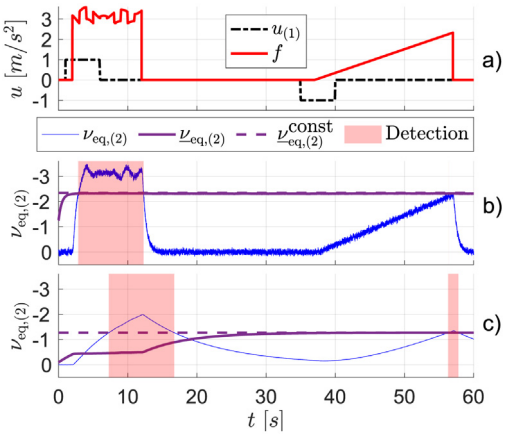

Fig. 4. (a) Input of lead vehicle and cyber-attack. (b), (c) Second element of EOI with its lower threshold. Vertical axes are inverted to highlight the estimation capability of the SMO. (b) Fast parameters; (c) Slow parameters.

7.2. Detection results for a simulation scenario

The scenario that has been simulated considers a platoon of two cars, the leader vehicle (vehicle 0) and the follower vehicle (vehicle 1). The true input of the leader vehicle is shown with the dashed black line in Fig. 4a. Furthermore, two attacks are introduced on the communication from the leader vehicle to the follower vehicle, which are depicted by the red solid line in Fig. 4a. First, at 2 s a varying step-like attack is introduced. Secondly, at 37 s a ramp attack is introduced.

For the scenario presented above we have applied the SMO from Keijzer et al. (2021) with the *slow* and *fast* parameter sets presented above. Detection performance for both parameter sets are shown in Figs. 4b and c, where the blue line is the element of the EOI relevant for detection, the solid purple line is the corresponding lower combined threshold, the dashed purple line is the lower constant combined threshold, and the red areas indicate cyber-attack detection by the constant combined threshold. Furthermore, note that for the considered combination of system and observer, by Proposition 3, we have $\hat{f} = -\nu_{eq,(2)}$. Therefore, the estimation capability of the SMO can also directly be seen from Figs. 4b and c. As shown in Figs. 4b and c, the threshold for the slow parameter set is closer to zero than for the fast parameter set. In general, the threshold is lower for lower values of K_2 and K_ν. Therefore, with the slow parameter set smaller cyber-attacks can be detected. This can also be seen in the presented scenario where the ramp-shaped attack is detected at 55.8 s with the slow parameter set but not with the fast parameter set. Conversely, if the attack is sufficiently large, detection with the fast parameter set is faster as illustrated by detection of the first step-like attack. Here the attack is detected at 3 s with the fast parameter set and at 7.1 s with the slow parameter set. In the considered platooning scenario, the step-like attack causes a crash between the vehicles at 6.2 s, meaning only detection with the fast parameter set is sufficiently fast. For the ramp attack a crash occurs at 56.2 s, meaning detection with the slow parameter set at 55.8 s is sufficiently fast. Therefore, both parameter sets need to be used simultaneously to provide sufficiently fast detection for this simulation example.

8. Concluding remarks

Sliding Mode Observers (SMOs) have been used extensively for fault estimation (FE), allowing for exact fault estimation under idealised assumptions such as the absence of measurement noise. In this paper the fault detection (FD) problem is addressed when these SMOs are applied to systems with unmatched uncertainties and measurement noise. To this end time-varying and constant robust thresholds are designed for which theoretical guarantees on detection performance are provided.

The applicability of the designed threshold can be evaluated based on three propositions relating the structure of the SMO error dynamics, boundedness of the healthy SMO errors, and the influence of the fault. Based on this, it can be concluded the threshold is applicable to a large class of SMOs. The SMO is finally applied to two existing SMOs, one of which is then demonstrated in a simulation of a Collaborative Vehicle Platoon. The simulation example shows that the theoretical detection guarantees provided hold in this scenario.

References

Alwi, H., Edwards, C., & Tan, C. P. (2008). Sliding mode estimation schemes for unstable systems subject to incipient sensor faults. In *American control conf.* (pp. 4703–4708).

Bejarano, F. J. (2011). Partial unknown input reconstruction for linear systems. *Automatica*, *47*(8), 1751–1756.

Chen, J., & Zhang, H. (1991). Robust detection of faulty actuators via unknown input observers. *International Journal of Systems Science*, *22*(10), 1829–1839.

de Loza, A. F., Henry, D., Cieslak, J., Zolghadri, A., & Davila, J. (2015). Sensor fault diagnosis using a non-homogeneous high-order sliding mode observer with application to a transport aircraft. *IET Control Theory & Applications*, *9*(4), 598–607.

Edwards, C., Spurgeon, S. K., & Patton, R. J. (2000). Sliding mode observers for fault detection and isolation. *Automatica*, *36*(4), 541–553.

Edwards, C., & Tan, C. P. (2006). A comparison of sliding mode and unknown input observers for fault reconstruction. *European Journal of Control*, *12*(3), 245–260.

Floquet, T., Edwards, C., & Spurgeon, S. K. (2007). On sliding mode observers for systems with unknown inputs. *International Journal of Adaptive Control*, 938–956.

Fridman, L., Davila, J., & Levant, A. (2008). High-order sliding-mode observation of linear systems with unknown inputs. *IFAC Proceedings Volumes*, *41*(2), 4779–4790.

Fridman, L., Levant, A., & Davila, J. (2007). Observation of linear systems with unknown inputs via high-order sliding-modes. *International Journal of Systems Science*, *38*(10), 773–791.

Hermans, F., & Zarrop, M. (1996). Sliding mode observers for robust sensor monitoring. *IFAC Proceedings Volumes*, *29*(1), 6530–6535.

Hmidi, R., Brahim, A. B., Hmida, F. B., & Sellami, A. (2020). Robust fault tolerant control design for nonlinear systems not satisfying matching and minimum phase conditions. *International Journal of Control, Automation*, *18*(9), 2206–2219.

Keijzer, T., & Ferrari, R. M. G. (2021). Detection of network and sensor cyber-attacks in platoons of cooperative autonomous vehicles: a sliding-mode observer approach. In *Eur. control conf.* (pp. 515–520).

Keijzer, T., Jarmolowitz, F., & Ferrari, R. M. G. (2021). Detection of cyber-attacks in collaborative intersection control. In *Eur. control conf.* (pp. 62–67).

Koenig, D. (2005). Unknown input proportional multiple-integral observer design for linear descriptor systems: Application to state and fault estimation. *IEEE Transactions on Automatic Control*, *50*(2), 212–217.

Lan, J., & Patton, R. J. (2017). Integrated fault estimation and fault-tolerant control for uncertain Lipschitz nonlinear systems. *International Journal of Robust and Nonlinear*, *27*(5), 761–780.

Levant, A. (2003). Higher-order sliding modes differentiation and output-feedback control. *International Journal of Control*, *76*(9–10), 924–941.

Odgaard, P. F., & Stoustrup, J. (2012). Fault tolerant control of wind turbines using unknown input observers. *IFAC Proceedings Volumes*, *45*(20), 313–318, 8th IFAC Symposium on FD, Superv. and Safety of Tech. Process.

Poznyak, A. S. (2003). Stochastic output noise effects in sliding mode state estimation. *International Journal of Control*, *76*(9–10), 986–999.
Raoufi, R., Marquez, H. J., & Zinober, A. S. (2010). H∞ sliding mode observers for uncertain nonlinear Lipschitz systems with fault estimation synthesis. *International Journal of Robust and Nonlinear*, *20*, 1785–1801.
Ríos, H., Davila, J., Fridman, L., & Edwards, C. (2015). Fault detection and isolation for nonlinear systems via high-order-sliding-mode multiple-observer. *International Journal of Robust and Nonlinear*, *25*, 2871–2893.
Saif, M., & Guan, Y. (1993). A new approach to robust fault detection and identification. *IEEE Transactions on Aerospace and Electronic Systems*, *29*(3), 685–695.
Tan, C. P., Crusca, F., & Aldeen, M. (2008). Extended results on robust state estimation and fault detection. *Automatica*, *44*(8), 2027–2033.
Tan, C. P., & Edwards, C. (2001). An LMI approach for designing sliding mode observers. *International Journal of Control*, *74*(16), 1559–1568.
Tan, C. P., & Edwards, C. (2002). Sliding mode observers for Robust fault detection & reconstruction. *IFAC Proceedings Volumes*, *35*(1), 347–352.
Tan, C. P., & Edwards, C. (2003). Sliding mode observers for robust detection and reconstruction of actuator and sensor faults. *International Journal of Robust and Nonlinear*, *13*(5), 443–463.
Tan, C. P., & Edwards, C. (2010). Robust fault reconstruction in uncertain linear systems using multiple sliding mode observers in cascade. *IEEE Transactions on Automatic Control*, *55*(4), 855–867.
Wang, X., Tan, C. P., & Zhou, D. (2017). A novel sliding mode observer for state and fault estimation in systems not satisfying matching and minimum phase conditions. *Automatica*, *79*, 290–295.
Yang, J., Zhu, F., & Zhang, W. (2013). Sliding-mode observers for nonlinear systems with unknown inputs and measurement noise. *International Journal of Control, Automation and Systems*, *11*(5), 903–910.
Zhang, J., Swain, A. K., & Nguang, S. K. (2013). Robust sensor fault estimation scheme for satellite attitude control systems. *Journal of the Franklin Institute*, *350*(9), 2581–2604.
Zhirabok, A. N., Shumsky, A. E., & Zuev, A. V. (2021). Fault diagnosis in linear systems via sliding mode observers. *International Journal of Control*, *94*(2), 327–335.
Zhirabok, A., Zuev, A., & Shumsky, A. (2021). Fault identification via sliding mode observers in nonlinear systems not satisfying matching and minimum phase conditions. In *Eur. control conf.*.

Twan Keijzer received the M.Sc. degree in Aerospace Engineering from Delft University of Technology, The Netherlands, in 2018. He is currently a Ph.D. candidate at Delft Center for Systems and Control under the supervision of Riccardo Ferrari, together with whom he won an Airbus Award at IFAC 2020 for the best contribution to the competition on Aerospace Industrial Fault Detection. His research interests include fault and cyber attack detection methods for aerospace and automotive applications, as well as distributed fault tolerant control approaches.

Riccardo M.G. Ferrari received the Laurea degree (Cum Laude and printing honours) in Electronic Engineering in 2004 and the Ph.D. degree in Information Engineering in 2009, both from University of Trieste, Italy. He is the recipient of the 2005 Giacomini Award of the Italian Acoustic Society and he obtained the 2nd place in the Competition on Fault Detection and Fault Tolerant Control for Wind Turbines during IFAC 2011. Furthermore, he was awarded an Honourable Mention for the Pauk M. Frank Award at the IFAC SAFEPROCESS in 2018. He has hold both academical and industrial R&D positions, in particular as researcher in the field of process instrumentation and control for the steel-making sector. He is a Marie Curie alumnus and currently an Assistant Professor with the Delft Center for Systems and Control, Delft University of Technology, The Netherlands. His research interests include wind power fault tolerant control and fault diagnosis and attack detection in large-scale cyber–physical systems, with applications to electric vehicles, cooperative autonomous vehicles and industrial control systems.