
Article:
Ahmad, S. and Ahmed, H. orcid.org/0000-0001-8952-4190 (2023) Robust intrusion detection for resilience enhancement of industrial control systems: an extended state observer approach. IEEE Transactions on Industry Applications. ISSN 0093-9994

https://doi.org/10.1109/tia.2023.3305361

Robust Intrusion Detection for Resilience Enhancement of Industrial Control Systems: An Extended State Observer Approach

Saif Ahmad and Hafiz Ahmed, *Senior Member, IEEE*

***Abstract*—We address the problem of attack signal estimation in industrial control systems that are subjected to actuator false data injection attack (FDIA) and where the sensor measurements are corrupted by non-negligible high-frequency measurement noise. The actuator FDIA signal is categorized as disturbance to be estimated and subsequently compensated, based on the concept of extended state observer (ESO). We investigate the efficacy of two alternatives to conventional ESO namely, cascade ESO (CESO) and low-power higher-order ESO (LHESO), that guarantee improved estimation performance in case of noisy measurement data as well as time-varying attack signals. Simulation and experimental results under different types of FDIAs demonstrate the advantages of designed schemes in comparison to conventional linear and nonlinear ESOs, using network motion control system as an illustrative example. The results highlight the limitations of conventional ESO under noisy measurement data, particularly nonlinear ESO which is based on $fal(\cdot)$ function and commonly used in control literature.**

***Index Terms*—actuator false data injection attack, industrial control system, extended state observer, measurement noise.**

I. Introduction

Technological advancements in the filed of digital communication have resulted in rapid adoption of networked control systems (NCSs) in the industrial setting due to various advantages such as increased flexibility in architecture, lower installation cost, easier maintenance and improved reliability, compared to a conventional control systems [1]. NCSs are characterized by remote sensors located near the physical system which collect and transmit data to control systems over a communication network. However, this interaction between the physical and cyber (communication) layer also gives rise to security issues as the system becomes susceptible to malicious cyber attacks at the sensor or actuator side and carries the risk of damaging the control system [2]–[7]. Over the years, an increasing number of cyber attacks on industrial control systems are being witnessed due to a proliferation of NCSs in the industrial setting, with over 16000 attacks reported in 2013 alone [2]. Furthermore, as per an IBM report on industrial control systems attacks, an increase of 110 percent cyber attacks had been observed in 2016 as compared to the previous year [5]. Intrusion detection and design of attack resilient cyber-physical industrial control systems is therefore of paramount importance to ensure safe and reliable operation of NCSs [5], [8]–[12].

A number of attack detection, isolation, estimation and control methods have been investigated in [2], [13]–[16]. References [2], [13] present a detailed survey on intrusion detection and recent advancements on the security issue in industrial cyber-physical systems along with the advantages and limitations of different techniques. A distributed nonlinear observer relying on higher-order sliding mode structure was constructed in [14] to estimate the system states along with unknown constant power load in a DC micro-grid scenario considering FDIA on the sensors. In [15], a bank of unknown input observers (UIO) were constructed for estimation of system states as well as the attack signal without using the input signals. An extended state observer (ESO) based approach was investigated for estimation of actuator FDIA in [16] in the context of a networked motion control platform where the attack signal was categorised as disturbance. It is to be noted that observer based estimation techniques studied in [14]–[16] are susceptible to high-frequency measurement noise that gets added during data collection. Furthermore, high-gain nature of the observers employed in [14], [16] give rise to numerical issue during practical implementation on fixed point digital signal processors due to finite word length.

Motivated by the aforementioned facts, we introduce two alternatives to conventional ESO, namely cascade ESO (CESO) [17], [18] and low-power higher-order ESO (LHESO) [19], that offer a promising solution to the problems associated with high-gain observers and analyze their effectiveness in the context of intrusion detection and attack signal estimation in a cyber-security setting considering the case of a networked motion control platform, similar to [16]. The present approach relies on attack signal estimation based on the difference between expected and actual system output under a specified control signal. An FDIA on the actuator side is considered in which the malicious data is added to the control signal during transmission over the communication network. However, unlike [16], we also consider the effect of high-frequency measurement noise that is often inevitable in sensor-based data acquisition. In particular, we show that the ability of CESO and LHESO to accurately estimate time-varying

S. Ahmad is with the Laboratoire Plasma et Conversion d'Énergie (LAPLACE), INP-ENSEEIHT, Toulouse 31071, France (e-mail: saif.ahmad@laplace.univ-tlse.fr).

H. Ahmed is with the Nuclear AMRC Midlands, University of Sheffield, Rutherford Way, Infinity Pk Wy, Derby DE73 5SS, UK (e-mail: hafiz.h.ahmed@ieee.org).

This work of H. Ahmed was supported by the Sêr Cymru II 80761-BU-103 project by Welsh European Funding Office (WEFO) under the European Regional Development Fund (ERDF). This work was supported in part by the Royal Society Short Industry Fellowship under grant SIF\R1\221035.

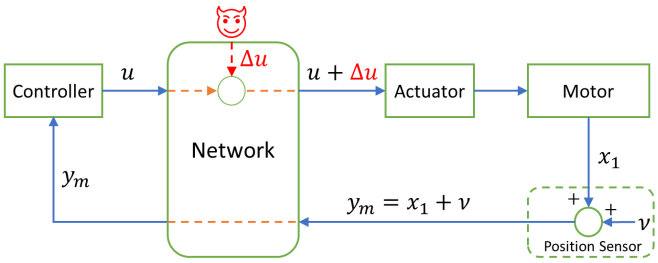


Fig. 1: Block diagram showing actuator FDIA on a networked motion control platform.

signals makes them a better alternative to conventional ESO. Furthermore, the low-power structure of LHESO limits the maximum observer gain to be implemented to 'two' which in turn takes care of the numerical issue associated with the practical implementation in a digital setting [20], [21]. We also highlight a major limitation of nonlinear ESO (NESO) in terms of oscillations around the steady state operating point which happens due to over-amplification of measurement noise. A preliminary version of this work has been published in [22]. This work builds on similar ideas and includes additional analysis, results and discussions. In particular, the current works includes the following aspects in addition to the work presented in [22]: **a.)** Rigorous stability analysis of model assisted CESO and LHESO which are employed as actuator FDIA estimators. Although the considered motion control platform exhibits linear dynamics, the estimators are designed for general nonlinear systems in strict feedback form and can be used for a wider class of systems. **b.)** Experimental validation on a motion control platform.

Remaining sections in this paper are organised as follows: Section II deals with the problem formulation considering actuator FDIA on a networked motion control system. Conventional linear and nonlinear ESOs are briefly revisited in Section III in the context of attack signal estimation. Sections IV and V introduce two noise suppressing ESOs, namely, CESO and LHESO, for attack signal estimation and highlights structural properties that result in superior estimation performance along with convergence analysis. Numerical study using Simulink/MATLAB environment is carried out in Section VI to highlight the effectiveness of the designed schemes. Comprehensive experimental validation using Quanser rotary servo unit SRV02 is presented in Section VII. The papers ends in Section VIII with a summary of conclusions and future perspectives.

II. Problem Formulation

In this paper, we consider a second order networked motion control platform studied in [16] and expressed as follows:

$$\begin{cases} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -ax_2 + bu \\ y_m &= x_1 + \nu, \end{cases} \tag{1}$$

where x_1, x_2 denote the position and speed of the motor, respectively and y_m is the sensed value of positions which is acted upon by an additive high-frequency measurement noise signal denoted by ν. A direct structure is considered for the networked control system which comprises a controller and a remote unit connected via a communication channel [1]. The remote unit further contains a physical plant i.e. servo motor, actuator and sensor for position feedback.

We consider a scenario where the system defined in (1) is subjected to a cyber attack at the actuator side (as shown in Fig. 1) where the attack signal is denoted by Δu. System (1) under actuator FDIA can be expressed as

$$\begin{cases} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -ax_2 + b[u + \Delta u] \\ &= -ax_2 + bu + \vartheta \\ y_m &= x_1 + \nu, \end{cases} \tag{2}$$

where $\vartheta = b\Delta u$ denotes the net effect of attack signal on the dynamics of motion control platform.

Considering that the system model in (1) is accurate, the attack signal (Δu) can be estimated by using the concept of extended state observer where the unknown FDIA signal is categorised as additive disturbance term. Including ϑ in the state space model, the augmented dynamics for (2) is obtained as

$$\begin{cases} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -ax_2 + \vartheta + bu \\ \dot{\vartheta} &= h \\ y_m &= x_1 + \nu, \end{cases} \tag{3}$$

where h denotes the derivative of ϑ.

III. Extended State Observer (ESO)

It is to be noted that the augmented system defined in (3) is in strict feedback form [20], and therefore, it is possible to design an extended state observer (ESO) of high-gain form to obtain its estimate. Following assumptions are made to ensure the stability of ESO:

Assumption 1: *Derivative of ϑ i.e. $h = \dot{\vartheta}$ is bounded in the manner $|h| \leq \mu_1$ [17].*

Assumption 2: *Measurement noise ν is bounded and the bound is given by $|\nu| \leq \mu_2$ [18].*

A nonlinear extended state observer (NESO) is designed for (3) following the general design approach given in [23] which gives

$$\begin{cases} e_1 &= y_m - \hat{x}_1 \\ \dot{\hat{x}}_1 &= \hat{x}_2 + \beta_1 \cdot \varsigma_1(e_1) \\ \dot{\hat{x}}_2 &= -a\hat{x}_2 + \hat{\vartheta} + bu + \beta_2 \cdot \varsigma_2(e_1) \\ \dot{\hat{\vartheta}} &= \beta_3 \cdot \varsigma_3(e_1), \end{cases} \tag{4}$$

where β_1, β_2, β_3 denote observer gains and $\varsigma_i(e_1)$ is the nonlinear error function which is expressed as

$$\varsigma_i(e_1) = fal(e_1, \alpha_i, \delta) = \begin{cases} \dfrac{e_1}{\delta^{1-\alpha_i}} & |e_1| \leq \delta \\ |e_1|^{\alpha_i} sign(e_1) & |e_1| > \delta, \end{cases} \tag{5}$$

where δ is the threshold value. However, the NESO is difficult to analyse and tune due to its nonlinear nature and large number of tuning parameters. Furthermore, the small error large gain nature of the $fal(\cdot)$ function [24] results in significant noise amplification around steady state and contaminates the attack signal estimate.

In order to have a simpler implementation as well as tuning, a linear ESO (LESO) was proposed in [25] where the nonlinear function ς_i is replaced by e_1. Furthermore, the observer gains are parameterized in terms of an observer bandwidth denoted by ω_o such that $\beta_i = \epsilon_i \omega_o^i$ where ϵ_i is a positive constant. However, high-gain nature of LESO also results in noise amplification in the obtained estimates as evidenced by the following estimation error bound obtained for a third order ESO [26]:

$$\begin{aligned} \lim_{t\to\infty} \|\tilde{\boldsymbol{x}}\| &\leq \kappa_1 |h| \omega_o^{-1} + \kappa_2 |\nu| \omega_o^2 \\ &\leq \kappa_1 \mu_1 \omega_o^{-1} + \kappa_2 \mu_2 \omega_o^2, \end{aligned} \tag{6}$$

for some $\omega_o \geq \omega_o^*$, where κ_1, κ_2 are some positive constants, $\|\tilde{\boldsymbol{x}}\| := \sqrt{\tilde{\boldsymbol{x}}^T \tilde{\boldsymbol{x}}}$ denotes the Euclidean norm of $\tilde{\boldsymbol{x}} := \boldsymbol{x} - \hat{\boldsymbol{x}}$, $\boldsymbol{x} := [x_1, x_2, \vartheta]^T$ and $\hat{\boldsymbol{x}} := [\hat{x}_1, \hat{x}_2, \hat{\vartheta}]^T$. The aforementioned inequality in (6) makes it clear that an increase in ω_o attenuates the effect of disturbance (h) by $\mathcal{O}(\omega_o^{-1})$ on the estimation error, however, the effect of measurement noise (ν) is amplified by $\mathcal{O}(\omega_o^2)$. This relation in turn forces a compromise between fast and accurate disturbance estimation and noise contamination of the estimates, while selecting the observer bandwidth. In addition, escalation of observer gains to ω_o^{n+1}, where n is the system order, gives rise to numerical issue during practical implementation on fixed-point digital signal processors [26]. These problems are addressed in the following sections by introducing alternatives to the conventional ESO structure.

IV. Cascade Extended State Observer (CESO)

Cascade ESO [17], [18], attempts to overcome the noise amplification issue through virtual decomposition of the total disturbance into N number of components and then estimating each component via a set of N cascaded ESO where the output of ESO in each level acts as a reference for subsequent level. In doing so, the noise sensitivity of the final set of estimates obtained from CESO is improved due to filtering at each level.

A. System Description

In order to tackle the FDIA estimation problem for a more general class of nonlinear systems, we consider a second order nonlinear system whose augmented state-space model is defined in the following form:

$$\dot{\boldsymbol{x}} = \boldsymbol{\mathcal{A}}\boldsymbol{x} + b\boldsymbol{\mathcal{B}}u + \boldsymbol{\Phi}(\boldsymbol{x}) + \boldsymbol{E}h, \tag{7}$$

where $\boldsymbol{\Phi}(\boldsymbol{x}) := [\phi_1(x_1, x_2, \vartheta), \phi_2(x_1, x_2, \vartheta), \phi_3(x_1, x_2, \vartheta)]^T$ is Lipschitz and

$$\boldsymbol{\mathcal{A}} = \begin{bmatrix} \boldsymbol{0} & \boldsymbol{I}_2 \\ 0 & \boldsymbol{0} \end{bmatrix}_{3\times 3}, \boldsymbol{\mathcal{B}} = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}_{1\times 3}^T, \boldsymbol{C} = \begin{bmatrix} 1 & \boldsymbol{0} \end{bmatrix}_{1\times 3},$$
$$\boldsymbol{E} = \begin{bmatrix} \boldsymbol{0} & 1 \end{bmatrix}_{1\times 3}^T.$$

For the particular case of networked motion control platform studied in this work (3), $\boldsymbol{\Phi}(\boldsymbol{x})$ is a linear combination given by

$$\boldsymbol{\Phi}(\boldsymbol{x}) = \boldsymbol{\phi}\boldsymbol{x}, \boldsymbol{\phi} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & -a & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

B. Design of CESO

In this paper, we aim to develop a two level CESO in order to estimate the actuator FDIA. Therefore, the FIDA signal is split into two components $\vartheta = \tilde{\vartheta}_1 + \tilde{\vartheta}_2$ where each component is estimated by an ESO in CESO. Considering the system defined in (7), the i^{th} level ESO in CESO is implemented via the following expression:

$$\dot{\hat{\boldsymbol{z}}}_i = \boldsymbol{\mathcal{A}}\hat{\boldsymbol{z}}_i + b\boldsymbol{\mathcal{B}}u + \boldsymbol{\Phi}(\hat{\boldsymbol{z}}_i) + \boldsymbol{L_i}(y_{i-1} - \boldsymbol{C}\hat{\boldsymbol{z}}_{\boldsymbol{i}}) + \sum_{k=1}^{i-1} \boldsymbol{\Gamma}\hat{\boldsymbol{z}}_k, \tag{8}$$

where

$$\boldsymbol{L_i} = [l_{i,1}, l_{i,2}, l_{i,3}]^T, \hat{\boldsymbol{z}}_i = [\hat{x}_{i,1}, \hat{x}_{i,2}, \hat{\tilde{\vartheta}}_i]^T, \boldsymbol{\Gamma} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix},$$

$y_i = \boldsymbol{C}\hat{\boldsymbol{z}}_{\boldsymbol{i}}$ for $i = \{1, 2\}, y_0 = y$.

In order to reduce the number of tuning parameters in the ESOs, the observer gains are selected such that all the poles are placed at $-\omega_{oi}$ as per bandwidth parameterization approach highlighted in [25], which results in $l_{i,1} = 3, l_{i,2} = 3, l_{i,3} = 1$, for third order ESOs used in the present study. Furthermore, the observer bandwidths for individual ESOs are selected as $\omega_{oi} = \omega_o a^{i-1},\ i = \{1, 2\}$ where $a > 1$ is a tuning parameter.

The final set of estimates of the system states as well as total disturbance are obtained as

$$\hat{\boldsymbol{x}} = [\hat{x}_1, \hat{x}_2, \hat{\tilde{\vartheta}}]^T = \hat{\boldsymbol{z}}_2 + \boldsymbol{E}\boldsymbol{E}^T\hat{\boldsymbol{z}}_1, \tag{9}$$

where the state estimates of system states i.e. $\hat{x}_1, \hat{x}_2$ are obtained from the 2^{nd} level ESO while estimate of FDIA is a sum of estimates obtained from each ESO.

Similar to LESO, the estimates of 1^{st} level in CESO are directly affected by measurement noise and have a relative degree of unity which is the primary reason behind poor noise suppression. However, cascade ESO attempts to overcome this limitation by selecting a lower observer bandwidth in first level of CESO compared to LESO, hence, the noise content in $\hat{\tilde{\vartheta}}_1$ is relatively low. Consequently, CESO results in improved noise suppression compared to LESO despite having the same relative degree between $\tilde{\vartheta} := \vartheta - \hat{\vartheta}$ and ν, i.e., unity [19]. However, CESO still suffers from the numerical issue as the observer gains to be implemented escalate to $\mathcal{O}(\omega_{oi}^{n+1}), i = \{1, 2\}$.

We define a combined estimation error variable as $\boldsymbol{e_z} := [\boldsymbol{e}_{\boldsymbol{z_1}}^T, \boldsymbol{e}_{\boldsymbol{z_2}}^T]^T$ where

$$\boldsymbol{e}_{\boldsymbol{z_i}} := \boldsymbol{x} - \hat{\boldsymbol{x}}_{\boldsymbol{i}},\ \hat{\boldsymbol{x}}_{\boldsymbol{i}} = \hat{\boldsymbol{z}}_{\boldsymbol{i}} + \boldsymbol{E}\boldsymbol{E}^T \sum_{j=1}^{i-1} \hat{\boldsymbol{z}}_{\boldsymbol{j}},\ \boldsymbol{i} = \{1, 2\}, \tag{10}$$

following the approach introduced in [18], which results in the following estimation error dynamics:

$$\dot{\boldsymbol{e}}_{\boldsymbol{z}} = \boldsymbol{\mathcal{A}}_{\boldsymbol{z}}\boldsymbol{e}_{\boldsymbol{z}} + \boldsymbol{\Phi}_{\boldsymbol{z}}(e_z) + \boldsymbol{E}_{\boldsymbol{z}}h - \boldsymbol{L}_{\boldsymbol{z}}\nu \tag{11}$$

where

$$\boldsymbol{\mathcal{A}}_{\boldsymbol{z}} = \begin{bmatrix} \boldsymbol{\mathcal{A}} - \boldsymbol{L_1 C} & \boldsymbol{0}_{3\times3} \\ \boldsymbol{L_2 C} - \boldsymbol{E E^T L_1 C} & \boldsymbol{\mathcal{A}} - \boldsymbol{L_2 C} \end{bmatrix}_{6\times6}, \boldsymbol{E}_{\boldsymbol{z}} = \begin{bmatrix} \boldsymbol{E} \\ \boldsymbol{E} \end{bmatrix}_{6\times1}$$

$$\boldsymbol{\Phi}_{\boldsymbol{z}} = \begin{bmatrix} \phi & \boldsymbol{0}_{3\times3} \\ \boldsymbol{0}_{3\times3} & \phi \end{bmatrix}_{6\times6}, \boldsymbol{L}_{\boldsymbol{z}} = \begin{bmatrix} \boldsymbol{L_1} \\ \boldsymbol{E E^T L_1} \end{bmatrix}_{6\times1}.$$

Remark 1: It is to be noted that the dynamics of motion control platform defined in (7) has been split into two parts, "$\boldsymbol{\mathcal{A}x}$" and "$\boldsymbol{\Phi}(\boldsymbol{x})$", where the first part conforms to the prime form which frequently appears in the literature pertaining to high-gain observers and allows us to illustrate some useful properties such as effect of high-gain parameter (ω_o in our case) on transient peaks, disturbance and measurement noise. The second part can be either linear or nonlinear and usually manifests in the form of a lower bound on the high-gain parameter in order to ensure convergence property of the designed observer which is illustrated in the following subsection.

C. Stability Analysis

In order to proceed with the stability analysis of the designed CESO, we assume that ***Assumption 1*** and ***2*** defined previously in Section III hold true. Now, we apply the following change of variables on (11) so as to highlight the compromise in selection of observer bandwidth (ω_o) in terms of minimizing the effect of disturbance versus noise noise suppression:

$$\boldsymbol{e}_{\boldsymbol{z}} \rightarrow \boldsymbol{\zeta}_{\boldsymbol{z}} := \boldsymbol{\mathcal{D}}_{\boldsymbol{z}}\boldsymbol{e}_{\boldsymbol{z}}, \tag{12}$$

where $\boldsymbol{\mathcal{D}}_{\boldsymbol{z}}$:=diag$\left[1, \omega_o^{-1}, \omega_o^{-2}, 1, a^{-1}\omega_o^{-1}, a^{-2}\omega_o^{-2}\right]$, which results in

$$\begin{aligned} \dot{\boldsymbol{\zeta}}_{\boldsymbol{z}} &= \boldsymbol{\mathcal{D}}_{\boldsymbol{z}}\boldsymbol{\mathcal{A}}_{\boldsymbol{z}}\boldsymbol{\mathcal{D}}_{\boldsymbol{z}}^{-1}\boldsymbol{\zeta}_{\boldsymbol{z}} + \boldsymbol{\mathcal{D}}_{\boldsymbol{z}}\boldsymbol{\Phi}_{\boldsymbol{z}} + \boldsymbol{\mathcal{D}}_{\boldsymbol{z}}\boldsymbol{E}_{\boldsymbol{z}}h - \boldsymbol{\mathcal{D}}_{\boldsymbol{z}}\boldsymbol{L}_{\boldsymbol{z}}\nu \\ &= \omega_o\boldsymbol{\Pi}_{\boldsymbol{z}}\boldsymbol{\zeta}_{\boldsymbol{z}} + \boldsymbol{\delta}_{\boldsymbol{z}} + \omega_o^{-2}\bar{\boldsymbol{E}}_{\boldsymbol{z}}h - \omega_o\bar{\boldsymbol{L}}_{\boldsymbol{z}}\nu \end{aligned} \tag{13}$$

where $\text{eig}(\boldsymbol{\Pi}_{\boldsymbol{z}}) = \{-1,-1,-1,-a,-a,-a\}$, $\bar{\boldsymbol{E}}_{\boldsymbol{z}} = \left[\boldsymbol{E}^T, a^{-2}\boldsymbol{E}^T\right]^T$, $\bar{\boldsymbol{L}}_{\boldsymbol{z}} = [\boldsymbol{L_1}^T, 0, 0, l_{2,3}a]^T$ and $\|\boldsymbol{\delta}_{\boldsymbol{z}}\| \leq \mu_z\|\boldsymbol{\zeta}_{\boldsymbol{z}}\|$.

We consider a Lyapunov function given by

$$V_z = \boldsymbol{\zeta}_{\boldsymbol{z}}^{\boldsymbol{T}}\boldsymbol{P}_{\boldsymbol{z}}\boldsymbol{\zeta}_{\boldsymbol{z}} \tag{14}$$

where $\boldsymbol{P}_{\boldsymbol{z}}$ is a symmetric positive definite matrix that satisfies

$$\boldsymbol{P}_{\boldsymbol{z}}\boldsymbol{\Pi}_{\boldsymbol{z}} + \boldsymbol{\Pi}_{\boldsymbol{z}}^{\boldsymbol{T}}\boldsymbol{P}_{\boldsymbol{z}} = -\boldsymbol{I}. \tag{15}$$

Taking derivative of V_z along (13), results in

$$\begin{aligned} \dot{V}_z \leq& -\omega_o\|\boldsymbol{\zeta}_{\boldsymbol{z}}\|^2 + 2\|\boldsymbol{P}_{\boldsymbol{z}}\|\|\boldsymbol{\delta}_{\boldsymbol{z}}\|\|\boldsymbol{\zeta}_{\boldsymbol{z}}\| \\ &+ 2\omega_o^{-2}\|\boldsymbol{P}_{\boldsymbol{z}}\|\|\bar{\boldsymbol{E}}_{\boldsymbol{z}}\|\|\boldsymbol{\zeta}_{\boldsymbol{z}}\||h| + 2\omega_o\|\boldsymbol{P}_{\boldsymbol{z}}\|\|\bar{\boldsymbol{L}}_{\boldsymbol{z}}\|\|\boldsymbol{\zeta}_{\boldsymbol{z}}\||\nu|, \\ \leq& -\omega_o\|\boldsymbol{\zeta}_{\boldsymbol{z}}\|^2 + 2\|\boldsymbol{P}_{\boldsymbol{z}}\|\|\boldsymbol{\zeta}_{\boldsymbol{z}}\|^2\mu_z \\ &+ 2\omega_o^{-2}\|\boldsymbol{P}_{\boldsymbol{z}}\|\|\bar{\boldsymbol{E}}_{\boldsymbol{z}}\|\|\boldsymbol{\zeta}_{\boldsymbol{z}}\|\mu_1 + 2\omega_o\|\boldsymbol{P}_{\boldsymbol{z}}\|\|\bar{\boldsymbol{L}}_{\boldsymbol{z}}\|\|\boldsymbol{\zeta}_{\boldsymbol{z}}\|\mu_2. \end{aligned} \tag{16}$$

For $\omega_o \geq 4\|\boldsymbol{P}_{\boldsymbol{z}}\|\mu_z$,

$$\begin{aligned} \dot{V}_z \leq& -\frac{1}{2}\omega_o\|\boldsymbol{\zeta}_{\boldsymbol{z}}\|^2 + 2\omega_o^{-2}\|\boldsymbol{P}_{\boldsymbol{z}}\|\|\bar{\boldsymbol{E}}_{\boldsymbol{z}}\|\|\boldsymbol{\zeta}_{\boldsymbol{z}}\|\mu_1 \\ &+ 2\omega_o\|\boldsymbol{P}_{\boldsymbol{z}}\|\|\bar{\boldsymbol{L}}_{\boldsymbol{z}}\|\|\boldsymbol{\zeta}_{\boldsymbol{z}}\|\mu_2. \end{aligned} \tag{17}$$

Therefore

$$\begin{aligned} \dot{V}_z \leq& -\frac{1}{4}\omega_o\|\boldsymbol{\zeta}_{\boldsymbol{z}}\|^2 \\ &\forall\|\boldsymbol{\zeta}_{\boldsymbol{z}}\| \geq 8(\omega_o^{-3}\|\boldsymbol{P}_{\boldsymbol{z}}\|\|\bar{\boldsymbol{E}}_{\boldsymbol{z}}\|\mu_1 + \|\boldsymbol{P}_{\boldsymbol{z}}\|\|\bar{\boldsymbol{L}}_{\boldsymbol{z}}\|\|\mu_2), \end{aligned} \tag{18}$$

which implies that

$$\lim_{t\to\infty}\|\boldsymbol{\zeta}_{\boldsymbol{z}}(t)\| \leq \kappa_1\omega_o^{-3}\mu_1 + \kappa_2\mu_2 \tag{19}$$

where $\kappa_1,\ \kappa_2$ are positive constants [18]. Assuming $\omega_o \geq 1$, it can be shown that $a^{-2}\omega_o^{-2}\|\boldsymbol{e}_{\boldsymbol{z}}\| \leq \|\boldsymbol{\zeta}_{\boldsymbol{z}}\| \leq \|\boldsymbol{e}_{\boldsymbol{z}}\|$ from (12) which in turn yields the following bound for $\|\boldsymbol{e}_{\boldsymbol{z}}\|$:

$$\lim_{t\to\infty}\|\boldsymbol{e}_{\boldsymbol{z}}(\boldsymbol{t})\| \leq \kappa_1 a^2\omega_o^{-1}\mu_1 + \kappa_2 a^2\omega_o^2\mu_2. \tag{20}$$

The actual estimation error vector $\boldsymbol{e} := \boldsymbol{x} - \hat{\boldsymbol{x}} = [x_1 - \hat{x}_1, x_2 - \hat{x}_, \vartheta - \hat{\vartheta}]^T$, is a sub-vector of $\boldsymbol{e}_{\boldsymbol{z}}$, which implies $\|\boldsymbol{e}\| \leq \|\boldsymbol{e}_{\boldsymbol{z}}\|$. Hence,

$$\lim_{t\to\infty}\|\boldsymbol{e}(\boldsymbol{t})\| \leq \kappa_1 a^2\omega_o^{-1}\mu_1 + \kappa_2 a^2\omega_o^2\mu_2. \tag{21}$$

The steady-state ultimate bound for $\|\boldsymbol{e}\|$ is valid for some $\omega_o \geq \omega_o^*$ where $\omega_o^* \geq 1$ and illustrates that the effect of disturbance on estimation error reduces upon increasing the value of ω_o, however, the obtained estimates become more sensitive to the effect of measurement noise. It is also evident that practical convergence of estimation error is only possible in the neighbourhood of origin and that the estimation error cannot be made arbitrarily small by selecting higher values of ω_o.

***Remark 2*:** It is to be noted that standard ESO used in conventional ADRC is a special case of CESO obtained for $N = 1$. Hence the design and stability analysis of conventional ESO has not been discussed separately. The estimation error bounds obtained for a two level CESO in (21) is also applicable for conventional ESO if we select $a = 1$ and results in error bounds given in (6).

***Remark 3*:** An interesting feature of CESO that relies on virtual decomposition of disturbance is that it naturally embeds a higher-order ESO (HESO) or generalized proportional integral observer (GPIO) [27] type property into the resulting structure, i.e., CESO is able to accurately estimate ramp-type attack signals where $\ddot{\vartheta} = 0$ despite being designed based on the assumption that ϑ is constant in steady-state. However, the output estimate ($\hat{x}_{2,1}$) is not accurate in the time-varying case and results in a steady-state error if it is used in feedback control design.

V. Low-power Higher-order Extended State Observer (LHESO)

In order to overcome both the issues associated with high-gain LESO, i.e., noise amplification as well as numerical implementation, a low-power higher-order ESO is designed for (2) using the structure introduced in [26].

A. System Description

The essence of higher-order augmented observer design lies in embedding higher-order time polynomial internal model for the unknown quantity, inside the state observer [27]. In our case, we assume that the FDIA denoted by $\vartheta(t)$ is a time varying quantity such that $\ddot{\vartheta} = 0$, which gives

$$\vartheta_1 = \vartheta, \dot{\vartheta}_1 = \vartheta_2, \dot{\vartheta}_2 = 0, \tag{22}$$

and is included in (2) to obtain the following augmented model:

$$\begin{cases} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -ax_2 + \vartheta + bu \\ \dot{\vartheta}_1 &= \vartheta_2 \\ \dot{\vartheta}_2 &= g, \\ y_m &= x_1 + \nu, \end{cases} \tag{23}$$

where g is second derivative of the non-zero residual term that does not match the assumed disturbance form in (22).

B. Design of LHESO

An LHESO is designed for the system defined in (23) having two state augmentations, using the following expression:

$$\begin{aligned} \Pi_1 :&= \begin{cases} \dot{\hat{x}}_1 &= \hat{\bar{x}}_2 + \gamma_1\omega_o(y_m - \hat{x}_1) \\ \dot{\hat{\bar{x}}}_2 &= -a\hat{\bar{x}}_2 + \hat{\bar{\vartheta}}_1 + bu + \bar{\gamma}_1\omega_o^2(y_m - \hat{x}_1), \end{cases} \\ \Pi_2 :&= \begin{cases} \dot{\hat{x}}_2 &= -a\hat{x}_2 + \hat{\bar{\vartheta}}_1 + bu + \gamma_2\omega_o(\hat{\bar{x}}_2 - \hat{x}_2) \\ \dot{\hat{\bar{\vartheta}}}_1 &= \hat{\bar{\vartheta}}_2 + \bar{\gamma}_2\omega_o^2(\hat{\bar{x}}_2 - \hat{x}_2), \end{cases} \\ \Pi_3 :&= \begin{cases} \dot{\hat{\vartheta}}_1 &= \hat{\bar{\vartheta}}_2 + \gamma_3\omega_o(\hat{\bar{\vartheta}}_1 - \hat{\vartheta}_1) \\ \dot{\hat{\bar{\vartheta}}}_2 &= \bar{\gamma}_3\omega_o^2(\hat{\bar{\vartheta}}_1 - \hat{\vartheta}_1), \end{cases} \end{aligned} \tag{24}$$

where $\hat{\bar{x}}_2, \hat{\bar{\vartheta}}_1$ act as reference signal for sub-blocks Π_2, Π_3 and $\gamma_i, \bar{\gamma}_i, (i = 1 \text{ to } 3)$ denote observer parameters.

Introducing estimation error vector as $\boldsymbol{e_\chi} := \boldsymbol{\chi} - \hat{\boldsymbol{\chi}}$ where $\hat{\boldsymbol{\chi}} := [\hat{\boldsymbol{\chi}}_{\mathbf{1}}^T, \hat{\boldsymbol{\chi}}_{\mathbf{2}}^T, \hat{\boldsymbol{\chi}}_{\mathbf{3}}^T]^T$, $\hat{\boldsymbol{\chi}}_{\mathbf{1}} := [\hat{x}_1,\ \hat{\bar{x}}_2]^T$, $\hat{\boldsymbol{\chi}}_{\mathbf{2}} := [\hat{x}_2,\ \hat{\bar{\vartheta}}_1]^T$, $\hat{\boldsymbol{\chi}}_{\mathbf{3}} := [\hat{\vartheta}_1,\ \hat{\bar{\vartheta}}_2]^T$, $\boldsymbol{\chi} = [x_1, x_2, x_2, \vartheta_1, \vartheta_1, \vartheta_2]^T$, we obtain error dynamics as

$$\dot{\boldsymbol{e}}_{\boldsymbol{\chi}} = \boldsymbol{A}_{\boldsymbol{\chi}}\boldsymbol{\chi} + \boldsymbol{\Phi}_{\boldsymbol{x}}(\boldsymbol{\chi}) + \boldsymbol{\mathcal{H}}g - \boldsymbol{\mathcal{F}}\nu, \tag{25}$$

where $\boldsymbol{\mathcal{F}} = [\gamma_1\omega_o, \bar{\gamma}_1\omega_o^2, \mathbf{0}_{1\times4}]^T$, $\boldsymbol{\mathcal{H}} = [\mathbf{0}_{1\times5}, 1]^T$ while error matrix $\boldsymbol{A}_{\boldsymbol{\chi}} = \boldsymbol{\Xi}_{\mathbf{3}}$ can be obtained recursively in the following manner:

$$\begin{aligned} &\boldsymbol{\Xi}_{\mathbf{1}} = \boldsymbol{E}_{\mathbf{1}}, \boldsymbol{\Xi}_{\boldsymbol{i}} = \begin{bmatrix} \boldsymbol{\Xi}_{\boldsymbol{i-1}} & \bar{\boldsymbol{N}}_{\boldsymbol{i}} \\ \bar{\boldsymbol{Q}}_{\boldsymbol{i}} & \boldsymbol{E}_{\boldsymbol{i}} \end{bmatrix}, \boldsymbol{E}_{\boldsymbol{i}} = \begin{bmatrix} -\gamma_i\omega_o & 1 \\ -\bar{\gamma}_i\omega_o^2 & 0 \end{bmatrix}, \\ &\bar{\boldsymbol{N}}_{\boldsymbol{i}} = \begin{bmatrix} \mathbf{0}_{\mathbf{2(i-2)\times2}} \\ \boldsymbol{N} \end{bmatrix}, \bar{\boldsymbol{Q}}_{\boldsymbol{i}} = \begin{bmatrix} \mathbf{0}_{\mathbf{2\times2(i-2)}} & \boldsymbol{Q}_{\boldsymbol{i}} \end{bmatrix}, \\ &\boldsymbol{Q}_{\boldsymbol{i}} = \begin{bmatrix} 0 & \gamma_i\omega_o \\ 0 & \bar{\gamma}_i\omega_o^2 \end{bmatrix}, \boldsymbol{N} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, i = \{2, 3\}, \boldsymbol{\Phi}_{\boldsymbol{x}}(\boldsymbol{\chi}) = \boldsymbol{\phi}_{\boldsymbol{x}}\boldsymbol{\chi}, \\ &\boldsymbol{\phi}_{\boldsymbol{x}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -a & 0 & 0 & 0 & 0 \\ 0 & 0 & -a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \end{aligned} \tag{26}$$

The eigen values of $\boldsymbol{A}_{\boldsymbol{\chi}}$ can be placed at $-\omega_o$ by selecting $\gamma_i = 2,\ i = \{1, 2, 3\}$, $\bar{\gamma}_1 = 3, \bar{\gamma}_2 = 1$ and $\bar{\gamma}_3 = \frac{1}{3}$, based on the concept of bandwidth parameterization. Such a selection also reduces the number of tuning parameters to unity and facilitates practical implementation. It is also worth noting that LHESO avoids the gain escalation problem which plagues high-gain observers (including ESO and CESO) and leads to numerical implementation complexity on fixed point digital signal processors by using gains that grow only up to ω_o^2 [19], [20].

Similar to the case of CESO, the error vector $\boldsymbol{e_\chi}$ is scaled in order to illustrate the effect of observer bandwidth on estimation error by using the transformation

$$\boldsymbol{e}_{\boldsymbol{\chi}} \rightarrow \boldsymbol{\zeta} := \boldsymbol{\mathcal{D}}\boldsymbol{e}_{\boldsymbol{\chi}}, \tag{27}$$

where $\boldsymbol{\mathcal{D}}$:=blkdiag$(\boldsymbol{\mathcal{D}_1}, \boldsymbol{\mathcal{D}_2}, \boldsymbol{\mathcal{D}_3})$ and $\boldsymbol{\mathcal{D}_i}$:=diag$(\omega_o^{-(i-1)}, \omega_o^{-i})$. Applying the preceding transformation on (25) gives

$$\begin{aligned} \dot{\boldsymbol{\zeta}} &= \boldsymbol{\mathcal{D}}\boldsymbol{A}_{\boldsymbol{\chi}}\boldsymbol{\mathcal{D}}^{-1}\boldsymbol{\zeta} + \boldsymbol{\mathcal{D}}\boldsymbol{\Phi}_{\boldsymbol{x}}(\boldsymbol{\chi}) + \boldsymbol{\mathcal{D}}\boldsymbol{\mathcal{H}}g - \boldsymbol{\mathcal{D}}\boldsymbol{\mathcal{F}}\nu \\ &= \omega_o\boldsymbol{\Pi}_{\boldsymbol{\chi}}\boldsymbol{\zeta} + \boldsymbol{\delta}_{\boldsymbol{\chi}} + \omega_o^{-3}\boldsymbol{\mathcal{H}}g - \omega_o\bar{\boldsymbol{\mathcal{F}}}\nu, \end{aligned} \tag{28}$$

where $\text{eig}(\boldsymbol{\Pi}_{\boldsymbol{\chi}}) = \{-1, -1, -1, -1, -1, -1\}$, and $\bar{\boldsymbol{\mathcal{F}}} = [\gamma_1, \bar{\gamma}_1, \mathbf{0}_{1\times2m}]^T$ and $\|\boldsymbol{\delta}_{\boldsymbol{\chi}}\| \leq \mu_{\boldsymbol{\chi}}\|\boldsymbol{\zeta}\|$.

C. Stability Analysis

In addition to ***Assumption 2*** which places a bound on measurement noise, following assumption is made on the disturbance ϑ in order to ensure the input-to-state stability of LHESO:

Assumption 3: *Second derivative of attack signal given by $\ddot{\vartheta} = g$ is bounded in the sense $|g| \leq \mu_3$, where $\mu_3 > 0$.*

***Remark 4*:** Although the time polynomial type disturbance model for $m = 2$ assumes $d^2\vartheta/dt^2 = g = 0$, the exact nature of FDIA on the system is mostly unknown. Hence, a generalised assumption of g being bounded is more practical and is used in the present study to show the convergence of LHESO.

We define a Lyapunov function

$$V = \boldsymbol{\zeta}^{\boldsymbol{T}}\boldsymbol{P}\boldsymbol{\zeta} \tag{29}$$

where $\boldsymbol{P}$ is a symmetric positive definite matrix that satisfies $\boldsymbol{P\Pi_\chi} + \boldsymbol{\Pi_\chi^T P} = -\boldsymbol{I}$. Taking derivative of V along (28), results in

$$\begin{aligned}\dot{V} \leq & -\omega_o\|\boldsymbol{\zeta}\|^2 + 2\|\boldsymbol{P}\|\|\boldsymbol{\delta_\chi}\|\|\boldsymbol{\zeta}\| + 2\omega_o^{-3}\|\boldsymbol{P}\|\|\boldsymbol{\zeta}\||g| \\ & + 2\omega_o\|\boldsymbol{P}\|\|\bar{\boldsymbol{\mathcal{F}}}\|\|\boldsymbol{\zeta}\||\nu|, \\ \leq & -\omega_o\|\boldsymbol{\zeta}\|^2 + 2\|\boldsymbol{P}\|\|\boldsymbol{\zeta}\|^2\mu_{\boldsymbol{\chi}} + 2\omega_o^{-3}\|\boldsymbol{P}\|\|\boldsymbol{\zeta}\|\mu_3 \\ & + 2\omega_o\|\boldsymbol{P}\|\|\bar{\boldsymbol{\mathcal{F}}}\|\|\boldsymbol{\zeta}\|\mu_2.\end{aligned} \tag{30}$$

For $\omega_o \geq 4\|\boldsymbol{P}\|\mu_{\boldsymbol{\chi}}$,

$$\dot{V} \leq -\frac{1}{2}\omega_o\|\boldsymbol{\zeta}\|^2 + 2\omega_o^{-3}\|\boldsymbol{P}\|\|\boldsymbol{\zeta}\|\mu_3 + 2\omega_o\|\boldsymbol{P}\|\|\bar{\boldsymbol{\mathcal{F}}}\|\|\boldsymbol{\zeta}\|\mu_2. \tag{31}$$

Therefore,

$$\dot{V} \leq -\frac{1}{4}\omega_o\|\boldsymbol{\zeta}\|^2, \forall\|\boldsymbol{\zeta}\| \geq 8(\omega_0^{-4}\|\boldsymbol{P}\|\mu_3 + \|\boldsymbol{P}\|\|\bar{\boldsymbol{\mathcal{F}}}\|\mu_2) \tag{32}$$

which implies that

$$\lim_{t\to\infty}\|\boldsymbol{\zeta}(t)\| \leq \omega_o^{-4}\kappa_3\mu_3 + \kappa_4\mu_2, \tag{33}$$

where κ_3, κ_4 are positive constants [19]. Assuming $\omega_o \geq 1$ gives $\omega_o^{-3}\|\boldsymbol{e_\chi}\| \leq \|\boldsymbol{\zeta}\| \leq \|\boldsymbol{e_\chi}\|$ from (27) which results in the following bound for $\|\boldsymbol{e_\chi}\|$:

$$\lim_{t\to\infty}\|\boldsymbol{e_\chi}(t)\| \leq \omega_o^{-1}\kappa_3\mu_3 + \omega_o^3\kappa_4\mu_2. \tag{34}$$

Since the actual estimation error vector $(\boldsymbol{e})$ is a sub-vector of $\boldsymbol{e_\chi}$, it can be written that $\|\boldsymbol{e}\| \leq \|\boldsymbol{e_\chi}\|$ which means

$$\lim_{t\to\infty}\|\boldsymbol{e}(t)\| \leq \omega_o^{-1}\kappa_3\mu_3 + \omega_o^3\kappa_4\mu_2. \tag{35}$$

The aforementioned inequality presents a similar compromise between disturbance rejection and noise attenuation and a straightforward comparison of the noise dependent terms in the inequalities (6) and (35) might indicate that noise amplification is more prominent in LHESO i.e. $\mathcal{O}(\omega_o^3)$, due to the inclusion of an extra augmented state. However, the bounds obtained in terms of measurement noise in both the inequalities is conservative in the sense that the frequency content of the noise signal is not taken into consideration. Particularly for $\tilde{\vartheta}$, it can be shown using frequency domain analysis that the relative degree with respect to measurement noise is unity in case of LESO as well as CESO and 3 in case of LHESO [26]. Therefore, LHESO results in better noise suppression in the high frequency range compared to LESO and CESO.

***Remark 5*:** Design of LHESO based on the disturbance model in (22) is in contrast to the assumption in LESO and NESO that the disturbance is constant in steady state and hence, results in better estimation of time-varying attack signals. In particular, LHESO results in the asymptotic convergence of estimation error to zero for ramp attack signals, in the absence of measurement noise as is evident from (35).

VI. Numerical Analysis

Numerical simulations were performed in Simulink/MATLAB environment using a fixed step-size of 1 ms and ode4 Runge-Kutta solver. In order to simulate the effect of sensor noise ν, a high frequency noise signal was generated by passing a band-limited white noise having noise power 2×10^{-8} and maximum frequency content of 500 Hz, through an 8^{th} order high-pass Butterworth filter having a pass-band edge frequency of $f_H = 200\ rad/s$. Parameters of the servo motor in simulation were selected in accordance with the ones identified for QUANSER Rotary Servo platform SRV02, shown in Fig. 2, using sinusoidal signals and are given as $a = 29.07$ and $b = 47.01$. In order to regulate the position of the servo platform, a proportional derivative controller with a derivative filter of the form

$$C_{PD}(s) = K_c\frac{1+\tau_D s}{1+T_f s}, \tag{36}$$

was implemented with controller parameters selected as $K_c = 21.153, \tau_D = 0.034$, and $T_f = 0.018$. Furthermore, a unit step reference signal was applied on the closed-loop system via a set-point filter of the form $F_{SP}(s) = \frac{1}{0.2s+1}$. The control signal was saturated outside the range of ± 10 units in order to accommodate the effects of actuator limitations.

The estimator parameters used in the present study are listed in Table I and are selected so as to have the same bandwidth for all the estimators in order to have a fair comparison. It is to be noted that the observer parameters selected for LESO, CESO, and LHESO in Table I do not place the observer poles at $-\omega_o$ due to the deviation of considered model from pure

TABLE I: Estimator parameters used in the numerical study

	Estimator Parameters
NESO	$\omega_o = 100rad/s, \beta_1 = 3\omega_o, \beta_2 = \frac{3\omega_o^2}{5}, \beta_3 = \frac{\omega_o^3}{9}, \delta = 0.01, \alpha_i = 1/2^{i-1}$
LESO	$\omega_o = 100rad/s, \beta_1 = 3\omega_o, \beta_2 = 3\omega_o^2, \beta_3 = \omega_o^3$
CESO	$\omega_{o1} = 50rad/s,\ \omega_{o2} = 100rad/s, l_{i,1} = 3\omega_{oi}, l_{i,2} = 3\omega_{oi}^2, l_{i,3} = \omega_{oi}^3, i = \{1,2\}$
LHESO	$\omega_o = 100rad/s, \bar{\gamma}_1 = 3, \bar{\gamma}_2 = 1, \bar{\gamma}_3 = 1/3, \gamma_1 = \gamma_2 = \gamma_3 = 2$

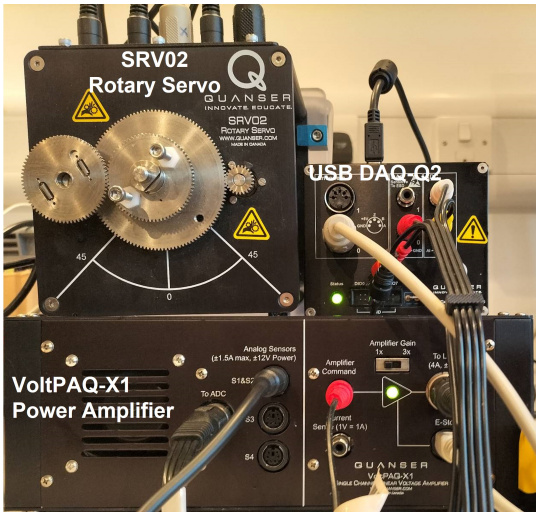


Fig. 2: QUANSER Rotary Servo unit SRV02 used in the experimental study.

integrating structure, however, the resulting structure is stable nonetheless as the poles are located in the left half of the s-plane. As mentioned earlier in ***Remark 1***, the deviation from prime form or pure integrating structure in the form of "$\mathbf{\Phi}$" in CESO and "$\mathbf{\Phi_x}$" in LHESO manifests in the form of a lower bound in the observer bandwidth in order to ensure stability and that the estimation error bounds given in (21) and (35). Therefore, if ω_o is selected high enough i.e. $\omega_o \geq \omega_o^*$, then the stability of the estimators is satisfied. It is also worth noticing that the observer gains to be implemented (as shown in Table I) escalate to $\mathcal{O}(\omega_o^3)$ for all the ESOs except LHESO, where it only grows up to $\mathcal{O}(\omega_o^2)$. This in turn facilitates practical implementation of LHESO based estimator on low cost DSP processors having finite word length.

Following type of attack signals are considered for evaluating the efficacy of the designed estimators:

S1: ***Bias Attack*** is characterized by a constant attack signal where the adversary adds a constant value (ρ_1) to the control signal in the attack duration and is given by

$$\Delta u(t) = \begin{cases} \rho_1, & t \in (t_i, t_f) \\ 0, & \text{otherwise.} \end{cases} \tag{37}$$

The magnitude of bias attack was considered as 5 units and starts at $t_i = 5s$.

S2: ***Ramp Attack*** is represented by a continuously increasing signal that rises with a constant slope (ρ_2) and is expressed as

$$\Delta u(t) = \begin{cases} \rho_2 \cdot (t - t_i), & t \in (t_i, t_f) \\ 0, & \text{otherwise.} \end{cases} \tag{38}$$

A slope of 0.25 units per second is used to simulate the effect of ramp type attack signal which starts at the time instance $t_i = 5s$.

S3: ***Geometric Attack*** starts by slowly drifting the control signal from its actual value and maximizes the damage towards the end of the attack. Such types of attacks are expressed in the following manner:

$$\Delta u(t) = \begin{cases} \rho_3 \cdot \rho_4^{(t-t_i)}, & t \in (t_i, t_f) \\ 0, & \text{otherwise,} \end{cases} \tag{39}$$

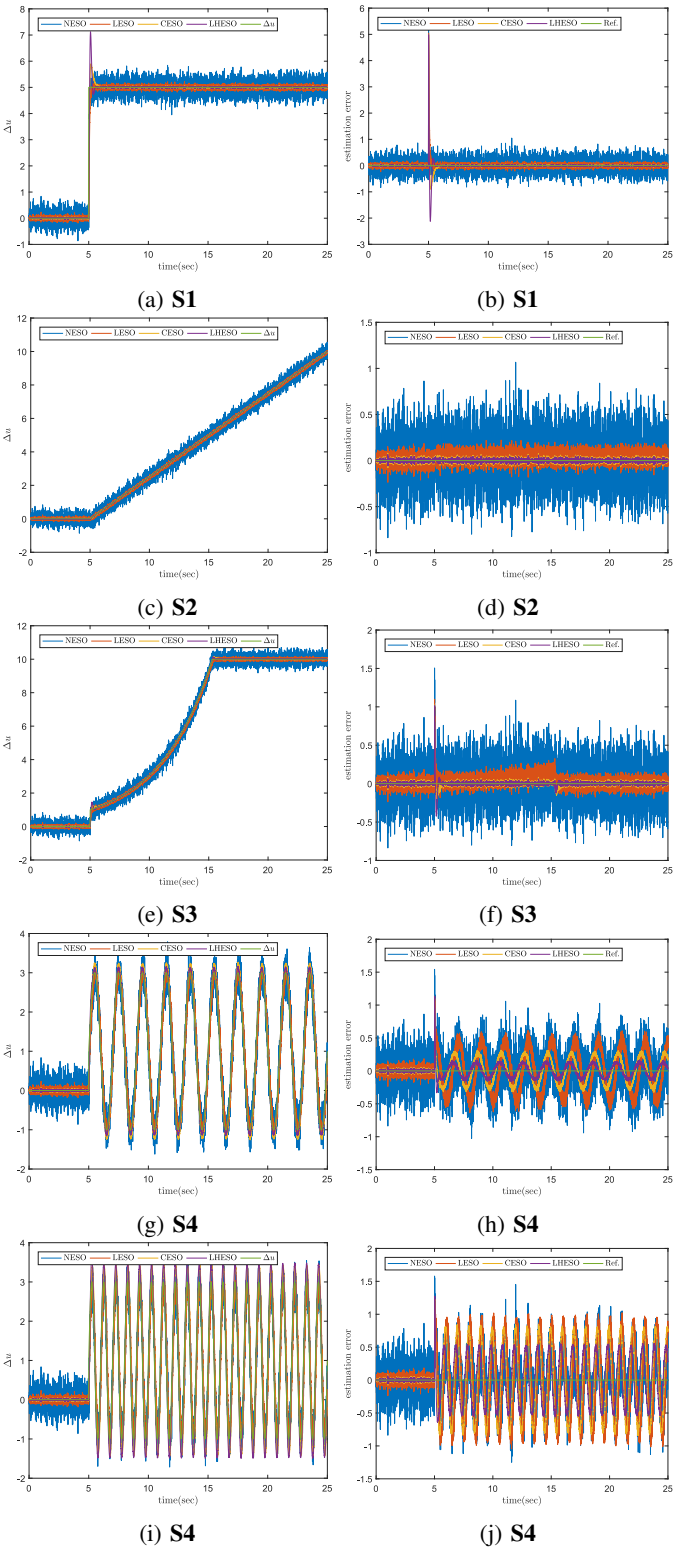
where $\rho_3 = 1,\ \rho_4 = 1.25,\ t_i = 5s$ are selected for simulation study.

S4: ***Sinusoidal Attack*** is represented using the following expression:

$$\Delta u(t) = \begin{cases} \rho_5 \sin\left(2\pi f(t - t_i)\right) + \rho_6, & t \in (t_i, t_f) \\ 0, & \text{otherwise,} \end{cases} \tag{40}$$

where ρ_5, ρ_6, f denote the amplitude, bias, frequency, respectively, and were selected as $\rho_5 = 2, \rho_6 = 3, f = \{0.5, 1\}$ Hz, to evaluate the estimation performance of different ESOs.

Simulation results for attack scenarios **S1** to **S4** are shown in Fig. 3. It is observed that LHESO and CESO are able to ensure better estimation accuracy despite the noisy measurement. Particularly in case of fast time-varying attack signals considered in **S3** and **S4**, LHESO and CESO result



(a) **S1** (b) **S1**

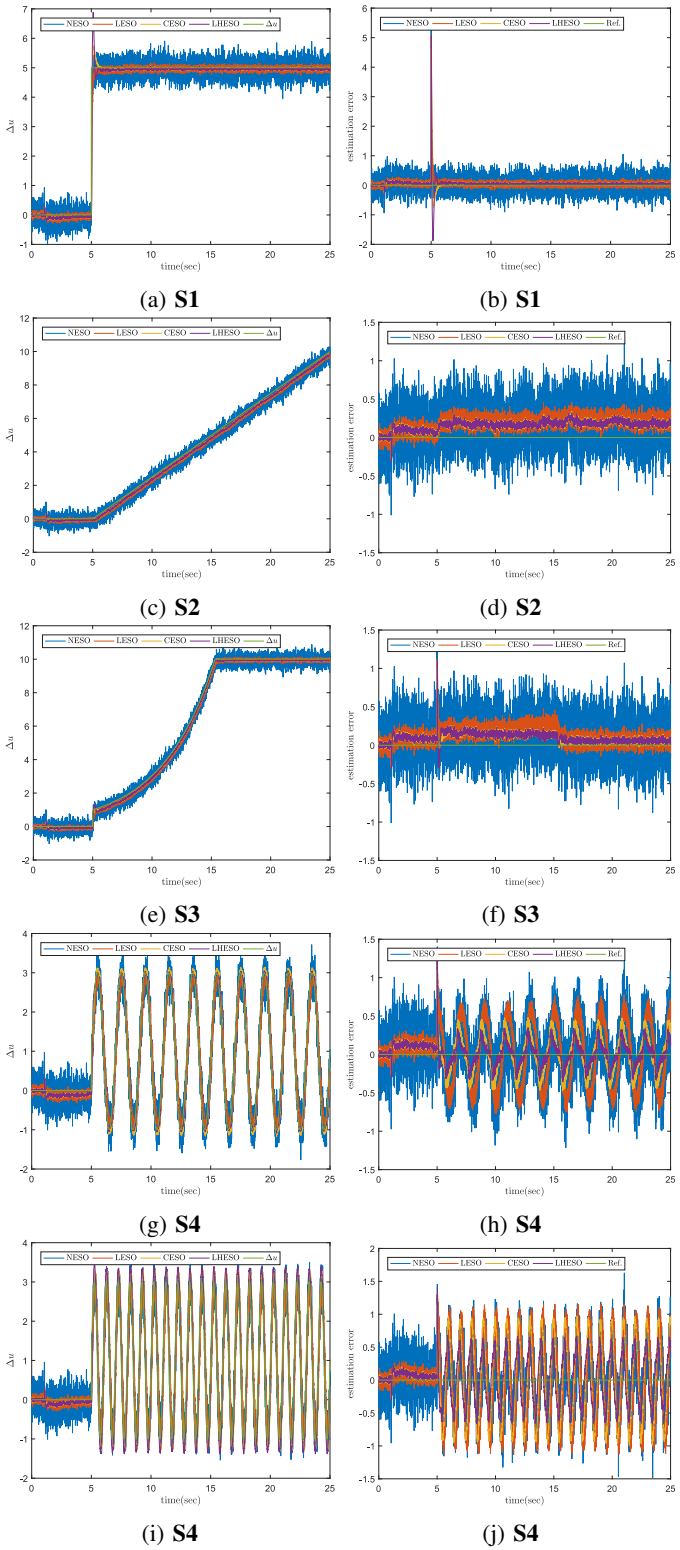
(c) **S2** (d) **S2**

(e) **S3** (f) **S3**

(g) **S4** (h) **S4**

(i) **S4** (j) **S4**

Fig. 3: Simulation plots for attack signal estimate (left) and estimation error (right) under scenarios **S1**, **S2**, **S3** and **S4**.



(a) **S1** (b) **S1**

(c) **S2** (d) **S2**

(e) **S3** (f) **S3**

(g) **S4** (h) **S4**

(i) **S4** (j) **S4**

Fig. 4: Experimental plots for attack signal estimate (left) and estimation error (right) under scenarios **S1**, **S2**, **S3** and **S4**.

in significantly lower estimation error compared to LESO and NESO, with LHESO being more accurate (lower peak-to-peak error amplitude in **S4** and **S3**) and having lower noise content among the two due to a higher relative degree (3 as opposed to 1 in case of CESO). In case of fast sinusoidal attack signals (Fig. 3g, 3h, 3i, 3j), LHESO exhibits significantly improved performance compared to CESO despite having the same tuning parameters. Furthermore, large oscillations can be observed in FDIA estimate as well as estimation error plots in Fig. 3 for NESO which is due to the small error high gain feature implemented via $fal(\cdot)$ function and leads to the over-amplification of measurement noise. Based on this observation, it can be expected that the estimates obtained from NESO will almost always be more corrupted by high frequency sensor noise as compared to comparatively tuned LESO, CESO and LHESO.

***Remark 6*:** The structure of NESO is designed to amplify the effect of estimation error near the origin by increasing the equivalent gain of the $fal(\cdot)$ function (in the range $[-\delta, \delta]$) in order to enhance the convergence speed, which consequently amplifies the noise content as well. Furthermore, the opposite approach is usually employed while designing noise suppressing switched observers where the gain of the nonlinear/switching function decreases near the origin to minimise the effect the of measurement noise. In some cases, it is also desirable to implement event-triggered error injection term so that the gain becomes zero in a narrow band close to the origin and remains non-zero outside this range. Such techniques are also desirable to minimise the communication burden of the channel. However, this compromise between faster convergence speed and noise amplification is to be expected and is always encountered while designing state or disturbance observers. In our study, we attempt to illustrate that this compromise is relaxed by using a combination of higher-order state augmentations along with additional low-pass filtering which manifests in the form of higher relative degree between the estimates and measurement noise.

VII. Experimental Validation

Simulation results obtained in the previous section were further validated on a QUANSER Rotary Servo platform SRV02 shown in Fig. 2, using the same estimator and closed-loop proportional derivative controller parameters. The attack signals (Δu) were applied on the actuator side inside Simulink in order to simulate the effect of FDIA. The sampling time and solver settings were kept the same as that of simulation study. The experimental results obtained for all the ESOs under different test scenarios are shown in Fig. 4. It can be observed that the experimental results follow a similar pattern to that of simulation plots obtained in Fig. 3 and closely resemble their corresponding simulation counterparts. Similar to the simulation study, CESO and LHESO result in comparable estimation error in case of bias and ramp type attack signals under scenarios **S1** and **S2**, but with much better noise attenuation in the estimates. This in turn results in smaller peak-to-peak oscillations in the estimation error plots obtained in Fig. 4b

and 4d. Furthermore, in case of fast time-varying attack signals under scenarios **S3**, **S4** and **S5**, the improvement in estimation quality is more significant and results in lower estimation error for CESO and LHESO compared to LESO. Among the noise suppressing ESOs, LHESO exhibits better performance compared to CESO due to its inherent structural properties that manifest in the form of higher relative degree between the attack signal estimate and measurement noise. Therefore, LHESO exhibits better noise suppression compared to CESO. Furthermore, the tuning approach for LHESO enables us to place all the observer poles at the same location (for a pure integrating structure) in contrast to the virtual decomposition approach in CESO which requires selection of progressively increasing bandwidths for ESO in each level. For NESO, the oscillations due to noise over-amplification is quite significant which degrades the quality of the obtained estimate, which again is a direct consequence of the small error high gain feature associated with $fal(\cdot)$ function. It is also observed that the estimation error in case of experimental plots is slightly higher compared to the simulation results, which is to be expected.

VIII. Conclusion

An ESO based actuator FDIA signal estimation approach was investigated in this paper. Through simulation and experimental studies performed on a motion control platform, it was demonstrated that CESO and LHESO present a much better alternative to conventional linear and nonlinear ESO structures in terms of accuracy while estimating time-varying FDIA signals as well as suppressing the effect of high-frequency measurement noise on the obtained estimates. In particular, it was shown that LHESO yields the best estimation performance while simultaneously addressing the numerical issue that restricts implementation of high-gain observers on fixed-point digital signal processors. Using the structure of noise suppressing ESOs as a base, it would be interesting to explore a combination of these techniques so as to leverage the benefits of each. It would also be interesting to integrate switched gain and event-triggered estimation approaches to these ESOs in order to obtain further performance improvement.

Acknowledgment

The authors greatly acknowledge the help and support of Dr. Andrew Pike, Coventry University, U.K., in conducting the experiment reported in this paper.

References

[1] Zhao, Y.B., Sun, X.M., Zhang, J. and Shi, P., 2015. Networked control systems: The communication basics and control methodologies. Mathematical Problems in Engineering.

[2] Zhang, D., Wang, Q.G., Feng, G., Shi, Y. and Vasilakos, A.V., 2021. A survey on attack detection, estimation and control of industrial cyber-physical systems. ISA Transactions, 116, pp.1-16.

[3] Manson, S. and Anderson, D., 2019. Cybersecurity for protection and control systems: An overview of proven design solutions. IEEE Industry Applications Magazine, 25(4), pp.14-23.

[4] Kumar, M. 2023. Resilient PIDA Control Design Based Frequency Regulation of Interconnected Time-Delayed Microgrid Under Cyber-Attacks, IEEE Transactions on Industry Applications, vol. 59, no. 1, pp. 492-502.

[5] Priyanga S, P., Krithivasan, K., Pravinraj, S., and Sriram V., S., S., 2020. Detection of Cyberattacks in Industrial Control Systems Using Enhanced Principal Component Analysis and Hypergraph-Based Convolution Neural Network (EPCA-HG-CNN), IEEE Transactions on Industry Applications, vol. 56, no. 4, pp. 4394-4404.

[6] Falliere N, Murchu LO, Chien E. W32.stuxnet dossier. 2011, url- https://www.symantec.com/content/en/us/enterprise/media/securityresponse/whitepapers/w32-stuxnet-dossier.pdf.

[7] H. Sandberg, S. Amin, and K. H. Johansson, Cyberphysical security in networked control systems: An introduction to the issue, IEEE Control Systems Magazine, vol. 35, no. 1, pp. 20-23, Feb. 2015.

[8] How to Compromise PLC Systems via Stealthy Pin Control Attacks. url- https://securityaffairs.co/wordpress/53069/hacking/plcattacks.html.

[9] Cecilia, A., Sahoo, S., Dragicevic, T., Costa-Castello, R. and Blaabjerg, F., 2021. On Addressing the Security and Stability Issues Due to False Data Injection Attacks in DC Microgrids- An Adaptive Observer Approach. IEEE Transactions on Power Electronics.

[10] Chen, G., Zhang, Y., Gu, S. and Hu, W., 2021. Resilient State Estimation and Control of Cyber-Physical Systems Against False Data Injection Attacks on Both Actuator and Sensors. IEEE Transactions on Control of Network Systems.

[11] Ma, R., Basumallik, S., Eftekharnejad, S. and Kong, F., 2021. A data-driven model predictive control for alleviating thermal overloads in the presence of possible false data. IEEE Transactions on Industry Applications, 57(2), pp.1872-1881.

[12] Siu, J.Y., Kumar, N. and Panda, S.K., 2022. Command Authentication Using Multiagent System for Attacks on the Economic Dispatch Problem. IEEE Transactions on Industry Applications, 58(4), pp.4381-4393.

[13] Hu, Y., Yang, A., Li, H., Sun, Y. and Sun, L., 2018. A survey of intrusion detection on industrial control systems. International Journal of Distributed Sensor Networks, 14(8), p.1550147718794615.

[14] Cecilia, A., Sahoo, S., Dragicevic, T., Costa-Castello, R. and Blaabjerg, F., 2021. Detection and Mitigation of False Data in Cooperative DC Microgrids With Unknown Constant Power Loads. IEEE Transactions on Power Electronics, 36(8), pp.9565-9577.

[15] Yang, T., Murguia, C., Kuijper, M. and Nesic, D., 2019, June. An unknown input multi-observer approach for estimation, attack isolation, and control of LTI systems under actuator attacks. In 2019 18th European Control Conference (ECC) (pp. 4350-4355). IEEE.

[16] Miao, K., Shi, X. and Zhang, W.A., 2020. Attack signal estimation for intrusion detection in industrial control system. Computers & Security, 96, p.101926.

[17] Lakomy, K. and Madonski, R., 2021. Cascade extended state observer for active disturbance rejection control applications under measurement noise. ISA transactions, 109, pp.1-10.

[18] Lakomy, K., Madonski, R., Dai, B., Yang, J., Kicki, P., Ansari, M. and Li, S., 2021. Active disturbance rejection control design with suppression of sensor noise effects in application to DC-DC buck power converter. IEEE Transactions on Industrial Electronics, 69(1), pp.816-824.

[19] Ahmad, S. and Ali, A., 2021. On active disturbance rejection control in presence of measurement noise. IEEE Transactions on Industrial Electronics, 69(11), pp.11600-11610.

[20] Astolfi, D. and Marconi, L., 2015. A high-gain nonlinear observer with limited gain power. IEEE Transactions on Automatic Control, 60(11), pp.3059-3064.

[21] Astolfi, D., Marconi, L., Praly, L. and Teel, A.R., 2018. Low-power peaking-free high-gain observers. Automatica, 98, pp.169-179.

[22] Ahmad, S. and Ahmed, H., 2022. Robust Intrusion Detection for Resilience Enhancement of Industrial Control Systems: An Extended State Observer Approach. IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, pp. 1-6.

[23] Li, J., Xia, Y., Qi, X. and Gao, Z., 2016. On the necessity, scheme, and basis of the linear-nonlinear switching in active disturbance rejection control. IEEE Transactions on Industrial Electronics, 64(2), pp.1425-1435.

[24] Gao, Z., 2002. From linear to nonlinear control means: A practical progression. ISA transactions, 41(2), pp.177-189.

[25] Gao, Z., 2006, June. Scaling and bandwidth-parameterization based controller tuning. In Proceedings of the American control conference (Vol. 6, pp. 4989-4996).

[26] Khalil, H.K., 2017. High-gain observers in nonlinear feedback control. Society for Industrial and Applied Mathematics.

[27] Sira-Ramirez, H., 2018. From flatness, GPI observers, GPI control and flat filters to observer-based ADRC. Control Theory and Technology, 16(4), pp.249-260.

Saif Ahmad received his B.Tech degree in electrical engineering from National Institute of Technology Patna, India, in 2014 and Ph.D. in electrical engineering from Indian Institute of Technology Patna, India, in 2021. He is currently a postdoc researcher at LAPLACE laboratory (CNRS UMR 5213), INP-ENSEEIHT, Toulouse, France. His research interests include disturbance estimation-based control, robust control of power converters, EV charging, energy management and optimization in network of renewable energy systems.

Hafiz Ahmed (Senior Member, IEEE) received Ph.D. degree in Control Engineering from the University of Lille 1, Lille, France, in 2016. From 2016 to 2023, he was with Clemson University, USA; Asia Pacific University, Bangladesh; North South University, Bangladesh; Coventry University, U.K.; Birmingham City University, U.K.; and Bangor University, U.K. Since May 2023, he has been with the Nuclear Advanced Manufacturing Research Centre (NAMRC), University of Sheffield, U.K., where he is currently the Head of Group - Controls and Instrumentation. He is interested in applied control engineering with special focus on energy and environment.

Dr. Ahmed was the recipient of the European Embedded Control Institute (EECI) Ph.D. Award in 2017 and the Best Ph.D. Thesis Award from the Research Cluster on Modeling, Analysis, and Management of Dynamic Systems (GDR-MACS) of the National Council of Scientific Research (CNRS) in France in 2017. He is an associate editor for the International Journal of Electrical Engineering Education. He is also actively involved in organizing special issues and sessions at various international journals and conferences.