

PAPER • OPEN ACCESS

## Electromechanical drive fault detection


To cite this article: R Iureva *et al* 2019 *IOP Conf. Ser.: Mater. Sci. Eng.* **643** 012114

View the [article online](#) for updates and enhancements.

You may also like

- [Electromechanical finite element modelling for dynamic analysis of a cantilevered piezoelectric energy harvester with tip mass offset under base excitations](#)  
M F Lumentut and I M Howard
- [Depolarization diagnosis of PWAS used for EMI based structural health monitoring system for composite plates](#)  
Mostafa S Amin and Mohamed A M Salem
- [Tolerance design of electromechanical products based on self-defined approximate model](#)  
J Deng, J M Lai and G F Zhai






The  
Electrochemical  
Society

Advancing solid state &  
electrochemical science & technology

**DISCOVER**  
how sustainability  
intersects with  
electrochemistry & solid  
state science research



# Electromechanical drive fault detection

**R Iureva<sup>1,\*</sup>, A Margun<sup>1</sup>, N Maltseva<sup>1</sup> and K Vedernikov<sup>2</sup>**

<sup>1</sup> ITMO University, Russia, Saint Petersburg

<sup>2</sup> PC “Diakont”, Russia, Saint Petersburg

\* E-mail: raddayurieva@gmail.com

**Abstract.** The paper presents the simulation model for the process of electromechanical drive disorder detection which is used to evaluate the drive reliability. The low efficiency and inoperability of the drive could be partial or complete. A proper functional drive provides under certain conditions the maximum efficiency of its use. The ability of the partially operating object application in the same conditions is less than the maximum possible one, but its indicators could be still within limits established for the proper functioning, which is considered normal. A partially inoperable object could function, and at the same time, its level of efficiency is lower than the allowed one. An inoperable object couldn't be used as it was intended, and the research presented in this paper shows how to enable providing the drive reliability evaluation and analyze its proper functioning.

## 1. Introduction

Intensification of technological processes increases the productivity and accuracy of cyber-physical systems which are inextricably linked to the complication of the overall scheme of automation of production and electric drive particularly. The failure of electric drive could lead to a release of defective products, a decrease in labor productivity, energy losses, stops and sometimes dysfunction of working machines and mechanisms, and as a result to significant economic losses. Under these conditions, the critical problem of ensuring reliable operation of electromechanical drives is put in the forefront. The task of improving the reliability of electric drives is a complicated and complex problem that should be solved both at the stages of design and manufacturing of its components and also during its installation, commissioning, and operation.

Reliability is the property of the electric drive “to preserve in time, within the established limits, the values of all parameters characterizing the ability to perform the required functions in the given modes and conditions of use, maintenance, storage and transportation” [1]. Reliability is a complex property that combines the concepts of efficiency, dependability, durability, maintainability, and safety. Energy is a state of the electric drive in which it can perform its functions.

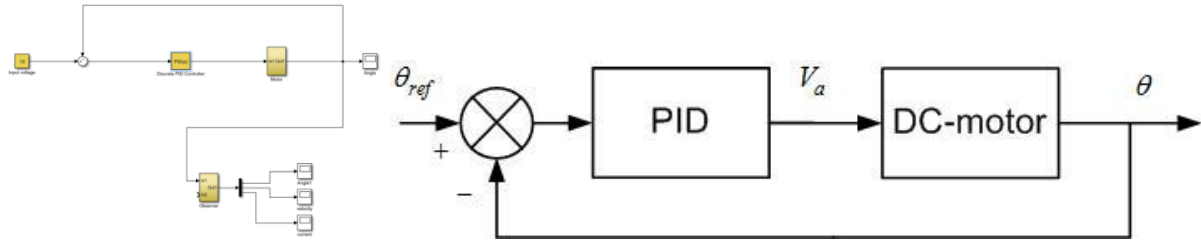
## 2. Simulation model and real electromechanical drive

The proposed electromechanical drive has high efficiency, small dimensions, high load-carrying capacity, and durability, and also has a high accuracy of positioning or turning the output shaft [2-5].

Figure 1 shows a model of a real motor (the continuous model describes valve and DC motors), which measures only the output angle. The engine is controlled by a discrete PID controller and an observer, which has been made for it and allows estimating the current, speed, and position of the engine [6-8].



We also have a discrete virtual model of the engine, for which an observer is also made. If observers have significantly different data, then something goes wrong [9].



**Figure 1.** Model of a real motor.

The actuator is well suited for being modeled by linear differential-algebraic systems. A smaller, but still considerable portion of systems admits a nonsingular linear representation. In this regard, we consider the following linear model for actuator:

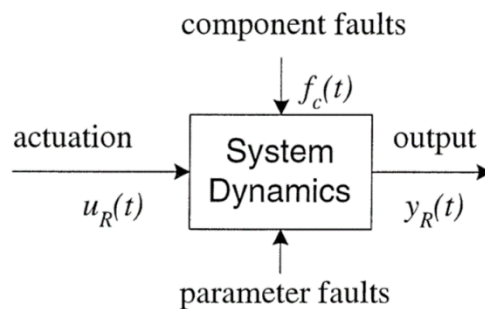
$$\begin{aligned}\dot{x}(t) &= Ax(t) + Bu_R(t) \\ y_R(t) &= Cx(t) + Du_R(t) \\ z_R(t) &= Hx(t) + Eu_R(t)\end{aligned}\tag{1}$$

Where  $x \in R^n$  is the state of the system,  $u \in R^m$  is the control input,  $y \in R^p$  is the measured output and  $z \in R^r$  is the regulated output. It is worth noticing that, in this model, the state  $x$  can include both physical, and cyber variables.

When an impact occurs in a system (see Figure 2), the dynamic model of the system can be described as:

$$\dot{x}(t) = Ax(t) + BU_R(t) + f_c(t)\tag{2}$$

Inputs to the system are supposed to be subject to constraints, such as physical limits for the mechanical inputs or limited bandwidth for digital inputs.



**Figure 2.** System dynamics.

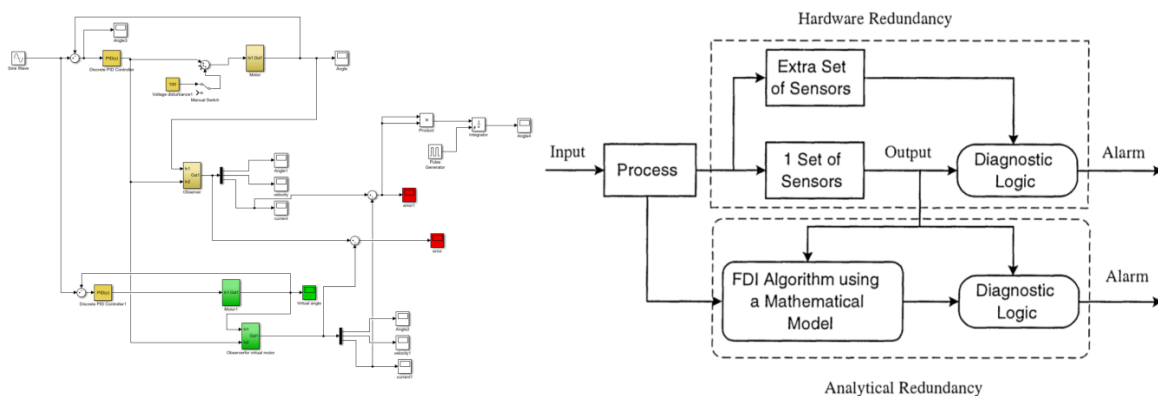
It is necessary to analyze the regularity of the system behavior under adverse conditions.

### 3. Experimental data

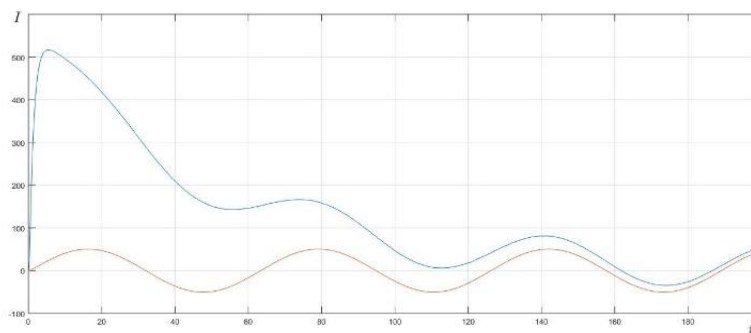
A rather common mistake is to concentrate maximum time efforts on preventing a cyber attack. At the first glance, this may seem to be the explicit goal of any cybersecurity politics. However, the fact that the most successful hacks were not detected within 180 days forces us to change this point of view. That is why an essential part of the cyber security of a motor-reducer is to identify the destructive impact to take measures for the routine work of the system [10-11].

If there is an impact on the motor-reducer, which includes white noise and voltage disturbance, it can be illustrated by Figure 3.

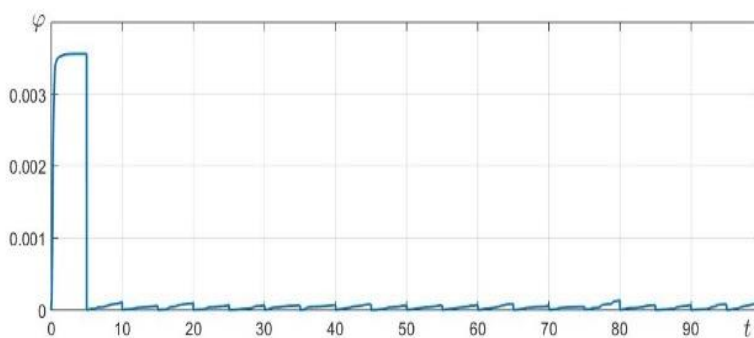
Under the destructive impact, the mismatch between normal mode and mode with devastating impact assumed as voltage disturbance on signal shown in Figure 4. The signal sampling ( $\varphi$ ) is presented in Figure 5, where we can see that PID-controller deals with this kind of impact, and the system switches to working in normal mode [3-5, 12-15].



**Figure 3.** Hardware vs analytical redundancy.



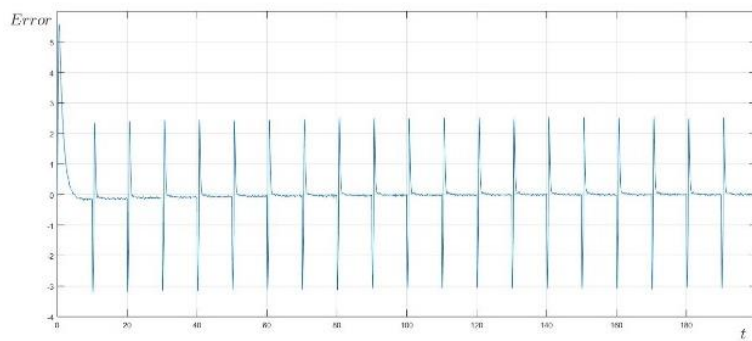
**Figure 4.** Brown line - normal mode of motor-reducer and blue line - mode with impact (voltage disturbance).



**Figure 5.** Signal sampling in conditions of white noise.

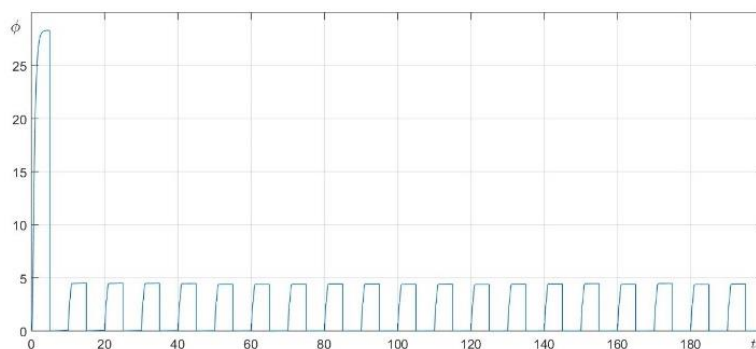
However, the main issue is to know whether it is enough to use PID-controller when the impact is inconstant (Figure 5), where one simulated a kind of impact on actuator feedback transducer in a form of inconstant white noise [16]. The resulting error could be neglected since the error is small. To avoid estimating the accumulated error and making the wrong decision about the presence of an attack, the error was sampled.

With a high level of attack on the control object, the difference between the normal mode and the mode under attack conditions is shown in Figure 6.



**Figure 6.** The mismatch between normal mode and mode with impacts (voltage disturbance and impact on actuator feedback transducer).

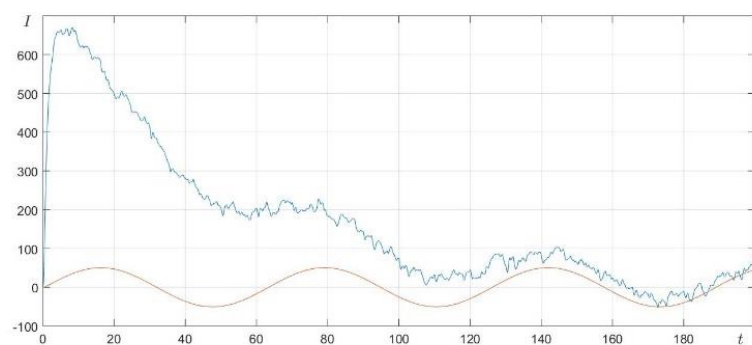
From the sampled signal (Figure 5) and its comparison with Figure 4, one can judge the destructive effect on the system.



**Figure 7.** Signal sampling in conditions of destructive impact on feedback and voltage disturbance.

In these conditions the mismatch between normal mode and studied mode are presented in Fig. 8. A hypothesis that type of attack or location of attack influences the curve can be made.

Nevertheless, the transient response (Figure 2) shows that in course of time the motor-reducer comes to normal mode, although the mismatch happens between the motor in steady-state operating conditions and impact.

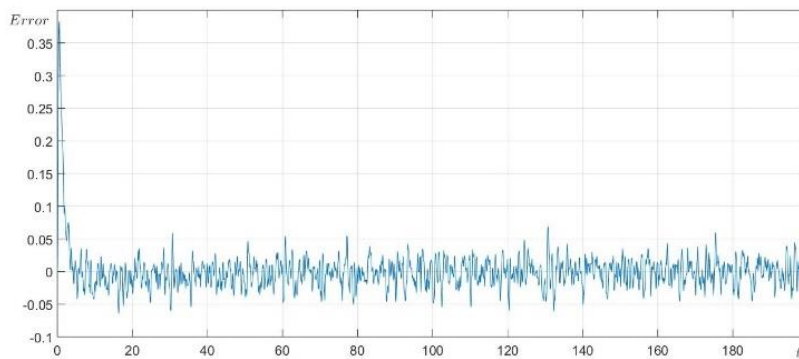


**Figure 8.** Constant attack on feedback with white noise both on system and feedback and also on voltage disturbance.

The comparison of primary attacks can be illustrated by Figures 8-9.

Exceeding the value of current consumed by an electric motor is an indirect cause of its failure, since with increasing current the heat generated by the motor increases, which is spent partly for warming up the surrounding area and partly for the engine heating. Engine heating depends on several factors: the environment, heat transfer, and heat capacity. Heat transfer, in turn, depends on the ambient temperature and the temperature of the engine itself [16-19]. With a small temperature difference between the motor-

reducer and the environment and at the same time with a large amount of energy emitted by the engine, the stator magnetic core, copper winding, housing, and rotor are heated, resulting in intense heating of insulating materials.



**Figure 9.** Comparison between operation modes with white noise constant attack both on system and feedback, and voltage disturbance without attack.

System reliability maintenance, fault detection, and fault-tolerant design techniques play a crucial role in the actuator development. Fault detection technique proposed earlier helps to support system and to make it more reliable. Further this technique can be applied for process control, robotics, manufacturing systems, and power systems [18-21].

#### 4. Conclusion

When analyzing reliability, particularly while choosing the drive reliability indicators, the decision of whether to use it or not (that should be made in case of an object failure) is essential. If the drive restoration after all fails for any reason is considered inexpedient or impracticable (for example, due to the impossibility of interrupting the function performed), then such an object is not recoverable in this situation. Thus, the same purpose, depending on the features or stages of operation, could be considered recoverable or non-recoverable. For example, the meteorological satellite drive at the storage stage refers to the recoverable one, and during the space flight it refers to non-recoverable one.

#### Acknowledgements

This research was supported by the RF Ministry of Education and Science (RF Government resolution №218, April 9, 2010. (R&D project № 03.G25.31.0251 dated April 28, 2017 at ITMO University “Creation of high-tech production of configurable frequency converters for new generation of synchronous precision high-speed high-power electromechanical drives”).

#### References

- [1] Garcia A, Cusido I, Rosero J A, Ortega J A, Romeral L. 2008 Reliable electro-mechanical actuators in aircraft *IEEE Aerospace and Electronic Systems Magazine* **23** 8
- [2] Renna R Chellali and Achard C 2012 Combination of annealing particle filter and belief propagation for 3d upper body tracking *Applied Bionics and Biomechanics* **9**(4) 443-56
- [3] Jie Chen, Patton R J 1999 Robust Model-Based Fault Diagnosis for Dynamic Systems, The International Series on Asian Studies in Computer and Information Science
- [4] Soares C G 2010 Safety and Reliability of Industrial Products, Systems and Structures. London: CRC Press
- [5] Amin S, Litrico X, Sastry S and Bayen A. M 2013 Cyber security of water SCADA systems - Part I: Analysis and experimentation of stealthy deception attacks *IEEE Transactions on Control Systems Technology* **21**(5) 1963-70
- [6] Zirn O, Treib T 1998 Similarity Laws of Serial and Parallel Manipulators for Machina Tools, MOVIC 98 Zürich, Switzerland, 25. – 28. August 1998, Vol. 3, pp. 865-70
- [7] Schmid R. and Ntogramatzidis L 2010 A unified method for the design of nonovershooting linear multivariable state-feedback tracking controllers *Automatica* **46**(2) 312-21

- [8] Makino et al 2006 Development of Active Suspension System Using Electric Linear Motors for Railway Cars. *Proc. 13th Jointed Railway Technology Symposium. Japan Society of Mechanical Engineers* **06-52** 519-22
- [9] Case D. U 2016 Analysis of the cyber attack on the Ukrainian power grid
- [10] Amin S, Litrico X, Sastry S and Bayen A. M 2013 Cyber security of water SCADA systems - Part I: Analysis and experimentation of stealthy deception attacks *IEEE Transactions on Control Systems Technology* **21(5)** 1963-70
- [11] Park M K, Go S J, Lee Y J, Sung K G 2011 Design and Performance Evaluation of Lightweight Dual Arm Robot Featuring Hollow Shaft Servo Assembly *Advanced Science Letters* **4** 1901-07
- [12] Damousis I G, Bakirtzis A G, Dokopoulos P S 2004 A solution to the unit-commitment problem using integer-coded genetic algorithm *IEEE Trans Power Syst* **19(2)** 1165-72
- [13] Kazarlis S A, Bakirtzis A, Petridis V 1996 A genetic algorithm solution to the unit commitment problem *IEEE Trans Power Syst* **11** 83-92
- [14] Carrión M, Arroyo J M 2006 A computationally efficient mixed-integer linear formulation for the thermal unit commitment problem *IEEE Trans Power Syst* **21** 1371-1378
- [15] John Matley, Malika Gandhi, Emily Yoo, Bill Jarmuz and Stefan Peterson 2016 Insuring the future of mobility, Deloitte University Press, May 13, 2016, <https://dupress.deloitte.com/dup-us-en/focus/future-of-mobility/mobility-ecosystem-future-of-auto-insurance.html>
- [16] Filaretov V, Zhirabok A, Zuev A and Protcenko A 2016 Fault identification in nonlinear dynamic systems,” in Proceedings of the 2016 5th International Conference on Systems and Control (ICSC), pp. 273-277, Marrakesh, Morocco, May 2016.
- [17] Viksnin I I, Iureva R A, Komarov I I, Drannik A L 2016 Assessment of Stability of Algorithms Based on Trust and Reputation Model, Proceedings of the 18th Conference of Open Innovations Association FRUCT, pp. 364-369
- [18] Uekura et al 2010 Development of Active Suspension Control System by Actuator of Decreased Air Consumption. *Proc. 17th Jointed Railway Technology Symposium Japan Society of Mechanical Engineers* **S5-1-1** 305-8
- [19] Dobriborsci D, Margun A, Kolyubin S 2018 Theoretical and experimental research of the discrete output robust controller for uncertain plant, 2018 European Control Conference, ECC 2018, pp. 533-8
- [20] Terai A, Abe S, Kojima S, Takano Y and Koshijima I 2017 Cyber- attack detection for industrial control system monitoring with support vector machine based on communication profile, IEEE European Symposium on Security and Privacy Workshops
- [21] Vidal R, Chiuso A, Soatto S and Sastry S 2003 Observability of linear hybrid systems,” International Workshop on Hybrid Systems: Computation and Control, pp. 626-539.