CYBER-PHYSICAL SYSTEMS: REVIEW OF ELECTRICAL DRIVES CASE

Nikonenko Y., M.S., PhD student, assistant, Peresada S., Sc.D., professor
Igor Sikorsky Kyiv Polytechnic Institute, Automation of Electromechanical Systems and Electrical Drives department

Introduction. All modern industrial systems and variety of generally used power systems can be considered as Cyber-Physical Systems (CPS). They consist of a physical system (grid, power transmission, electric vehicles, industrial and home (personal) applications etc.) and a cyber system (which include control algorithms, data acquisition, tracing, processing, programming and interactive features). Applications of CPS are often associated with but not limited to core infrastructures and sensitive data. Therefore it makes them attractive in terms of vulnerability, data breach, and denial of services [1].

Electrical drives play the key role in all major industry, transport applications and home appliances. However, it’s effect on stability of integrated systems (part of technological process, or device), reliability properties with respect to different types of cyber-attacks, prevention and mitigation techniques are under development [2].

Motivation of ongoing research of CPS is to develop precautions methods, diagnostics, mitigation and cyber-attack prevention methods for the most critical and network-connected systems. Some examples of major cyber-attacks and their consequences worldwide can be found in [3].

Recent reviews about cybersecurity in different power systems are given in [2], [3], [5]. Examples of cyber-attack-mitigation techniques designed for automated electric vehicles can be found in [6] – [9]. Several approaches on detection and mitigation of cyber-attacks on sensors data and key parts of control algorithms for electrical drives are presented in [10] – [14].

The aim of this paper is to highlight the role of the electrical drives as a part of the CPS and to stress the CPS features which are crucial for the electrical drives applications.

Cyber-attacks types on electrical drives’ side. The main types of cyber-attacks on power systems are targeting [4]: 1) sensors and actuators data; 2) computing systems (controller); 3) feedback signals; 4) communication with higher level systems. Independently on the targeting area, the aim of basic cyber-attacks on electrical drives can be with a focus on either electrical part (power/energy spikes) or mechanical part (mechanical damage), or both [10]. In the latter case the negative impact is usually lesser than if aiming one of the electrical drives’ subsystems.

Basic cyber-attacks on the electrical drives control systems include: spoofing of sensor data, variation of motor parameters, PWM characteristics and protection levels, as well as in-depth viruses that alter all the control system.

Moreover the physical damage caused by mechanisms and electrical power (energy) consumption can be provided very rapidly with momentarily results, or very slowly with gradually increasing outcome [15]. It goes without saying that the former attacks can be identified and therefore prevented (mitigated) much easily than the latter due to their influence is more obvious. Furthermore, sophisticated cyber-attacks usually go from one dynamic shape to another so that, for instance, gather most intel in “silent mode” and do most damage in “attack mode”. In order to prevent different types of cyber-attacks, the detection systems incorporated in electrical drives control and upper level control systems of industrial plants must be flexible [2], [3], [5].

Cyber-attacks types on energy supply side of the electrical drives. Depending on the supply type, different results can be achieved on electrical drives with cyber-attacks targeted its prime energy supply.

If electrical drives are connected to the mains, the main influences that can be feasible are: 1) changing its main parameters (voltage amplitude and/or frequency); 2) deteriorating the secondary parameters such as total harmonic distortion factor (for example, by activating the most renewable energy sources systems). If these changes are considerably low so that they cannot be identified as a threat to the power grid, they will cause uncontrolled damage on electrical drives side [2].

In case when electromechanical systems are autonomous, various cyber-attacks paths can be considered depending on the type of the energy source: battery-only; supercapacitors-only; fuel cells-only; hybrid energy storage system with combined sources etc. [16]. Comparing typical Li-ion batteries and supercapacitors, the former are characterized by higher capacitance than the latter, so the supercapacitor unit can be used to deal more rapid damage (up to it limits) while the batteries may be applied for long-term slowly increased damage. In case if hybrid energy storage systems are controlled (active), i.e. they have DC-DC converters for power flow control; they can be also used in order to change supply voltage for inverter of traction motor or to create spike currents in a DC-link.

If electrical drive is a part of the system with a combined supply, such as in hybrid electric vehicles, where the main propulsion is carried out by internal combustion engine, the main non-electrical power can cause damage through internal combustion engine to electrical drive depending on the topology.

Monitoring and detection. Most of the means used in cyber-attacks monitoring and detection in electrical drives are based on the already installed sensors needed for their proper operation [10] – [13]. For widely used vector-controlled electrical drives they include up to: three three-phase current sensors, sensor of mechanical coordinates, DC-link voltage sensor, motor temperature sensor, technological processes sensors.

The simplest cyber-attacks that are being studied [10] include false data (changing transfer gain, offset or setting wrong value) from one type of the sensors which can be easily identified using data from the sensors of other type. However, such approach cannot be effectively applied if, for example, all sensors are compromised so that the control system is operated normally while new variables are added in order to bypass feedback and limitation levels. Other means for cyber-attacks detection lay in the electrical drives control systems. Typical examples are [11] – [13]: the controllers outputs of mechanical and electrical coordinates, stator current phase portrait and THD, speed and torque ripple and integral values of the states tracking errors. Usual approaches to detect cyber-attacks are: rule-based techniques, fuzzy controllers, neural networks, etc. [11] – [16].

In general, the system detection properties can be enhanced by increasing the number of the applied criteria, since no criteria by its own can successfully identify various types of cyber-attacks whose number grows rapidly [11] – [13].

Another approach that can improve detection is the implementation of state-space observers [2]. Theory of adaptive observers used for parameters identification and outputs estimation is well developed for variety of widely used modern electrical drives. Therefore it makes it a perfect tool for online detection.

Mitigation and resilience. In case the means for detection are effective enough to identify the cyber-attack target, the standard means for mitigation its effect can be applied. They usually require more knowledge in coding and communication than in power systems area [2], [4],]16]. Such approaches include: 1) re-initialize the system or the target device; 2) changing system IP; 3) applying different firewall rules etc.

However with adaptive observers and similar approaches which allow to estimate or to predict the electrical drive's operation, it is also possible to use the information from the observers instead of, for example, a cyber-attacked sensor in order to continue safe operation while re-initializing physical sensor.

Another solution that can improve robustness properties to various types of cyber-attacks are so-called "digital twins" of the systems which lay in copying the full detailed model of a system in a cloud, online analyzing and comparing it with the real setup [17]. However such solutions are typically rather complex in the part of secure communication between the system and cloud.

It is worth mentioning that the most sophisticated cyber-attackers with profile orientation background tend to learn from the scientific world in order to enhance their skills. It makes all cyber-security oriented research verily attractive for them and thus it should be kept out of publicity [18].

Conclusions. Cyber-attacks can be directed on all parts of electrical drives control systems from the sensors to tuning and constraints. Cyber-attacks affect systems differently to physical faults. Systems which detect and mitigate or prevent cyber-attacks are required. Usual signals used for detection in electrical drives are information from the sensors, as well as main control system variables. It is recommended to apply as many criteria as possible since different cyber-attacks lead to various consequences.

Most often researchers study effects of sensor additive and multiplying cyber-attacks, because it is easier to simulate and requires low understanding of electrical drives operation of cyber-attackers. For the most responsible applications the systems which are robust or adaptive with respect to different cyber-attacks are required.

References

1. W. Wei, C. -H. Hsu, V. Piuri and A. Rayes, "Guest Editorial: Deep Learning Driven Secure Communication for Cyber Physical Systems," in *IEEE Wireless Communications*, vol. 29, no. 2, pp. 14-15, April 2022, doi: 10.1109/MWC.2022.9801719.
2. R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa, "Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications," in *IEEE Access*, vol. 8, pp. 151019-151064, 2020, doi: 10.1109/ACCESS.2020.3016826.

3. R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, P. Manoharan, L. Mihet-Popa, J. Zhaof, V. Terzija, “A specialized review on outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid”, *International Journal of Electrical Power & Energy Systems*, Elsevier, No. 136, 2021, 29 p.

4. U. Sharma (ed.), P. Nand (ed.), J. M. Chatterje, *Cyber-Physical Systems – Foundations and Techniques*, 2022, Wiley-Scrivener.

5. M. Bharathidasan, V. Indragandhi, V. Suresh, M. Jasiński, Z. Leonowicz, “A review on electric vehicle: Technologies, energy trading, and cyber security”, *Energy Reports,* Elsevier, No. 8, 2022, pp. 9662-9685.4

6. W. Cao, Z. Zhu, J. Nan, Q. Yang, G. Gu and H. He, "An Improved Motion Control With Cyber-Physical Uncertainty Tolerance for Distributed Drive Electric Vehicle," in *IEEE Access*, vol. 10, pp. 770-778, 2022, doi: 10.1109/ACCESS.2021.3136573.

7. A. Petrillo, A. Pescapé and S. Santini, "A Secure Adaptive Control for Cooperative Driving of Autonomous Connected Vehicles in the Presence of Heterogeneous Communication Delays and Cyber-attacks," in *IEEE Transactions on Cybernetics*, vol. 51, no. 3, pp. 1134-1149, March 2021, doi: 10.1109/TCYB.2019.2962601.

8. C. Lv, X. Hu, A. Sangiovanni-Vincentelli, Y. Li, C. M. Martinez and D. Cao, "Driving-Style-Based Co-design Optimization of an Automated Electric Vehicle: A Cyber-Physical System Approach," in *IEEE Transactions on Industrial Electronics*, vol. 66, no. 4, pp. 2965-2975, April 2019, doi: 10.1109/TIE.2018.2850031.

9. Y. Zhang, L. Chu, Y. Ou, C. Guo, Y. Liu and X. Tang, "A Cyber-Physical System-Based Velocity-Profile Prediction Method and Case Study of Application in Plug-In Hybrid Electric Vehicle," in *IEEE Transactions on Cybernetics*, vol. 51, no. 1, pp. 40-51, Jan. 2021, doi: 10.1109/TCYB.2019.2928945.

10. B. Yang, L. Guo, F. Li, J. Ye and W. Song, "Vulnerability Assessments of Electric Drive Systems Due to Sensor Data Integrity Attacks," in *IEEE Transactions on Industrial Informatics,* vol. 16, no. 5, pp. 3301-3310, May 2020, doi: 10.1109/TII.2019.2948056.

11. B. Yang, L. Guo, F. Li, J. Ye and W. Song, "Impact Analysis of Data Integrity Attacks on Power Electronics and Electric Drives," 2019 *IEEE Transportation Electrification Conference and Expo (ITEC),* 2019, pp. 1-6, doi: 10.1109/ITEC.2019.8790574.

12. L. Guo, J. Ye and B. Yang, "Cyber-attack Detection for Electric Vehicles Using Physics-Guided Machine Learning," in *IEEE Transactions on Transportation Electrification*, vol. 7, no. 3, pp. 2010-2022, Sept. 2021, doi: 10.1109/TTE.2020.3044524.

13. L. Guo and J. Ye, "Cyber-Physical Security of Electric Vehicles With Four Motor Drives," in *IEEE Transactions on Power Electronics*, vol. 36, no. 4, pp. 4463-4477, April 2021, doi: 10.1109/TPEL.2020.3025718.

14. V. S. B. Kurukuru, M. A. Khan and S. Sahoo, "Cybersecurity in Power Electronics Using Minimal Data – A Physics-Informed Spline Learning Approach," in *IEEE Transactions on Power Electronics*, vol. 37, no. 11, pp. 12938-12943, Nov. 2022, doi: 10.1109/TPEL.2022.3180943.

15. P. Eder-Neuhauser, T. Zseby, J. Fabini, and G. Vormayr, “Cyber attack models for smart grid environments,” *Sustainable Energy, Grids and Networks*, vol. 12. Elsevier BV, pp. 10–29, Dec-2017.

16. M. B. F. Ahsan, S. Mekhilef, T. K. Soon, M. B. Mubin, P. Shrivastava, and M. Seyedmahmoudian, “Lithium-ion and supercapacitor-based hybrid energy storage system for electric vehicle applications: A review,” *International Journal of Energy Research*, vol. 46, no. 14. Wiley, pp. 19826–19854, 09-Aug-2022.

17. A. Saad, S. Faddel, T. Youssef and O. A. Mohammed, "On the Implementation of IoT-Based Digital Twin for Networked Microgrids Resiliency Against Cyber Attacks," in *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5138-5150, Nov. 2020, doi: 10.1109/TSG.2020.3000958.

18. E. Karangelos and L. Wehenkel, “Cyber–physical risk modeling with imperfect cyber-attackers,” *Electric Power Systems Research*, vol. 211. Elsevier, p. 108437, Oct-2022.