IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 19, 2021, accepted May 20, 2021, date of publication May 25, 2021, date of current version June 3, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3083499

Towards Secured Online Monitoring for Digitalized GIS Against Cyber-Attacks Based on IoT and Machine Learning

MAHMOUD ELSISI[1,2], MINH-QUANG TRAN[1,3], KARAR MAHMOUD[4,5], DIAA-ELDIN A. MANSOUR[6], (Senior Member, IEEE), MATTI LEHTONEN[4], AND MOHAMED M. F. DARWISH[2,4]

[1]Industry 4.0 Implementation Center, Center for Cyber-Physical System Innovation, National Taiwan University of Science and Technology, Taipei 10607, Taiwan
[2]Department of Electrical Engineering, Faculty of Engineering at Shoubra, Benha University, Cairo 11629, Egypt
[3]Department of Mechanical Engineering, Thai Nguyen University of Technology, Thai Nguyen 250000, Vietnam
[4]Department of Electrical Engineering and Automation, School of Electrical Engineering, Aalto University, 02150 Espoo, Finland
[5]Department of Electrical Engineering, Faculty of Engineering, Aswan University, Aswan 81542, Egypt
[6]Department of Electrical Power and Machines Engineering, Faculty of Engineering, Tanta University, Tanta 31511, Egypt

Corresponding authors: Mohamed M. F. Darwish (mohamed.m.darwish@aalto.fi; mohamed.darwish@feng.bu.ed.eg) and Karar Mahmoud (karar.mostafa@aalto.fi)

This work was supported in part by the Department of Electrical Engineering and Automation, Aalto University, Espoo, Finland, and in part by the Center for Cyber-Physical System Innovation from the Featured Areas Research Center Program in the Agenda of the Higher Education Sprout Project, Taiwan.

ABSTRACT Recently, the Internet of Things (IoT) has an important role in the growth and development of digitalized electric power stations while offering ambitious opportunities, specifically real-time monitoring and cybersecurity. In this regard, this paper introduces a novel IoT architecture for the online monitoring of the gas-insulated switchgear (GIS) status instead of the traditional observation methods. The proposed IoT architecture is derived from the concept of the cyber-physic system (CPS) in Industry 4.0. However, the cyber-attacks and the classification of the GIS insulation defects represent the main challenges against the implementation of IoT topology for the online monitoring and tracking of the GIS status. For this purpose, advanced machine learning techniques are utilized to detect cyber-attacks to conduct the paradigm and verification. Different test scenarios on various defects in GIS are performed to demonstrate the effectiveness of the proposed IoT architecture. Partial discharge pulse sequence features are extracted for each defect to represent the inputs for IoT architecture. The results confirm that the proposed IoT architecture based on the machine learning technique, that is the extreme gradient boosting (XGBoost), can visualize all defects in the GIS with different alarms, besides showing the cyber-attacks on the networks effectively. Furthermore, the defects of GIS and the fake data due to the cyber-attacks are recognized and presented on the dashboard of the proposed IoT platform with high accuracy and more clarified visualization to enhance the decision–making about the GIS status.

INDEX TERMS Internet of Things, machine learning, cyber-security, gas-insulated switchgear, partial discharge.