

Chapter 48

A Cyber–Physical Photovoltaic Array Monitoring and Control System

Gowtham Muniraju

*SenSIP Center, Arizona State University, Tempe,
USA*

Cihan Tepedelenlioglu

*SenSIP Center, Arizona State University, Tempe,
USA*

Sunil Rao

*SenSIP Center, Arizona State University, Tempe,
USA*

Pavan Turaga

*SenSIP Center, Arizona State University, Tempe,
USA*

Sameeksha Katoch

*SenSIP Center, Arizona State University, Tempe,
USA*

Mahesh K Banavar

*Clarkson Center for Complex Systems Science,
Clarkson University, Potsdam, USA*

Andreas Spanias

*SenSIP Center, Arizona State University, Tempe,
USA*

Devarajan Srinivasan

Poundra Inc, Tempe, USA

ABSTRACT

A cyber physical system approach for a utility-scale photovoltaic (PV) array monitoring and control is presented in this article. This system consists of sensors that capture voltage, current, temperature, and irradiance parameters for each solar panel which are then used to detect, predict and control the performance of the array. More specifically the article describes a customized machine-learning method for remote fault detection and a computer vision framework for cloud movement prediction. In addition, a consensus-based distributed approach is proposed for resource optimization, and a secure authentication protocol that can detect intrusions and cyber threats is presented. The proposed system leverages video analysis of skyline imagery that is used along with other measured parameters to reconfigure the solar panel connection topology and optimize power output. Additional benefits of this cyber physical approach are associated with the control of inverter transients. Preliminary results demonstrate improved efficiency and robustness in renewable energy systems using advanced cyber enabled sensory analysis and fusion devices and algorithms.

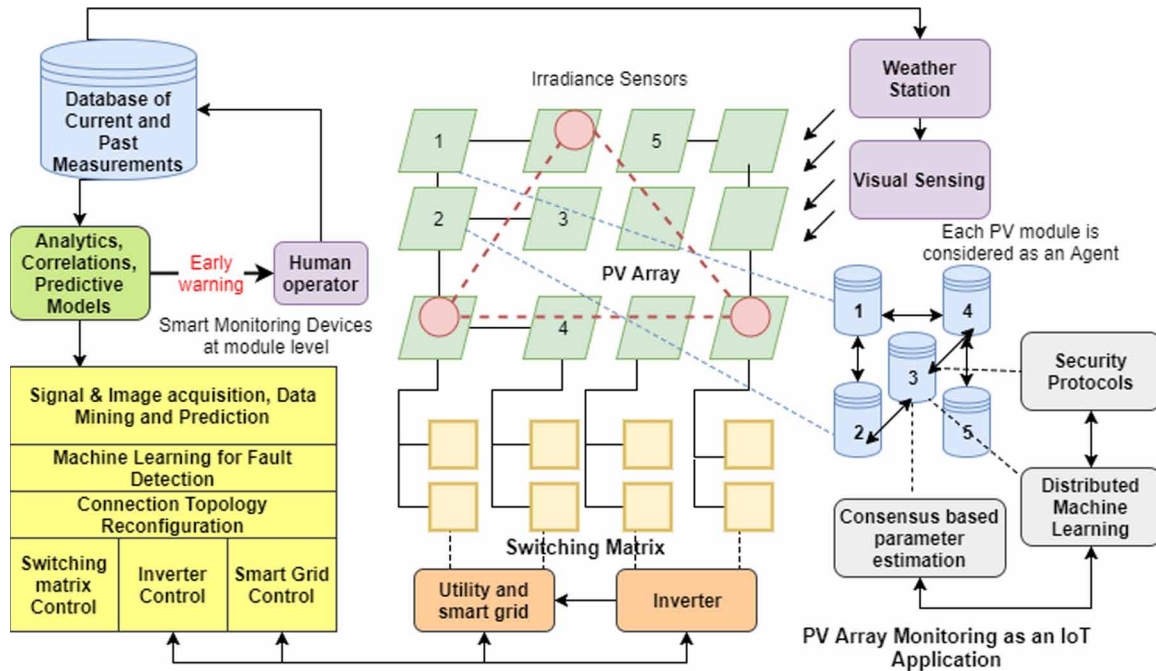
DOI: 10.4018/978-1-7998-2466-4.ch048

1. INTRODUCTION

Utility-scale photovoltaic (PV) array systems are being rapidly deployed in several areas and are now capable of generating several megawatts of power. Although progress in several associated technologies enabled increased efficiencies and reduced cost, the large number of panels installed in remote areas makes it difficult and expensive to detect and localize faults. Solar power generation is affected by several factors such as shading due to cloud cover, soiling on the panels, unexpected faults and weather conditions. Hence, the efficiency of solar energy farms requires detailed analytics on each panel by sensing individual panel voltage, current, temperature and irradiance. Parameters estimated can be used to determine and repair faults, predict performance, and reconnect panels using relays to optimize power.

We present in this paper, a unique cyber-physical concept that uses sensors, actuators, controllers and network communications for solar energy monitoring and control. The CPS concept is shown in the block diagram of Figure 1, where hardware and algorithms are integrated to detect faults, predict shading, provide real-time analytics for each panel, optimize power, and reduce transients.

Figure 1. Networked PV Array Concept enabling: a) weather feature correlations, b) local shading prediction, c) decision support, and d) fault detection



Our study describes machine learning, computer vision, wireless sensor network communications, and distributed consensus estimation algorithms whose aim are to improve the efficiency and reliability of utility-scale solar arrays. Theoretical and experimental aspects of this comprehensive CPS approach are described along with implementation details. The methods presented in this paper will be validated on a state of the art solar array testbed shown in Figure 2 (also described in detail later in section 6). This testbed consists of 104 panels with a power generation capacity of 18kW and was developed by

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/a-cyber-physical-photovoltaic-array-monitoring-and-control-system/251463

Related Content

The Changing Face of Electronic Aggression: The Phenomenon of Online Trolling within the Context of e-Participation in the United Kingdom

Shefali Virkar (2014). *International Journal of Cyber Warfare and Terrorism* (pp. 29-46).

www.irma-international.org/article/the-changing-face-of-electronic-aggression/127385

A Study of Good-Enough Security in the Context of Rural Business Process Outsourcing

Reena Singhand Hemant Jalota (2018). *Psychological and Behavioral Examinations in Cyber Security* (pp. 239-252).

www.irma-international.org/chapter/a-study-of-good-enough-security-in-the-context-of-rural-business-process-outsourcing/199892

From Conventional to Sophisticated: A Cyber Guise to Terrorism in the Middle East

Mustafa Küçük Firat (2019). *Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism* (pp. 203-239).

www.irma-international.org/chapter/from-conventional-to-sophisticated/228472

On the Analysis of Horror Stories in the Militants' Narratives as Markers of Violent Behavior and Conflict Identity: Case of "L/DPR" During the Warfare in Donbass, East Ukraine, 2014-2021

Yuriy V. Kostyuchenko and Viktor Pushkar (2022). *International Journal of Cyber Warfare and Terrorism* (pp. 1-19).

www.irma-international.org/article/on-the-analysis-of-horror-stories-in-the-militants-narratives-as-markers-of-violent-behavior-and-conflict-identity/297856

Advances in Digital Forensics Frameworks and Tools: A Comparative Insight and Ranking

Muhammad Abulaish and Nur Al Hasan Haldar (2020). *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 165-191).

www.irma-international.org/chapter/advances-in-digital-forensics-frameworks-and-tools/251424