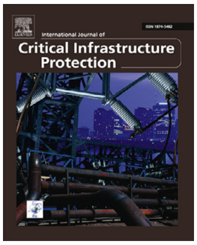
International Journal of Critical Infrastructure Protection 17 (2017) 3–14

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/IJCIP



Wind farm security: attack surface, targets, scenarios and mitigation

*Jason Staggs, David Ferlemann, Sujeet Shenoi**

Tandy School of Computer Science, University of Tulsa, 800 S. Tucker Drive, Tulsa, Oklahoma 74104, USA

ARTICLE INFO

Article history:
Received 28 December 2016
Revised 3 February 2017
Accepted 6 February 2017
Available online 24 March 2017

Keywords:
Wind Farms
Renewable Energy Generation
Industrial Control Systems
Attack Surface
Attack Targets
Attack Scenarios
Attack Mitigation

ABSTRACT

As modern society grows more reliant on wind energy, wind farm deployments will become increasingly attractive targets for malicious entities. The geographic scale of wind farms, remoteness of assets, flat logical control networks and insecure control protocols expose wind farms to myriad threats. This paper attempts to clarify the gaps in the understanding of wind farm threats and their implications. The paper describes the anatomy of a generic wind farm and the attack vectors that can be leveraged to target its information technology, industrial control and physical assets. It discusses attack scenarios involving unauthorized wind turbine control, wind turbine damage, wind farm disruption and damage, and substation disruption and damage. Additionally, the paper highlights mitigation techniques that provide robust security coverage and reduce the negative cyber and physical impacts. The attack surface, targets, scenarios and mitigation techniques presented in this paper are common across wind farm deployments. However, it is still possible to add details about the unique aspects of wind farm assets, configurations and operations in order to develop a holistic risk management program geared for a specific wind farm deployment.

1. Introduction

Wind is a ubiquitous commodity that is rapidly becoming the predominant source of renewable energy [21]. Utility companies are rolling out massive wind farm deployments to harvest this "green" energy and convert it to electricity that is injected into the bulk power grid [3]. In 2015, wind energy accounted for 4.7% of electricity generated in the United States [29]. By 2030, the wind energy contribution to the power grid is expected to increase to 20% [28]. As modern society becomes more reliant on wind energy, wind farm deployments will draw the attention of attackers ranging from hackers and criminals to terrorists and nation states.

At the lowest level, a wind farm infrastructure comprises wind turbines that generate electricity. Each turbine is connected to a step-up transformer whose power output is sent to a substation; the substation collects electricity generated by multiple turbines and steps-up the power before injecting it into the grid. Groups of turbines in a wind farm are arranged in fiber optic rings for communications and command and control; these turbine rings are often daisy chained to a substation. A substation has two segmented supervisory control and data acquisition (SCADA) networks, an operations control network for managing wind turbine operations and a transmission control network for managing the collection and injection of power into the grid. A control center provides centralized command and control of wind farm networks comprising wind turbines and substations.

The geographic scale of a wind farm, remoteness of its turbines and substations, flat logical configurations of its control networks and use of insecure SCADA protocols expose wind farm assets to myriad threats. These threats can be realized by attackers to disrupt operations or damage turbines and substations, leading to significant financial losses on the part of

* Corresponding author.
E-mail address: sujeet@utulsa.edu (S. Shenoi).

http://dx.doi.org/10.1016/j.ijcip.2017.03.001
1874-5482/© 2017 Elsevier B.V. All rights reserved.

wind farm owners and operators. The potential also exists to disrupt the transmission of electricity and, perhaps, inject disturbances into the bulk power grid.

Some wind farms have hundreds of turbines and multiple substations; these wind farm infrastructures can have valuations in the billions of dollars. Because of the vast amounts of power they supply to the grid, these wind farms also have extrinsic value as critical infrastructure assets. However, despite their monetary value and criticality, limited research has been published that formally describes the wind farm attack surface, targets and major cyber-physical attack scenarios, let alone strategies and tactics for mitigating the risks posed by sophisticated attacks [8,12,15,22,26,32].

This paper attempts to address the gaps in the understanding of wind farm (in)security and the implications. The paper begins by elucidating the anatomy of a generic wind farm and the attack vectors that may be leveraged to target its information technology, industrial control system (ICS) and, ultimately, physical assets. The paper also describes scenarios involving unauthorized wind turbine control, wind turbine damage, wind farm disruption and damage, and substation disruption and damage. While the attack vectors involve physical and/or cyber access, the attack scenarios involve cyber attacks that significantly impact physical assets; these scenarios are realized by leveraging custom tool sets developed for conducting security assessments of wind farm control networks. Finally, the paper outlines several mitigation techniques for addressing the threats to wind farm assets and operations. These mitigation techniques, which include physical security, network segmentation, system hardening, system assurance, and policies and procedures, provide robust security coverage and reduce the negative cyber and physical impacts to wind farm assets.

Wind farms are large, distributed infrastructures with diverse assets. The research described in this paper is based on security assessments of five U.S.-based wind farms totaling more than a thousand turbines spanning multiple equipment models from five major vendors. Efforts have been made to extract the commonalities and crystallize them when describing the attack surface, targets, scenarios and mitigation techniques. Thus, the results presented in this paper are, for the most part, common across wind farm configurations and vendor products. Indeed, this work can be used as a foundation to which details about the unique aspects of wind farm assets, configurations and operations can be incorporated in developing a holistic risk management program geared for a specific wind farm deployment.

2. Wind farm infrastructure

Wind farms incorporate a number of components to ensure the safe, efficient and reliable generation, transmission and injection of electricity into the power grid [19]. From the perspective of functionality and security, a wind farm can be envisioned as having two interconnected, cooperative infrastructures: (i) power infrastructure; and (ii) communications infrastructure. The IEC 61400 international standard [13] defines uniform design, operations and communications requirements for wind turbine suppliers.

Fig. 1 presents a schematic diagram of a wind farm power infrastructure. Wind turbines in a wind farm convert rotational kinetic energy into electricity. A step-up transformer at each turbine site increases the output voltage from a few hundred volts to a medium voltage distribution level (nominally 34.5 kV) for transmission to a collector at a substation. Grounding transformers are positioned in each wind turbine circuit to provide a ground path to an ungrounded Y-connected or delta-connected system, helping ensure that all protection devices (e.g., circuit breakers and fuses) work properly. A collector aggregates the input electrical energy and transforms it to a high voltage (e.g., 100 kV) for injection into the bulk electric power grid.

A wind farm may have hundreds of wind turbines and can span many hundreds of square miles. Therefore, it is common to have multiple substations with inputs to the bulk power grid.

Fig. 2 presents a schematic diagram of a generic wind farm communications infrastructure, which is vital to ensuring safe, efficient and reliable operations [1,23,30,31]. IEC 61400-25 [13,14] specifies uniform communications requirements for the monitoring and control of wind turbines. Multiple wind turbines are arranged in a fiber ring for IP-based communications and command and control. The fiber rings are frequently daisy chained for efficient and redundant communications; the resulting network is often configured to have a flat logical

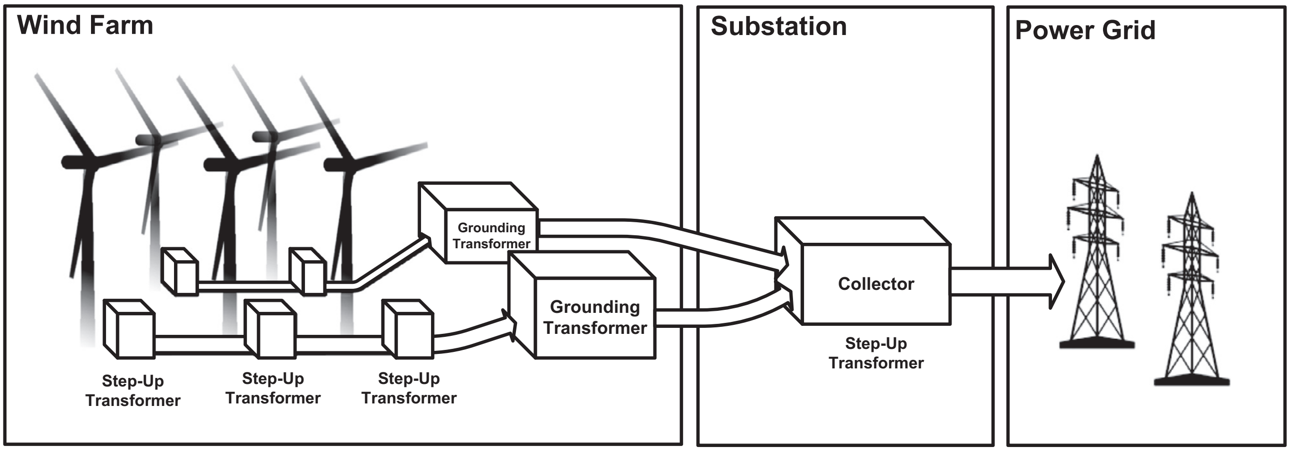


Fig. 1 – Wind farm power infrastructure.