Cyber Intrusion of Wind Farm SCADA System and Its Impact Analysis

Jie Yan, *Student Member, IEEE,* Chen-Ching Liu, *Fellow, IEEE,* and Manimaran Govindarasu, *Senior Member, IEEE*

***Abstract*—The increased and concentrated penetration of wind power makes the power network more dependent on, and vulnerable to, the wind energy production. The dynamic performance of power system can be affected by the wind farm operations. Cyber attacks on the cyber systems of wind farm present a potential threat for power system dynamics. The cyber security for the SCADA system of a wind farm is studied in this paper by incorporating the impact on the power system dynamics. The vulnerabilities of a wind farm SCADA system are identified. Credible attack scenarios are developed consequently. The simulation results show that cyber attacks can cause major problems for a power system, including economy loss, overspeed of a wind turbine, and equipment damage.**

***Index Terms*—wind power, power system dynamics, SCADA, cyber security**

I. Introduction

The installed wind power capacity is increasing rapidly in recent years. The year 2008 was a record year for wind generation in the United States with a total increase of 8,360 MW which is 50% of the total wind capacity at the end of 2007 [1]. Wind energy accounted for 42% of the total new capacity added. Report [2] from the Department of Energy anticipates that wind could power 20% of US grid by 2030.

The increased and concentrated penetration of wind power makes the power network more dependent on, the wind energy production. Moreover, the newly installed large wind farms will be connected directly to the high voltage transmission grid. Until recently, wind farms have been connected to the distribution system, which typically has either 10/20 kV or 50/60 kV grids [3]. This situation means that future wind farms must be able to replace conventional power stations, and thus be active controllable elements in the power supply network. In other words, wind farms must be enabled with the control capabilities of a power plant [4].

The dynamic performance of a power system can be affected by wind farm operations. Cyber attacks on the Supervisory Control And Data Acquisition (SCADA) system of a wind farm present a potential threat for power system stability.

This research is funded in part by the National Science Foundation, USA, through Grant No. # CNS-0915945. Professor C. C. Liu would like to acknowledge the partial support from Science Foundation Ireland (SFI) through the Principal Investigator award.

978-1-61284-788-7/11/$26.00 ©2011 IEEE

The cyber threat is real for power systems. Power system network has been, and continues to be, a target of malicious groups and individuals intent on disrupting this system. For example, in January 2003, the "Slammer" Internet worm took down monitoring computers at a power plant in the U.S. A subsequent report by Nuclear Regulatory Commission (NRC) concluded that although the infection caused no outage, it blocked commands that operated other power utilities [5]. There is a growing concern that the US infrastructure systems including power grids are vulnerable to cyber attacks [6]-[8]. It would take relatively few resources to attack a target, e.g. a large network or infrastructure system, and cause serious damages from a major or prolonged service disruption [9].

Cyber systems of wind farms could be attacked in order to disrupt the power system operations. The SCADA system is of specific concern among the cyber systems. Successful cyber attacks on the SCADA system can lead to a widespread disruption of power system operation. Cyber security for the SCADA system of a wind farm needs to be investigated. Cyber security here addresses the protection of cyber-based systems that comprise the critical SCADA systems of wind farms.

Cyber security for the SCADA system is an emerging area of research in power system engineering. A potential cyber threat to SCADA systems, ranging from computer system to power system aspects, has been recognized in [10]. Efforts by International Electrotechnical Commission Technical Council (IEC TC 57) on power systems management and associated information exchange have advanced communication protocols with stronger encryption and authentication mechanisms. Specifically, this has been proposed in IEC 62351 for data and communication security that assures access to sensitive power equipment and provides higher reliability with audit capabilities [11]. Reference [12] presents a modeling language and a quantitative evaluation approach for the security of power information systems. The impact of a cyber attack on SCADA system is studied systematically in [13]. It is evaluated by the resulting loss of load through power flow computation.

Cyber security for the SCADA system of a wind farm is studied in this research by incorporating the impact on power system dynamics. The vulnerabilities of a wind farm SCADA system are identified. Credible attack scenarios are developed consequently. The cyber defense and response of a wind farm to the attack scenarios are examined. The impact of cyber

attacks on power system dynamics is shown with computer simulation results.

The remainder of this paper is organized as follows. Section II presents the primary architectures of a wind farm SCADA system. In Section III, the vulnerabilities of communication infrastructures are identified. Section IV proposes the attack scenarios based on the identified vulnerabilities. Section V provides the simulation results of cyber attacks. Finally, Section VI gives the conclusion.

II. Wind Farm SCADA System Architectures

Three primary communication architectures of a SCADA system for wind farm are identified in this context.

The first architecture of the SCADA system of a wind farm is illustrated in Fig. 1. This implementation utilizes a stand-alone network isolated from other communication networks of the wind power company. Servers in a control room support the monitoring and control of wind turbines within the wind farm.

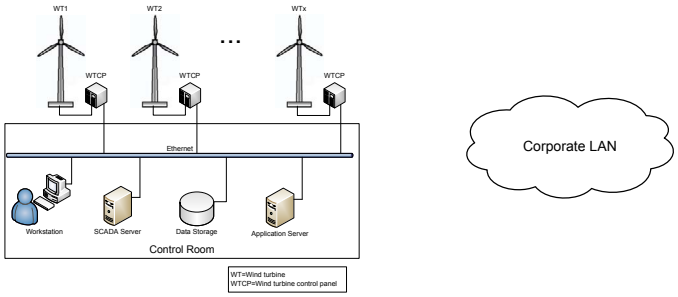

Fig. 1. Stand-alone network

The next implementation approach utilizes an independent communication infrastructure but interfaces restrictively with other parts of the corporate network for business and operational reasons, as shown in Fig. 2. The corporate LAN is connected to vendors through communication links, such as VPN over Internet.

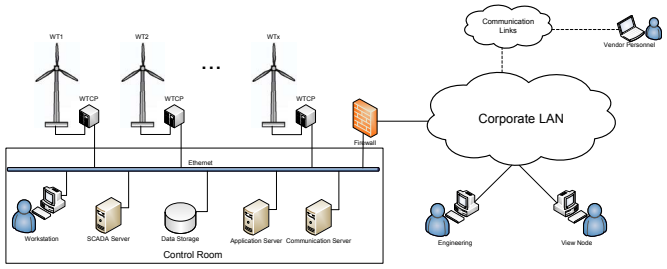

Fig. 2. Partially integrated network

Finally, some wind power companies, having multiple wind farms in separated locations, integrate all wind farms into a single Energy Management System (EMS) in a main control center through a control WAN, as shown in Fig. 3. The SCADA network of one single wind farm is similar to the second primary architecture, but the control room is normally not staffed, and it is only for maintenance use. Wind power companies use private utility Intranet, VPN or digital microwave as communication links for control WAN.

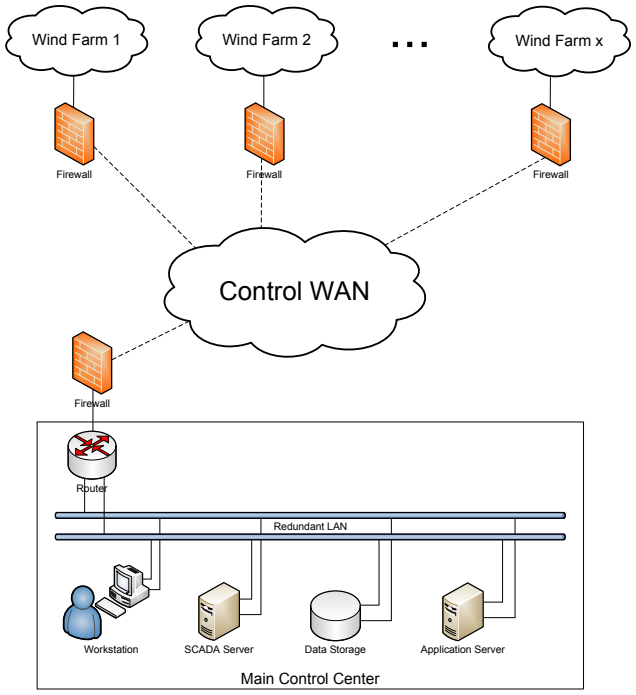

Fig. 3. Fully integrated wide-area control network

III. Vulnerabilities

Six major sources of vulnerability are identified. The vulnerabilities will be addressed in terms of these architectures in order to analyze the impact of the vulnerabilities.

A. Configuration Management

Wind turbine is equipped with a control and monitoring unit with operating keys and a small display screen which is normally mounted in the tower base and may be easily accessible. It is the wind turbine control panel (WTCP), primarily used by the maintenance personnel for acquisition of data characterizing the instantaneous operating status, and for retrieval of measurement values about the status of most important units. In addition, certain operations required for maintenance can be performed "manually" on WTCP.

WTCP has the capability to change the configuration settings of a wind turbine. It must support authentication for configuration update as required by the NERC critical infrastructure protection (CIP) series [14]. A program must be documented and implemented for managing configuration changed by WTCP.

Security Considerations

The configuration management of WTCP may not be well established. WTCP is built on open ground, and it could be accessed by unauthorized individuals to gain physical access to the facilities. Even though WTCP supports user authentication such as a pin, the pin may be cracked.

The pin can be cracked by a brute force attack. For example, if the key length of pin is 6, there will be 10^6 possible pins. The brute force attack will traverse the search space of possible pins until a correct one is found. There are a few techniques to help significantly reduce the search space.

Hackers can try the initial factory password and some simplistic passwords, as people tend to use those passwords for pins. Hackers may also scan fingerprints on the pin pad left by authorized users. In the best-case scenario, hackers are able to identify the 6 keys of the 6-digit pin, which will reduce the possible pins to 720.

The chemical combinatorial attack in [15] could be used to identify the pin directly. The attack consists in depositing on each pin pad key a small ionic salt quantity (e.g. some NaCl on key 0, some KCl on key 1, LiCl on key 2, SrCl2 on key 3, BaCl2 on key 4, CaCl2 on key 5...). As the user enters his or her pin, salts get mixed and leave the pin pad in a state where secret information can be leaked. The next phase of attack includes collecting samples from the pin pad and analyzing these using a mass spectrometer.

The chemical combinatorial attack could be extremely dangerous for WTCPs. Unlike ATMs, only a few users such as maintenance personnel operate the WTCPs, and they do not do it frequently. During a chemical combinatorial attack, the salts on the pin pad would not be mixed evenly, and therefore give a clear hint of the pin.

Compensating controls include monitoring physical access to the WTCP, utilizing motion-activated cameras, or adding authentication solutions.

B. Continuity of Operations

The SCADA system of a wind farm is expected to continue operating normally under disruptions. Disruptions include natural disasters such as earthquakes, and manmade events such as vandalism.

Security Considerations

It is noted that wind farm control room communicates with WTCPs by fiber optics. The optical fiber cables were buried along with power cables. The underground optic fibers are subject to breakage in the event of a disruption. The failure could be difficult to pinpoint and recover. Meanwhile, if the fiber cables are connected from a point to another point, there will be no redundant communication channel to resume communication under the failure. It requires a secondary form of communication to ensure continuity of operations in case of a disruption.

C. Fiber Optics

Optical fibers are used heavily in communication infrastructures of wind farms. Optical fibers are glass or plastic that allow propagation of light as a communication medium. It can be used for long distances without the need for signal enhancement. The optical fibers also offer high bandwidth capacities with a single fiber, being able to achieve transfer rates of up to 40 Gigabit/second.

Security Considerations

Optical fiber cables are simpler to tap than are generally believed. There are various optical fiber tapping methods. Splicing is the easiest form of tapping but is detectable by most network security systems. Splicing will create a momentary lapse of data and is noticeable. More advanced tapping methods include injecting additional light into the fiber and deducing the underlying optical signal by gauging certain interactions between the two. Bending the fiber to create micro-bends can make light leak from the fiber without disrupting communication. This method is preferred in this context.

As described in reference [16], a hacker can purchase inexpensive hardware necessary to tap into a fiber. The tap consists of bending the fiber to the point that it leaks light, as shown in Fig. 4. The fiber cable is placed into a micro-bend clamping device. Then the light leaks from the cable. The optical photo detector detects the leaking light and sends it to an optical-electrical converter. The converter changes the light pulses to electrical information and sends it to the hacker's PC through an Ethernet cable.

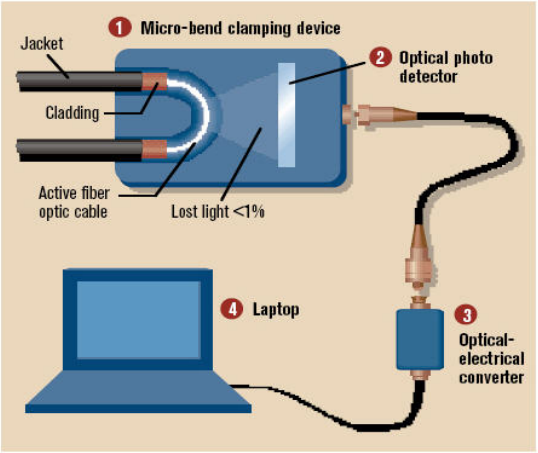

Fig. 4. An example of tapping
Source: http://blogs.techrepublic.com.com/security/?p=222&tag=leftCol;post-223.

Moreover, some tapping devices may be utilized not just for passive sniffing, but for active tapping, according to Oyster Optics [17]. Through such devices, a hacker is able to inject malicious signals into the fiber cables. Those attacks are not detectable in real-time. They are also difficult to locate, since the optical taps are subtle in nature.

Fiber taps present a high risk for SCADA systems of wind farms. Wind farms are built on open ground, and some of them are not staffed. Hackers can gain physical access to the fiber optics. Although fiber cables are normally buried underground, they can dig holes in order to reach the cables.

Compensating methods include encrypting data in transit. Another solution is the fiber intrusion detection device. These devices are highly-sensitive to various intrusion events, and allow immediate alerts of network tapping attempts.

D. Wireless

Wireless technology is considered for SCADA system of wind farms, which is an alternative to optical fibers. The reasons are:

- Wireless technology has the advantages of reduced

cost, flexibility of configuration, and ease of maintenance.

- Wireless network can be deployed in a tough terrain where wired infrastructure is difficult to install.
- Wireless communication could be used as a back-up for fibers to ensure continuity of operations when the fiber cable is broken or under attack.

An example of a wireless communication architecture for the wind farms can be found in [18].

Security Considerations

Wireless network is subject to some common attacks including sniff, spoof, man-in-the-middle attack and denial-of-service (DoS) attack. Even if strong encryption and authentication are applied, the wireless communication can still be affected by the jamming attack.

A jamming attack occurs when a hacker analyzes the signal spectrum being used by wireless network and then transmits a powerful signal to interfere with communication on the discovered frequencies. Jamming is easy to implement in practice. For example, a Bluetooth device located within ten meters of 802.11b network, will cause a jamming. The jamming attack could force the wireless network to hold the transmissions until the disruptive signal has gone, or switch to a slower data transmission rate since data needs to be retransmitted from time to time.

E. VPN

Virtual Private Network (VPN) over Internet is used in wind farm SCADA systems for remote communication. The IP Security (IPSEC) suite of protocols is commonly used to implement the VPN. It offers authentication and encryption at the internet protocol (IP) packet level.

Security Considerations

DoS attacks using a Botnet or other means (e.g., SYN Flooding) cause a large number of compromised computers to flood a huge volume of network traffic toward a target server or a subnet to the extent of affecting or destabilizing the victim. When such an attack happens in a wind farm SCADA, the real-time monitoring and control operation of the wind farm will be severely affected.

F. Human Errors

Human errors can interfere with normal operations of the SCADA system. A trusted user of a SCADA system can cause an internal attack. Hackers outside may gain access to the SCADA system through malware introduced into the system by infected portable storage devices. Oversight or negligence during key generation, distribution and management could cause critical information to be corrupted.

The possible solution to human errors is to provide and update comprehensive staff training constantly.

Configuration management and continuity of operations are questionable in all the three primary architectures. They are more risky for the third infrastructure, since the control rooms of wind farms are not staffed. The vulnerability of fiber optics is found in the three primary infrastructures, but it is more risky for the third one for the same reason above. Wireless technology should be employed with caution. Control WAN in the third infrastructure using VPN is less secure compared to private utility Intranet. Human error cannot be completely eliminated in the three primary architectures, as long as they are not completely automated.

IV. Attack Scenarios

Multiple attack scenarios are developed by exploiting the vulnerabilities described in Section III. Their influence on power system dynamics is studied in the following.

A simplified dynamical model of the cyber-power system of a wind farm is represented in Fig. 5. The variable speed wind turbines utilizing Doubly Fed Induction Generators (DFIGs) are used in this research. DFIG is the most widely used generator type, especially for wind turbines above 2.0 MW (e.g. GE Wind Energy, Vestas, RE Power, Nordex, NEG Micon) [19]. The dynamical model of wind turbine-generator set used in this context is close to that illustrated in [3]. SCADA servers in a control room support monitoring and control of wind turbines in real-time through WTCPs. The most common control commands include Q_{ref} command, P_{ref} command and θ_{ref} command, as shown in Fig. 5.

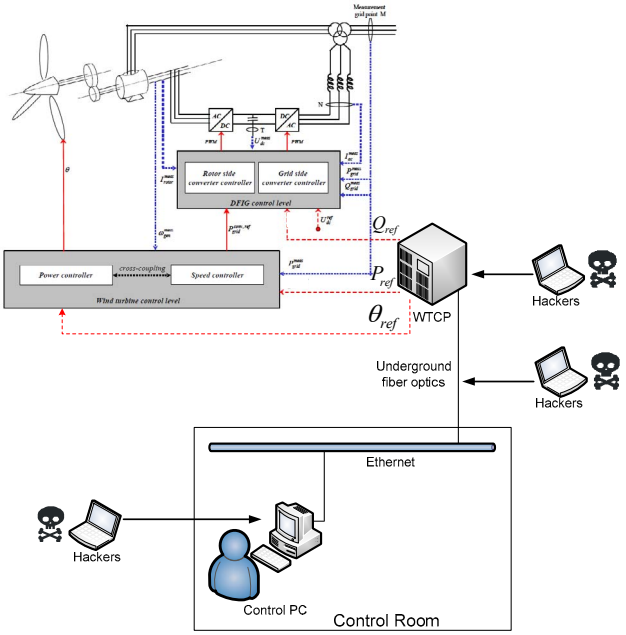

Fig. 5. Dynamical model of cyber-power system of wind farm

Attack scenario I:

1) Crack the pin of WTCP by attacks such as chemical combinatorial attack as illustrated in subsection III.A.
2) Sneak into the wind farm.
3) Enter the pin on the pin pad of WTCP, and gain the authority to control the wind turbine through WTCP.
4) Send malicious commands to wind turbine.

The attack could be detected, as wind farm operators are monitoring the wind turbines. However, damage could be

done before the operators react to the attack.

Attack scenario II:

1) Install surreptitious taps on optical fiber cables as described in subsection III.C.
2) Launch man-in-the-middle attack, sending faked measurement data to wind farm operators and malicious control commands to wind turbine.

The attack is difficult to detect, as the operators may not be aware of the real situation.

Attack scenario III:

As mentioned in subsection III.F, a human error could grant a malicious person access to the control PC of a SCADA system.

- Internal attack: a corrupted user gains physical access to the control PC, and then sends malicious commands to wind turbines.
- Infected portable storage device attack:
    1) Hackers drop infected memory stick somewhere around a wind farm operator.
    2) The operator picks it up, and plugs it in his PC out of curiosity. By doing so, malware such as Stuxnet is introduced into the PC.
    3) Malicious control commands will be sent out by the malware, if the control PC is infected.

V. Simulation Results

The impact of the attack scenarios is simulated within a one single wind turbine to infinite bus system through Digsilent Powerfactory, as shown in Fig. 6. The rated power output of wind turbine is 2 MW.

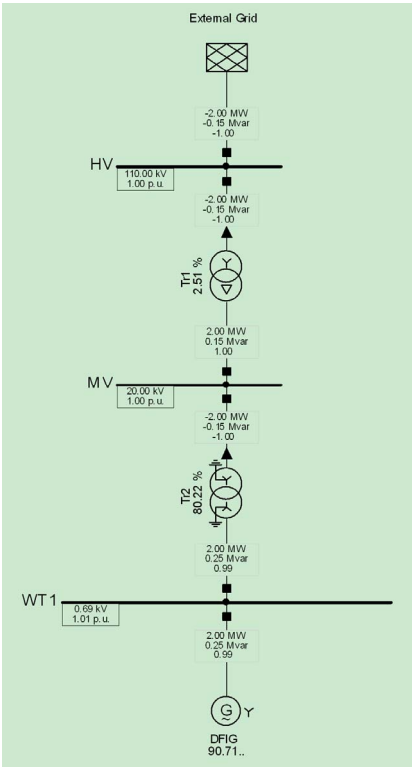

Fig. 6. One single wind turbine to infinite bus system

Attack a – malicious Q_{ref} command

Malicious Q_{ref} command is sent to DFIG, forcing it to generate (consume) a very high amount of reactive power, in order to cause voltage instability. The simulation results show that the attack is not able to cause a major problem. The terminal voltage is stable. It is reasonable since the rated power output of DFIG is limited, and it is connected to an infinite bus.

Attack b – malicious P_{ref} command

Malicious P_{ref} command is sent to DFIG, forcing the DFIG to reduce its active power output all of a sudden, while the mechanical power input doesn't change instantaneously, so that the attack may result in overspeed of wind turbine, and even equipment damage.

For example, let $P_{ref} = 0.1\,p.u.$ at $t = 2s$, and then the active power output of DFIG reduces to $0.1\,p.u.$ instantaneously due to the fast control of power converter. The rotor speed goes up for a while, as shown in Fig. 7. However, the speed controller module of the wind turbine detects the low power output of DFIG. According to the control strategy in [3], a low power output corresponds a low rotor speed, so that the speed controller sends a corresponding low *speed_ref* command to pitch control. The pitch control increases the pitch angle to reduce the mechanical power input so that the speed decreases to *speed_ref*.

Hence, attack *b* causes less active power output successfully, and then the economy loss. But it can only cause overspeed for a few seconds, and then the speed controller and pitch control drive the rotor speed down.

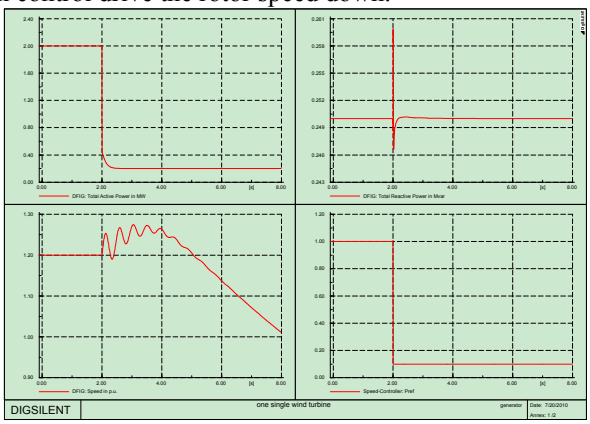

Fig. 7. Simulation results of attack *b*

Attack c – malicious θ_{ref} command

Malicious θ_{ref} command is sent to pitch control to set up the pitch angle directly, so that speed controller is not able to control the speed through pitch control. For example, assume that there is a wind gust at $t = 1s$, wind speed v_w increases from 8 m/s to 16 m/s. The reference speed remains a nominal speed of $1.2\,p.u.$, and the pitch angle increases. Let $\theta_{ref} = 0$ at $t = 3s$, and then the speed goes up to $1.6\,p.u.$ in merely 1 second, as shown in Fig. 8. The crowbar protection is triggered around $t = 4s$. Then the power converter is bypassed by a bypass circuit, and the DFIG becomes a regular

motor. Because its load is negative (wind power input), DFIG does not have power exchange with external.

Hence, attack *c* is able to cause overspeed, and then trigger the crowbar to disconnect DFIG from the power system.

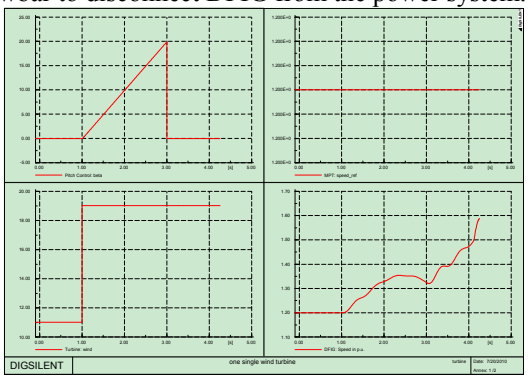

Fig. 8. Simulation results of attack *c*

Attack d – a sophisticated combination of attack b and c

For example, let $P_{ref} = 0.1\,p.u.$ and $\theta_{ref} = 0$ at $t = 2s$. As the active power output decreases, speed controller sends a lower reference speed to pitch control, but pitch angle is set at 0 deg, so the rotor speed still goes up, as shown in Fig. 9. The crowbar is triggered around $t = 5.5s$.

Hence, attack *d* has a similar impact as attack *c* when there is a wind gust.

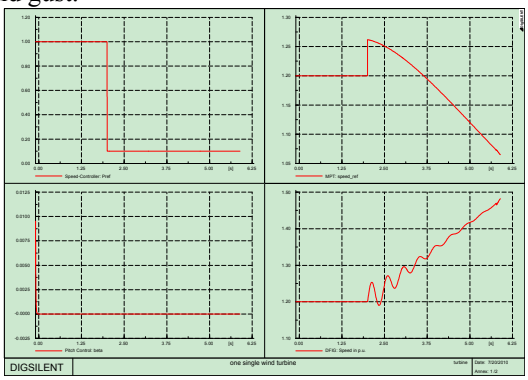

Fig. 9. Simulation results of attack *d*

Attack e –attack d in the case that crowbar is disabled.

For example, let $P_{ref} = 0.1\,p.u.$ and $\theta_{ref} = 0$ at $t = 2s$, while the crowbar protection is disabled. Then rotor speed is constantly increasing, as shown in Fig. 10.

Hence, attack *e* is able to cause overspeed for a long time period, and could result in an equipment damage.

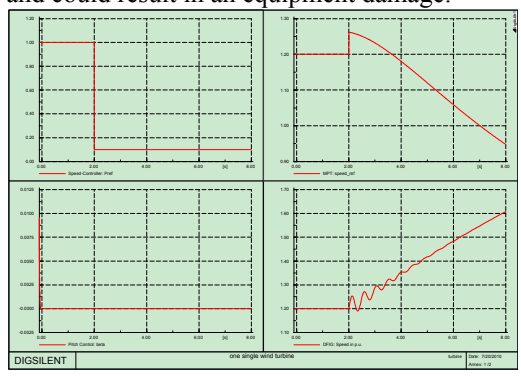

Fig. 10. Simulation results of attack *e*

VI. Conclusion

Credible attack scenarios have been developed based on the vulnerabilities of the SCADA system of a wind farm. The simulation results show that cyber attacks are able to cause major problems within a power system, including economy loss, overspeed of wind turbines, and even an equipment damage. Future work includes analytical evaluation of the impact of cyber attacks on power system dynamics within a large system, and corresponding mitigation mechanisms based on cost-effectiveness analysis.

References

[1] American Wind Energy Association: 2009. Another Record Year for Wind Energy Installations.

[2] U.S. Department of Energy: 2008. 20% Wind Energy by 2030. DOE/GO-102008-2567. Washington, DC.

[3] A. D. Hansen, C. Jauch, P. Sørensen, F. Iov, and F. Blaabjerg, "Dynamic wind turbine models in power system simulation tool DIgSILENT," Risø-R-1400(EN), Risø National Laboratory, 2004.

[4] P. Sørensen, B. Bak-Jensen, J. Kristiansen, A. D. Hansen, L. Janosi, and J. Bech, "Power plant characteristics of wind farms, wind power for the 21st century," *Proc. International Conference*, Kassel, Germany, September 2000.

[5] http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6901/cr6901.pdf

[6] D. Denning, "Is cyber terror next?" *Social Science Research Council*, Sept. 2001. [Online]. Available: http://www.ssrc.org/sept11/essays/denning.html

[7] T. Shimeall, P. Williams, and C. Dunley, "Countering cyber war," *Nato Review*, Winter 2001/2002.

[8] M. Vatis, "Cyber attacks during the war on terrorism: A predictive analysis," *Inst. for Sec. Tech. Studies*, Dartmouth College, Sept 22, 2001.

[9] M. G. Devost, B. K. Houghton, and N. A. Pollard, "Organizing for information warfare, the truth is out there," Terrorism Res. Center, 1997. [Online]. Available: http://www.terrorism.com

[10] Supervisory Control and Data Acquisition (SCADA) Systems, National Communications System, Technical Information Bulletin 04-1, 2004. [Online]. Available: http://www.ncs.gov/library/tech bulletins/2004/tib 04-1.pdf.

[11] F. Cleveland, "IEC TC57 security standards for power system's information infrastructure—Beyond simple encryption," Proc. IEEE Power Eng. Soc. General Meeting, Tampa, FL, 2007.

[12] Y. Hu, X. Xie and Y. Xin, "Power information systems security: modeling and quantitative evaluation," Proc. IEEE Power Eng. Soc. General Meeting, vol. 1, pp. 905-910, Denver, CO, 2004.

[13] C. W. Ten, C. C. Liu, and G. Maninaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836-1846, Nov. 2008.

[14] NERC CIP series. [Online]. Available: http://www.nerc.com/page.php?cid=2%7C20

[15] E. Brier, D. Naccache, and P. Paillier, "Chemical combinatorial attacks on keyboards," International Association for Cryptographic Research ePrint Archive 2003, 217 (2003).

[16] http://blogs.techrepublic.com.com/security/?p=222&tag=leftCol;post-223.

[17] Oyster Optics, Inc., "Securing fiber optic communications against optical tapping methods," [Online]. available: http://www.rootsecure.net/content/downloads/pdf/fiber_optic_taps.pdf

[18] http://www.arcadiannetworks.com/article.aspx?MID=5000&CID=8071

[19] M. Poller, "Doubly-fed induction machine models for stability assessment of wind farms," Proc. 2003 IEEE PowerTech Conference, Bologna, 2003.