NOVATEUR PUBLICATIONS
International Journal of Research Publications in Engineering and Technology [IJRPET]
ISSN: 2454-7875
VOLUME 3, ISSUE 3, March-2017

VULNERABILITES AND MITIGATION IN COMMUNICATION SYSTEM FOR GRID INTEGRATION OF WIND ENERGY

ANAGHA. A. BOKARE
Government polytechnic gadchiroli ,Maharashtra(india)

ABSTRACT:

This paper provides the `concept of communication system challenges in power grid integration .The scada has been used as communication,fault diagnosis ,though the reliability of communication with scada in drastic environment but the problems to faced such as security ,policy, system network problems are in online internet facility. We discuss all the SCADA vulnerabilities in this paper they are attributable to the lack of a well-developed and meticulously practiced security policy also we provide some mitigation of SCADA system which is ongoing process.

KEYWORDS: Communication system, scada, vulnerabilities.

INTRODUCTION:

The scenario of wind power distribution in todays has some unique challenges. The power generation of wind required different factors of networked interconnection & telecommunication technologies for monitoring and controlling using scada technologies. The scada is used for increasing availability of machines and plants, reducing maintenance costs and quality assurance.A wind farm must rely on constant, reliable data flow for peak performance, reliability and safety even in installations covering large areas that are subject to local weather variations. Sensors monitor blade operation, system variables such as vibration, and outside environmental factors such as ice all of which can impact power generation and system safety. The data from system sensors fed into the SCADA systems for preventive maintenance action.

Energy flow through power grid to meet customer demandwhile information flows through communication system to monitor the system status ,control the dynamic energy flow presented in the grid and transfer the information collected from on interval of smart device for sensing and control across the power grid.It may occur in CMS that the available data base should span the entire monitoring period. A reduced data base will compromise the information quality and may give rise to inaccurate diagnoses.

CONDITION MONITORING:

The aim of condition-based maintenance, which has proven its merit in all areas of power generating technology for decadesis to maximize component utilization by extending the equipment’s service life. WTGs should be no exception to the rule that continuous status supervision with the support of online conditioning monitoring systems (CMS) ought to be a tool employed in any comprehensive maintenance scheme. This is a prerequisite for trouble-free equipment operability and, at the same time, high availability rates. The main task of aCMS is to detect deviations from normal operating level on the basis of structure-borne noise produced by the monitored components.

By detecting when a monitored component exceeds pre-defined limit values, the operator and technical operations manager of a wind farm will be able to implement a timely, effective and cost-efficient response in co-operation with the insurer. This will minimize the necessary repair times and costs while avoiding prolonged shutdowns and the associated consequential costs, e.g., due to the lack of spare parts. An efficient monitoring of WTGs poses special demands on the condition monitoring systems used. In order to demonstrate that a CMS will meet real-life operating requirements while ensuring a high information quality of the measurements obtained, only certified systems are to be employed.

STRUCTURE AND FUNCTION OF A CMS:

The operation of a condition monitoring system is based on the measurement and analysis of vibrations emitted by the monitored WTG components. Depending on their geometry, mounting location and rotational speeds (r.p.m.), typical kinematic frequencies can be attributed to each individual component of a WTG power train (antifriction bearings, gear wheels, shafts). These measurement signals are reproducibly detected by the installed sensors and then analysed by means of software. Significant changes in measured vibrations form the basis for diagnosis and the generation of alarm messages. In evaluating the vibration analysis, variables characterizing the equipment's operating status (e.g., wind direction, wind velocity, etc.) are likewise taken into account so that condition-related vibration changes can be distinguished from operationally induced ones.

The backbone of each CMS is the multiple signal transducers fitted on the monitored WTG components and the associated software which among other things, executes the measuring functions and signal processing.

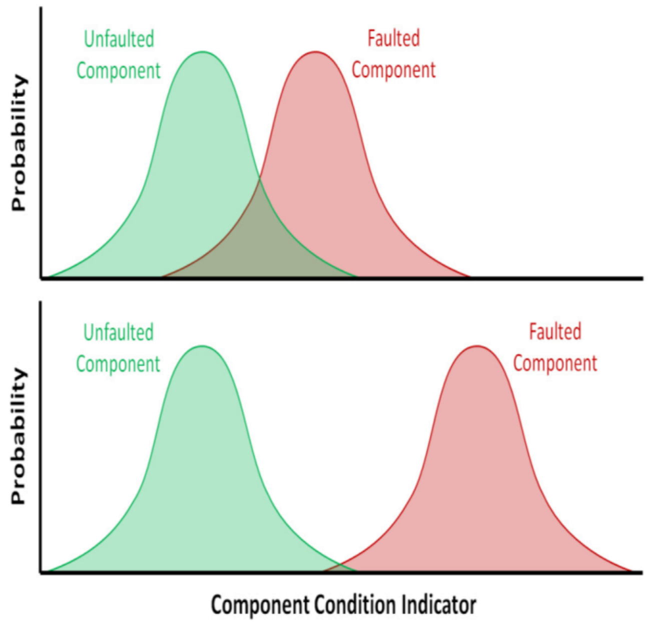

Figure 1: Effective data processing is the difference between poor fault discrimination (top) and good fault discrimination (bottom)

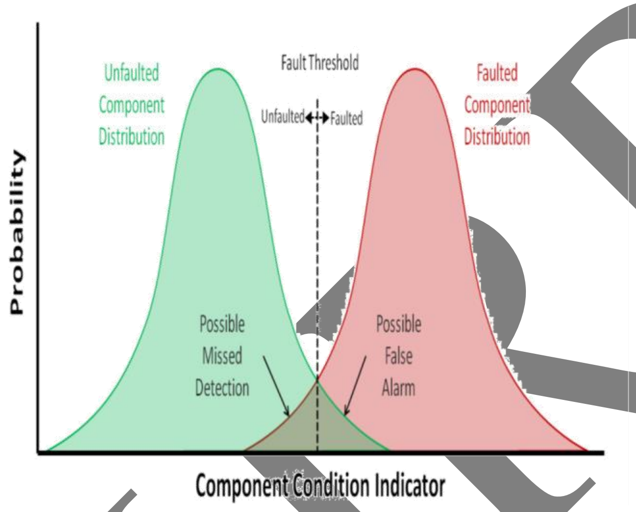

Figure 2: The threshold level and how it is chosen is critical to system performance.

SPACE MONITORING:

Interior (e.g., nacelle, tower) and exterior (transformer, substation) areas containing WTG components must be monitored by the fire detection system. The fire alarm sensors employed have to be designed for the specific ambient conditions (temperature, air humidity, etc.). For monitoring within the WTG, alarm sensors should preferably operate on the smoke detection principle. Since operating conditions will vary, e.g., as a function of the mounting location within the WTG, the suitability of the fire alarm sensors employed should as a matter of principle be examined together with the system vendor for each specific application.

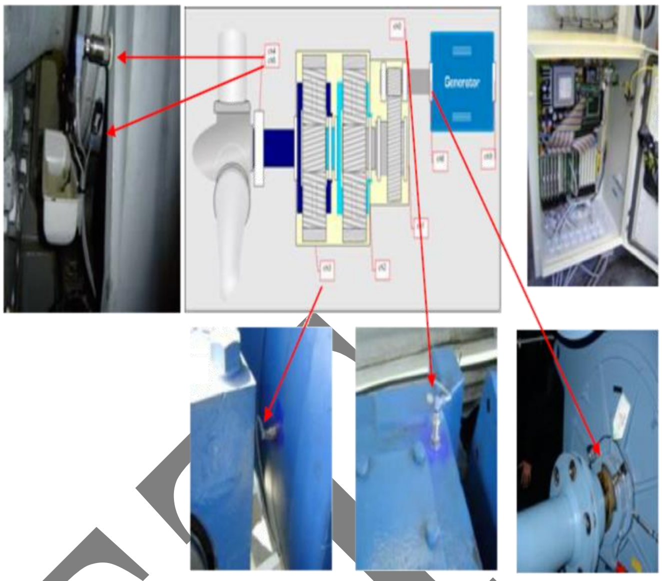

Figure 3:Schematic views of a WTG power train with online CMS and structural-noise sensors

SCADA VULNERABILITIES:

Cyber security is very expensive. However, the presence of vulnerabilities requires it.. The order ofvulnerabilities does not reflect a priority in terms of likelihood of occurrence or severity ofimpact. Typical vulnerabilities in SCADA systems aregrouped in the categories (1) policy/procedure/configuration management, (2) system, (3)network, and (4) platform to assist in determining how to provide the best mitigation strategy. Agiven SCADA system usually only exhibits a subset but may also havesome unique system specific vulnerabilities.

TYPICAL VULNERABILITIES IN SCADA SYSTEMS:

1] POLICY/PROCEDURE/CONFIGURATION MANAGEMENT:

The SCADA system has no specific documented security policy or security plan. There is no formal configuration management and no official document procedures. Hence, there are neither formal requirements, nor a consistent approach of configuration management. There is neither formal security training nor official documented security procedures.

SYSTEM:

Sensitivity levels for SCADA data are not established, making it impractical to identify which communication links to secure, databases requiring protection, etc. No security perimeter has been defined for the existing system that defines access points to the system that should be secured. Physical security alarms reside on the SCADA system; hencea failure in the SCADA system affects the integrity of the physical security.

Critical monitoring and control paths are not identified in order to determine necessaryredundancy or contingency plans.

NETWORK:

Dial-up access exists on individual workstations within the SCADA network. The dial-up access into the SCADA network utilizes shared passwords and shared accounts. Administrative and SCADA networks utilize the same. This removes thepossibility to implement extranets, data diodes, filtering, etc. Inadequate data protection exists as the SCADA data traverse other networks, both asdata is transferred to other SCADA segments and as the data is sent to servers on theadministrative network. The data is used for a variety of purposes, including public display and engineering efforts. Wireless bridging used without strong mutual authentication and/or data integrityprotection on supported data flows. Wireless LAN technology used in the SCADA network without strong authenticationor data protection between clients and access points. There is inadequate physical protection of network equipment. There is no security monitoring on the SCADA network.

PLATFORM:

Default operating system configurations are utilized, which enables insecure and unnecessary services. There is no regular virus checking. A PC is allowed connection to both the SCADA network and the Internet. There are no time limit, character length, or character type requirements for the passwords. OS security patches are not maintained as part of a formal procedure of process.

SECURITY PROVIDED IN SCADA:

Several documents involved in this section provide insights into system level security However, detailed SCADA-specific security documentation is limited. SinceSCADA systems utilize IT infrastructure and corresponding architectures, security solutionsfrom the IT community often apply to the new SCADA environment. This section lists someuseful texts in the areas of (1) security policies, (2) network security (both wireless and wired),and (3) platform security. Additional sources are available and we are not endorsing these textsand documents as better than others available. We are merely seeking to provide the reader withan initial and reasonably comprehensive coverage of the important aspects of informationsecurity applicable to modern SCADA systems.

SECURITY POLICY:

The text provided in this system should be in conjunction with formation of security policy.

NETWORK SECURITY:

The network security provide guidance on how to create a secure network and contain discussionson threats, network device configurations, cryptographic solutions, and secure networkarchitectures. Although some coverage of security polices and platform security is provided, theprimary focus is on the networking technology.

PLATFORM SECURITY:

Along with network devices, the configuration for operating systems used in SCADA systemsholds the greatest opportunity for both insecure implementations and corresponding Vulnerabilities. These vulnerabilities can include unnecessary network services, shared accounts

CONCLUSION:

The generation of wind power and utility used for fault finding diagnosis is easily possible with SCADA. The technology implemented in SCADA while desiginig has so security problems as discuss in terms. So wind power SCADA system can made a secure, environmental changing, maintaining sustainable security provided is basic requirement., In this paper we are focused on system level vulnerabilities, not point security problems, such as physical security, awell-developed security policy balances operational performance and security requirements, is necessary for sustained security. This security policy also guides the integration of technology and the development of security procedures is ongoing process

REFERENCES:

1) *Communication vulnerabilities and mitigations in wind power scada system same Rican wind energy association wind power* 2003 conferenceaustin, texassession 3b – technology performance part 1,may 19,2003
2) www.windenergy.com
3) www.renewableNRGsystems.com
4) www.inwea.org/installed capacity on 5th may2015