www.WindHSE.org

Commonwealth (Crown) Licence Wind Farm Technicians SCADA & PLC Cybersecurity

---

Guideline for the Cybersecurity Certification of Wind Turbine Service Technicians (Edition 2019)

City & Guilds President: HRH Princess Royal

Michael Mattocks, Commonwealth (Crown) City & Guilds Examiner, Microsoft HQ User Groups mentor & Forensics Penetration Tester explained the relevance of the new guidelines:

"It is important for governments. owners and manufacturers of wind turbines as well as banks and insurers involved to know the different Cybersecurity certification processes and guidelines for Wind Turbine Service Technicians. Recent endorsements by Tulsa University PHD Research on hacking Wind farms, Dept Homeland Security Accredited Cybersecurity Org (FireEye) and UL.com Wind Farm Cybersecurity Auditors signify the urgency for the Certification of all Wind Farm Technicians. If this does not happen imminently then the likelihood for a Statewide grid blackout, loss of lives and hundreds of $millions increases."

The origin of this Commonwealth Certification is the Wind Farm Technician Apprenticeship developed by the RenewableUK steering committee members including Siemens , Repower, Vestas and utilities such as RWE and the Lloyd's Underwriters representative of the European Wind Turbine Committee.
This Certification has been successfully piloted by DNV-GL the Lloyd's Underwriters certification body for Wind Turbines and Lloyd's Underwriters auditor for this Commonwealth Certification.

This Certification comes into force August 2019 and is licensed in Australia by Australian Wind Energy Institute. Australian Wind Energy Institute Board Members

Chris Blask. Nuclear Energy SCADA SME (Conference Roundtable with EDF)

Julie Mackenzie. MA Cybersecurity Law Latrobe University 2018-2019.
Counter-terrorism Force Representative. Ex-Victorian Police

Michael Mattocks. MA Cybersecurity Law Latrobe University 2019-2020

The Certification is currently seeking an upgrade with a request for consultation with Rachel Noble, Deputy Secretary & National Cyber Security Advisor at Australian Department of Home Affairs as well as Head, Australian Cyber Security Centre, Australian Signals Directorate. The Certification will take reference from the **Security of Critical Infrastructure Act 2018.**

Table of Contents

City & Guilds Qualification Level 3 Electrical Power Engineering-Wind Turbine Maintenance
2339 79 Unit 750 Health and Safety in the power industry

Demonstrate an understanding of Health and Safety

1.1 Identify statutory regulations and organisational requirements for Health and Safety
Reference: **Security of Critical Infrastructure Act 2018.**

1.6 Identify the reasons for accidents happening and the importance of putting in place preventative measures
Reference: IEEE.org: 'Cyber intrusion of wind farm SCADA system and its impact analysis'

1.13 Identify hazards associated with fire
Dead in **Fire** Wind Turbine. Police Investigation Report

1.1 Identify statutory regulations and organisational requirements for Health and Safety

It is paramount for Wind Turbine Service Technicians to understand that they have a partnership arrangement with their Operational Controllers when controlling the supply of Wind generated electricity. There are important control panel security protocols that they must be aware of as Ethernet Technicians.

Cyber Security of industrial processes is now so pertinent that inter/national government departments are forming partnerships to raise employee awareness of these threats.

http://www.hse.gov.uk/horizons/current-issues/science-and-technology/cybersecurity.htm

'Implications:

> Accidental failure or malicious attack on process control systems could result in loss of system-critical safety functions such as interlocking and emergency shutdown systems and disruption of control of the process, potentially resulting in serious risks to operators and possibly the public. Whilst it is good practice to isolate safety-critical control or protection systems from any connectivity to the 'outside world' this approach is being challenged by the changing nature of plant electronic control and management systems. This is leading to increased vulnerability of plant to electronic attack, whilst at the same time the threat level is increasing. The possibility of such electronic attack of control systems is recognised as a threat to the Critical National Infrastructure . Understanding electronic attacks.'

In Australia, Wind Farm Technicians should take their responsibilities according to the
Security of Critical Infrastructure Act 2018
Division 3—Obligation to give information and notify of events

23 Initial obligation to give information

(1) This section applies if an entity is, or will be, a reporting entity for a critical infrastructure asset at the end of the grace period for the asset.

Note: Once an entity has given information in relation to an asset under this section, the reporting entity for the asset must comply with section 24 (ongoing obligation to give information and notify of events).

(2) The entity must give the Secretary the following information in accordance with subsection (3):

(a) if the reporting entity is the responsible entity for the asset—the operational information in relation to the asset;

(b) if the reporting entity is a direct interest holder in relation to the asset—the interest and control information in relation to the entity and the asset

Civil penalty: 50 penalty units.

Wind Farm Technicians at this stage should be aware that many of the Wind Farm Computer Controllers have the same Siemens Microsoft components as those affected by **Stuxnet** which caused the infamous Iran Nuclear Centrifuges to overspin and explode.

Malware transfer by say USB or laptop r may affect the wind farm safety software code causing a statewide blackout similar to the recent one in South Australia

https://support.industry.siemens.com/cs/document/43876783/simatic-wincc-simatic-pcs-7%3A-information-about-malware-viruses-trojan-horses?dti=0&lc=en-WW

Updated	Current status of infected computers
11.03.2011	To date a total of 24 Siemens customers in the industrial sector worldwide have reported being infected with the Trojan horse. The malware was able to be removed in all cases. In none of these cases did the infection have an adverse impact on the automation solution.

Recommended procedure to identify and remove a Stuxnet infection
We recommend examining the following types of computers: 1. Embedded systems (e.g. Microbox) 2. Other computers Infrastructure computers (file servers, domain controllers, other servers...) Computers with and without WinCC installation

The following safety precautions also apply:

- All connections with the outside world must be checked and cleaned (customer data, USB devices, others).
- If possible, do not use any third-party USB sticks and/or mobile data carriers.
- Always check the safety concepts. For example, disable/uninstall services that are not needed.
- Installation of the Microsoft Patch is recommended for the operating systems listed by Microsoft

http://www.us-cert.gov/control_systems/pdf/ICSA-12-158-01.pdf

These vulnerabilities may be remotely exploited.

AFFECTED PRODUCTS

Siemens WinCC 7.0 SP3 web server and web applications are affected. These vulnerabilities may allow an attacker to gain unauthorized access, read from, or write to files and settings on the target system.

BACKGROUND

Siemens SIMATIC HMI is a software package used as an interface between the operator and the programmable logic controllers (PLCs) controlling the process. SIMATIC HMI performs the following tasks: process visualization, operator control of the process, alarm display, process value and alarm

archiving, and machine parameter management. This software is used in many industries, including Wind Farms. Nuclear , oil and gas, and chemical.

WinCC web applications are susceptible to reflected cross-site scripting because they do not filter out characters when parsing URL parameters. Exploitation of this vulnerability may give an attacker authenticated access to WinCC web applications.

The object-oriented SCADA system Simatic WinCC Open Architecture allows you to implement integration of a wide variety of components

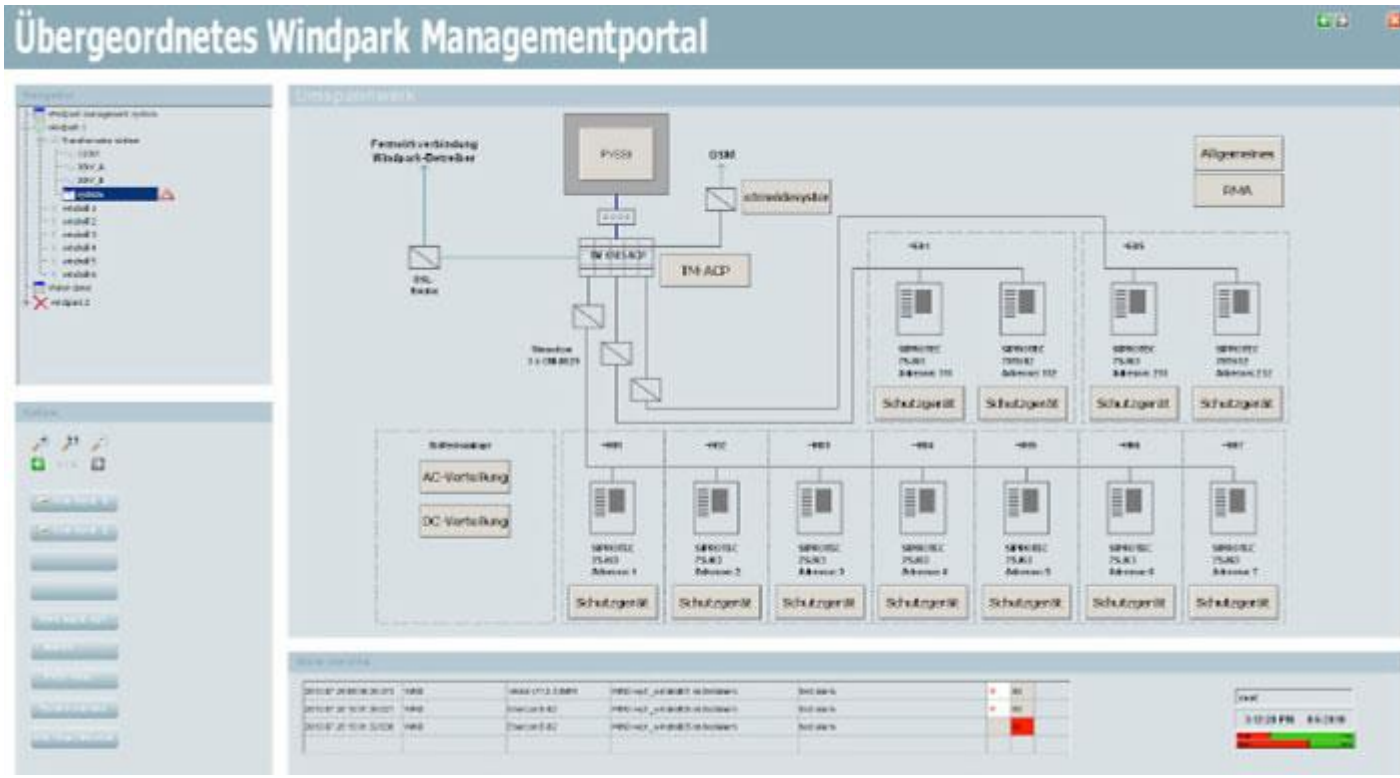
However this comes at a cost of potential intrusion & technicians need to be mindful of this during their operations:

http://www.industry.siemens.com/verticals/global/en/wind-turbine/wincc/pages/default.aspx

Efficient Wind Farm Management

Central Control Desk with SIMATIC WinCC Open Architecture

SIMATIC WinCC Open Architecture from Siemens is a SCADA system that can be flexibly adapted to your specific requirements. This system is ideally suited as a central control desk for high-availability wind power plants. If personnel are distributed over a large geographical area or if a large number of wind farms have to be managed, the scalability of our SCADA system across several spatially distributed servers is a distinct advantage. Your benefit: From a central control desk, you have full access to all measured data, alarms, histories, and configurations of your wind turbines



WinCC and PCS 7 are the first SCADA systems to be specifically targeted by malware. The Stuxnet worm can spy on and even reprogram infected systems.It can cause Blades to overspin in replay control instructions where Blades can cause physical damage to a tower. Stuxnet can provide false feedback to controllers 'ensuring that they will not know is going wrong till it's too late to do anything about it' (IEEE.org)

Forensic Protocol for Wind Farm Technicians

In the event Wind Farm Technicians find anomalies on the Wind Turbine Control Panel and PLC Controller when for example examining or changing the parameters it is important that they report this to their supervisor and operational controller. This is the case irrespective of the system including TCP/IP cabling, ethernet or Standard com port + adapter.
The control parameters and system should be left alone so that a forensic mode penetration test can be made by external investigators.
These supervisors should then have the responsibility to complete a report for the Secretariat of the Critical Infrastructure Act 2018.

1.4 Demonstrate and implement safe working practices with respect to safe working areas.

Security

Security measures should be sufficient to prevent access by any unlawful visitors without causing them harm.

All security measures should be put into effect prior to construction work starting and should be updated as necessary throughout occupation of the site. The measures should:

• ensure provision to prevent unauthorised access to the site;

• ensure materials are stored without risk to Health and Safety;

• ensure construction plant is secured against unauthorised operation;

• establish procedures for control of visitors;

• establish procedures for visiting workers; and

• ensure provision to monitor the effectiveness of the security arrangements.

Additional measures will be required when reviewing security arrangements during the construction and operational phases offshore.

These Additional measures whether for offshore or onshore wind farms increasingly include measues to prevent unauthorised Electronic access of the PLC.

Unfortunately these Security Measures have not been consistently applied across the globe and Tulsa University PHD Research has demonstrated that a whole Wind Farm have been placed at risk which ultimately could lead to a StateWide Blackout from potential Terrorists.

DEF CON 25 Conference - Jason Staggs - Breaking Wind: Adventures Hacking Wind Farm Control Networks

https://www.aer.gov.au/wholesale-markets/compliance-reporting/investigation-report-into-south-australias-2016-state-wide-blackout

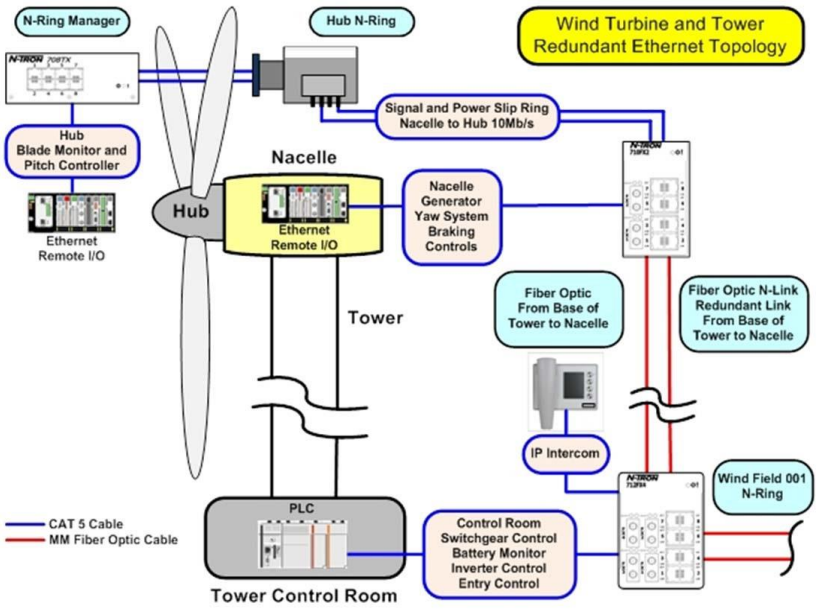
Wind Technicians should not be in any doubt that Wind Farms have already been and are a major target for cybercriminals and terrorists. This is well demonstrated during this Dragos Cyber security expert video (see part 33mins 20) explaining a bitcoin cyberattack on a Nordic Wind Farm demonstrates.

1.6 Identify the reasons for accidents happening and the importance of putting in place preventative measures

17th November 2015 UK Chancellor warns of pending cyber attacks on the control panels of the National Grid http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11999607/islamic-state-cyber-attack-plot-britain-george-osborne-warns.html

Control intelligence may be distributed around the turbine, including in the hub. Control panels contain controller PLCs plus standard panel hardware to interface with sensors and auxiliary systems and combined may weigh up to 500kg. In some cases, CANbus or similar systems are used for interfacing between controller hardware and sensors, including via fibre-optic cables.

In parallel to the control system, a safety system protects the turbine from control system or operator error. Key sensors for this overriding safety system include speed and vibration sensors. This make up is illustrated here



As IEEE.org paper "Cyber Intrusion of Wind Farm SCADA System and Its Impact Analysis" indicates there is a Technician responsibility to maintain PIN and ethernet security with regards to Control Panel control of components

This can be done through avoid leaving chemical based fingerprints on pin pads. Thus wiping clean pin pads should become second nature.

Best practice would also mean avoid using USB sticks collected at conferences or 'on the ground' that could be infiltrated with malware such as Stuxnet or Flame.

Encryption and anti-virus checks of all files on PDAs would become common practice to avoid malware that could be used for espionage and direct 'replay attacks'. These attacks could lead to distorted PLC instructions and direct physical damage as oversped blades that may crash into the Towers or cause short circuit generator fires.

System logs (syslogs) on the Control software should be checked and any anomalies should be immediately elevated to the Computer Incident Response Team

This has been recently highlighted in May 2015 Windpower Monthly edition 'Wind farm owners should also emphasise the importance of never using USB drives or other peripheral media devices of unknown origins on secure systems - it still surprises me how many employees collect and use USB drives from unknown sources'

UL.com expert Wind Farm Penetration Testers demonstrate in their video (see point 8 min 31 secs) that when consulting with Wind Farm Owners regards their Cybersecurity Protocols that Wind Farm Technicians have uploaded malware to the turbine from their laptop causing turbine outages.

This has been acknowledged by the American Wind Energy Association.

https://www.windpowermonthly.com/article/1464061/awea-2018-increase-cyber-security-attacks-inevitable-expert-warns

A video from Infosec Institute highlights how Stuxnet can boot automatically from a USB Stick.

It is therefore recommended that Technicians use premium encrypted USB sticks that are easily identified as their own only.

1.13 Identify hazards associated with fire

There are many possible sources for fire hazards in a WTG as there alot of flammable liquids and gases. It is important that the WTG Technician uses all sensors and actuators to diagnose and minimise any risk of fire

We should re-examine the cause of a fires described in recent online publication:

Dead in Fire Wind Turbine

30/10/2013

Two service technicians have died following a turbine fire at Deltawind's 21MW Piet de Wit wind farm near Ooltgensplaat in the Netherlands.

The mechanics, aged 19 and 21, were working on one of 12 Vestas V66-1.75MW units at the site when the fire broke out yesterday afternoon.

Deltawind said it is possible that a short circuit on the unit caused the fire but warned it is awaiting the result of a police report into the incident.