Smart Grids

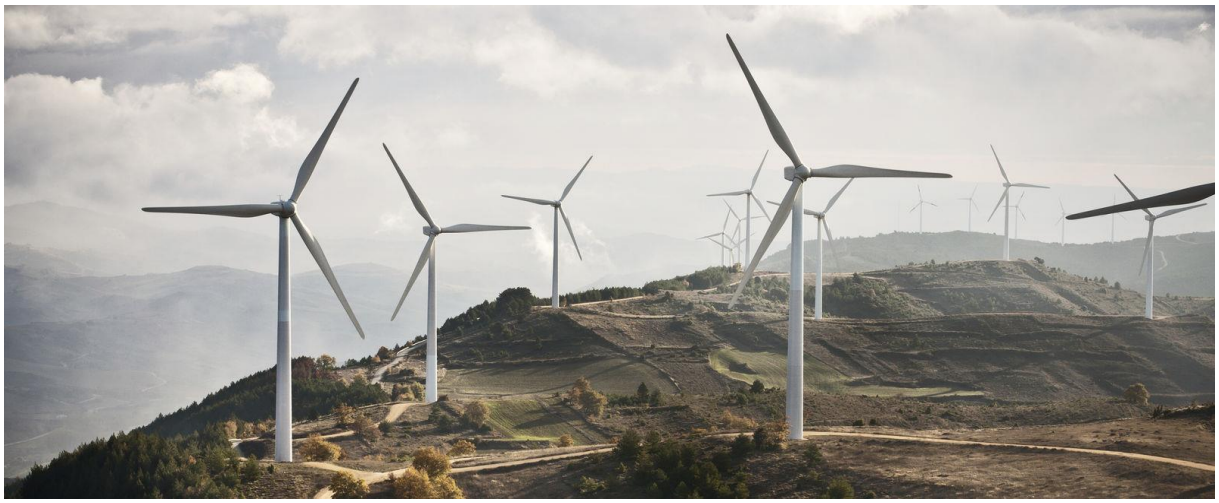
Teil 3: Erneuerbare Energie und Cyber Security

www.copadata.com
sales@copadata.com

zenon
do it your way

Nach den ersten beiden Artikeln über Smart Grid beschäftigen wir uns in diesem Whitepaper mit zwei weiteren Themen. Zum einen mit dem Thema erneuerbare Energien welches durch die aktuellen Diskussionen rund um das Thema Atomkraft einen zusätzlichen Boost bekommen hat. Und zum anderen mit dem Thema Cyber Security im Smart Grid.

1. Atomenergie ade?!



Für einige Länder ist die Atomkraft nach wie vor eine zukunftsträchtige Quelle für kostengünstigen Strom. Andere Länder, wie zum Beispiel Deutschland, wollen ihre Atomkraftwerke so schnell wie möglich vom Netz nehmen. Die aufklaffende Lücke in der Energieversorgung soll mit erneuerbaren Energien geschlossen werden. Das größte Potential die Lücke zu schließen hat, neben der Fotovoltaik, die Windenergie. Um alle 17 deutschen Atomkraftwerke zu ersetzten müsste die Anzahl der Windturbinen in Deutschland ca. verdoppelt werden. Auch wenn der Ausstieg nicht von heute auf morgen passieren wird und auch wenn die Erzeugung der fehlenden Energie nur zum Teil durch Windkraftanalgen erfolgen wird, wird der Ausbau der Windenergie stetig fortschreiten. Die Anzahl der bereits knapp 22.000 installierten Turbinen wird sich in den kommenden Jahrzehnten sicherlich vervielfachen.

Hierzu sei erwähnt, dass das Softwaresystem zenon eine große Bedeutung bei den Aufgaben „Lokale Turbinensteuerung“ und „Parkmanagement“ hat. Die lokale Turbinensteuerung in der Gondel oder im Turm einfach und effizient zu visualisieren ist eine wesentliche Stärke von zenon. Durch seine Skalierbarkeit spielt es seine Stärke als One-Tool-for-many-Platforms

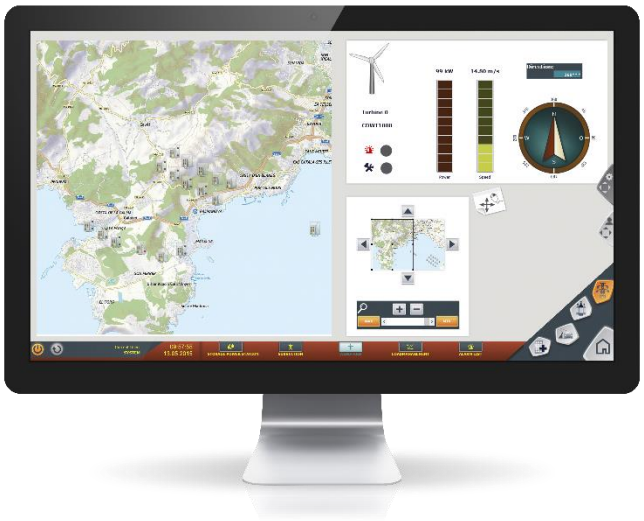
gekonnt aus. Was darin resultiert, dass im übergeordneten Parkmanagement ohne weiteres Zutun auf die GUI (Bedienoberfläche) der Turbinensteuerung zugegriffen werden kann. Die flexible Gestaltung der Parkmanagementanwendung durch die Werkzeuge und Module von zenon werden durch eine Vielzahl an integrierten Kommunikationsmöglichkeiten abgerundet. So ist zum Beispiel die Kommunikation über IEC 61400-25 einfach und schnell zu konfigurieren. Aber auch eine möglicherweise benötigte direkte Weiterleitung der Daten aus dem Parkmanagementsystem über ein Fernwirkprotokoll wie IEC 60870-5-101/-104 deckt das System ab.

Neben dem Ausbau der erneuerbaren Energien innerhalb eines Landes werden aber auch immer wieder Konzepte mit einem großen Anteil von Energieimporten vorgestellt. Zum einen denkt man darüber nach, die Grundlast in Zukunft mit den französischen Atomkraftwerken abzudecken.

Für Frankreich ist der Atomausstieg keine Option. Mit fast 60 in Betrieb befindlichen Atomreaktoren ist Frankreich erstens abhängig von dieser Energiequelle, und zweitens wird sehr viel Geld mit dem Energieexport aus Atomenergie verdient.

Zum anderen verfolgt man eine hundert Jahre alte Idee Strom aus der Wüste zu nutzen. Unter dem Namen „Desertec“ werden solarthermische Kraftwerke in Wüsten gebaut. Innerhalb von sechs Stunden erhalten die Wüsten mehr Energie von der Sonne als die Menschheit in einem Jahr verbraucht. Oder andersrum: Die Wüsten dieser Welt könnten theoretisch das 300-fache an Energie erzeugen was die Menschheit benötigt[1]. Der Plan ist es die Sonnenenergie der Sahara in elektrischen Strom umzuwandeln und zu den großen Energieverbrauchern zu leiten. Die großen Energieverbraucher liegen nördlich der Sahara – in Europa. Wie soll man also diese Energiemengen über mehrere tausend Kilometer möglichst verlustfrei transportieren? HVDC (High Voltage Direct Current) oder auf Deutsch HGÜ (Hochspannungs-Gleichstrom-Übertragung) ist die Technologie, die geringere Verluste bei der Übertragung verspricht. Man spricht von 3% Verlust auf 1000 Kilometer. Das ist ungefähr ein Zehntel der Verluste einer 380 kV Leitung herkömmlicher Technologie mit Wechselstrom. Diese HVDC-Leitungen könnten in Zukunft die „Energie-Nabelschnüre“ für Europa werden. Besonders zu den Zeiten, in denen in Europa kein Wind weht. Daher werden diese Leitungen gut überwacht werden z. B. mit SCADA-Systemen wie zenon.

[1] Dr. Gerhard Knies; Physiker; Hamburg



Damit aber nicht nur der Prozess (die Übertragung von Energie) überwacht ist, sondern auch das System als solches von außen geschützt wird, müssen Vorkehrungen zu Prävention von Cyberkriminalität getroffen werden.

2. Cyber Security

Durch das Zusammenwachsen der Energieversorgung mit dem Internet entsteht zwangsläufig ein Angriffspotential durch Attacken von Hackern. Neben Stromdiebstahl stellen die größte Bedrohung Hacker mit terroristischer Motivation dar. Daher wird in einer Vielzahl von Forschungsprojekten und Arbeitsgruppen erörtert wie man dieser Bedrohung Herr wird. Auf Grund der Sensibilität gegenüber terroristischen Aktivitäten ist die USA hier gegenüber Europa praktisch schon eine Runde weiter. Die im Energiebereich vielgeachteten CIP (Critical Infrastructure Protection) Standards von der NERC (North American Electric Reliability Corporation) bilden die Grundlage für Hardening Guidelines europäischer Hersteller und Integratoren.

Dass in diesem Bereich definitiv Handlungsbedarf besteht, zeigt eine Studie von Red Tiger Security[2] auf. Schon in der aktuellen, klassischen Konstellation Energie-Erzeugung, Energie-Übertragung und Energie-Verteilung findet man eine Vielzahl von Sicherheitslücken. Das interessante daran war unter anderem, dass Sicherheitslücken im Schnitt erst 331 Tage nach deren Bekanntwerden geschlossen wurden. So lange hätten also Hacker Zeit gehabt Attacken

[2] Electricity for Free? The Dirty Underbelly of SCADA and Smart Meters; Jonathan Pollet, CISSP, CAP, PCIP; July 2010

durchzuführen. Die meisten Sicherheitslücken befanden sich zwischen dem Firmennetzwerk und dem HMI-Netzwerk. Zwischen diesen beiden Domänen befindet sich meist das Netzwerk für Archivierung, Domain Controller, Webserver und diverse Applikationen für z. B. Optimierungs- und Prognosedienste. Da dieser Bereich quasi die Schnittstelle zweier Welten ist – IT Welt und SCADA Welt – und diese beiden Welten von unterschiedlichem Personal gewartet werden, fehlen hier oft klare Verantwortlichkeiten. Das führt dann dazu, dass es beispielsweise zu unregelmäßigen Wartungszyklen kommt und Security Patches erst zeitverzögert eingespielt werden. Allein diese Erkenntnis beweist wieder einmal, dass Security nicht nur mit Technik und Technologie zu tun hat, sondern sehr viel mit Zuständigkeit, Verantwortung, Arbeitsabläufen und Dokumentation.

Klarerweise müssen Verantwortlichkeiten und Abläufe immer intern geklärt und definiert werden. Darauf aufbauend sollte man sich dann aber auf ein System verlassen können, welches die entsprechenden Security-Anforderungen erfüllt wie z. B. zenon.

Hier ein paar Eigenschaften die zenon mitbringt um für die Erstellung sicherer Applikationen gewappnet zu sein:

- Ablagen im binären Format
- Verschlüsseltes Netzwerkprotokoll
- Passworte verschlüsselt abgelegt
- Kein SQL Server zur Laufzeit
- Userverwaltung – Active Directory bzw. ADAM
- Dokumentation über Systemkomponenten
- Separierung von Applikation und Engineering
- Wenn möglich: Authentifizierung und Verschlüsselung von Kommunikationsprotokollen

Außerdem unterstützt COPA-DATA seine Kunden bei der Erstellung sicherheitsrelevanter Unterlagen. Die Herausforderungen werden in Bezug auf das Thema Security für Energieversorgungsunternehmen definitiv mehr. Wir wollen Sie dabei unterstützen.

Wenn Sie mehr über intelligente Stromnetze, die Sicherheitsfeatures von zenon oder die zenon Energy Edition erfahren möchten, besuchen Sie uns auf www.copadata.com/energy oder schreiben Sie uns an energy@copadata.com.