Smart Grids

Part 3: Renewable Energy and Cyber Security

www.copadata.com
sales@copadata.com

zenon
do it your way

Following COPA-DATA's first two articles about Smart Grids, we will review two more topics in this white paper. Firstly, the very current topic of renewable energies – which has received an additional boost as a result of the current discussions about nuclear power. And secondly, the topic of cyber security in the Smart Grid.

1. Goodbye nuclear power?

For some countries, nuclear power remains a seminal source of cost-effective electricity. Other countries, such as Germany for example, want to take their nuclear power plants out of the grid as soon as possible. The gaping hole in energy generation is to be filled with renewable energies. The greatest potential for closing the hole is, in addition to photovoltaics, wind energy. In order to replace all 17 German nuclear power plants, the number of wind turbines in Germany has to be more or less doubled. Even though the pull-out from nuclear power will not – and cannot – be carried out overnight, and even though generation of the energy shortfall can only be made up in part by wind power plants, the growth of wind energy will continue. The number of wind turbines already installed, just under 22,000 in Germany alone, will certainly multiply in the coming years.

It should be noted that COPA-DATA's software system zenon, plays a significant role in "local turbine control" and "park management". Efficient visualization of local turbine control in the nacelle or in the tower is one of zenon's major strengths. Due to its scalability, zenon ably plays on its strength as one tool for many platforms. This results in the GUI (user interface) of the turbine control being accessible with overlaid park management without additional software being required. The flexible design of the park management administration through the tools and modules of zenon are enhanced by a multitude of integrated communication possibilities.

For example, communication via IEC 61400-25 can be configured quickly and easily. However, direct forwarding of data to a telecontrol protocol such as IEC 60870-5-101/-104, if required, completes the system.

In addition to the expansion of renewable energies at a national level, solutions being presented are increasingly dependent on energy imports. In Germany, one option being considered for the future is fulfilling the basic load with power from French nuclear plants.

Abandoning nuclear power is not an option for France. With nearly 60 nuclear reactors in operation, France is dependent on this source of energy and also earns a great deal of revenue from exporting energy produced by nuclear power plants.

Another option being pursued is the hundred-year old idea of producing power from the desert. Solar-thermal power plants are being constructed in the desert under the name of “Desertec”. Within six hours, the deserts will receive more energy from the sun than humanity consumes in a year. Or to put it another way: The deserts of the world could theoretically generate 300 times the amount of energy that humanity requires[1]. The plan is to convert solar energy from the Sahara into electrical energy and to route this to the major energy consumers. The major energy consumers are north of the Sahara – in Europe. How can these amounts of energy be transported over several thousands of kilometers whilst keeping loss as low as possible? One technology that promises low losses during transfer is High Voltage Direct Current (HVDC). A loss of 3% over 1000 kilometers is cited. This is approximately a tenth of the loss from a 380 kV cable using conventional A/C technology. HDVC lines between Africa and Europe could become an “umbilical cord” for Europe in the future. This will hold especially true at times when there is no wind in Europe.

[1] Dr. Gerhard Knies; Physician; Hamburg

These lines will therefore need to be well monitored, using, for example, SCADA systems such as zenon. In order for not only the process (i.e.: the transmission of energy) to be monitored, but also the system to be protected from external threats, precautions to prevent cyber-crime must be taken.

2. Cyber Security

Due to the convergence of energy generation and web technologies within the Smart Grid, energy companies must now consider the risk of attack from hackers. In addition to the theft of energy, the greatest threat comes from hackers with a terrorist motive. For this reason, discussions in a number of research projects and working groups are concerned with overcoming this threat. Due to its sensitivity in relation to terrorist activities, the USA leads the field ahead of Europe in this. The CIP (Critical Infrastructure Protection) Standards from the NERC (North American Electric Reliability Corporation), to which much attention is given in the energy sector, form the basis for the strengthening of guidelines for European manufacturers and integrators.

A study from Red Tiger Security[2] shows that there is a need to take action. There are already a multitude of loopholes in the classic set-up of energy generation, energy transmission and energy distribution. What was interesting about this study was, amongst other things, that security loopholes were closed on average only 331 days after they became known. Hackers

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

would have had time to carry out attacks during this 331 day period. Most shortfalls in security were between the company network and the HMI network. Between these two domains, there is usually the network for archiving, the domain controller, web server and various applications for tasks such as optimization and forecasting services. Because this area is something of an interface between two worlds – the IT world and the SCADA world – and these two worlds are maintained by different personnel, there is often no clear accountability here. This then leads to things such as irregular maintenance cycles, or security patches only being implemented after a delay. This finding alone proves once again that security is not just a matter of systems and technology, but instead one of accountability, responsibility, working processes and documentation.

Clearly, responsibilities and processes must always be clarified and defined internally. It should then be possible to rely on a system which meets the corresponding security requirements, such as zenon.

Properties that zenon possesses in order to create more secure applications include:

- Storage in binary format
- Encrypted network protocol
- Password stored in encrypted form
- No SQL server when the program is running
- User administration – Active Directory or ADAM
- Documentation of system components
- Separation of applications and engineering
- Option for authentication and encryption of communication protocols

Furthermore, COPA-DATA supports its customers in creating security-related documentation.

The challenges in relation to system security for energy supply companies are definitely increasing. We want to support you with this.

If you would like to find out more about Smart Grids, the security features of zenon or zenon Energy Edition, visit us at http://www.copadata.com/energy or email us at energy@copadata.com.