Newton-Evans Research Company's

Market Trends Digest

February 2016

Newton-Evans research company

www.newton-evans.com

Introducing Guest Authors For This Edition Of Market Trends Digest

by Chuck Newton

For this special edition of Market Trends Digest, we have three guest articles for our readers. Two relate closely to the topic of cyber security and the third is a follow-on article to the January 2016 edition discussing the vital role of equipment testing.

Our first article "Mitigating the Risk of Cyber Attacks on Power Substations" has been submitted by Amit Slutzky of Radiflow. The article discusses the recent cyber intrusion into the Ukrainian electric power grid, focusing on gaining an understanding how the network was penetrated, what the intrusion actually did once the network was successfully breached, and how the cyber-attack was carried out. The author proposes prevention methods and solutions offered by Radiflow.

The second guest article is entitled "Development Field Testing for Asset Management and Integration of Renewables. The article follows on to the recent MTD article on the role of various lab testing methodologies for assuring quality and reliability of T&D equipment. This article was submitted by Paul Leufkens, an independent technical consultant who has been the North American commercial manager for KEMA PowerTest – a component of DNV GL and a leading equipment test lab facility in North America.

The third guest article, "Protecting the Power Grid against Cyber Attacks" is by Omri Green of ICS^2. This article discusses the development of an industrial intrusion detection system (or IIDS) is now pivotal in gaining an understanding of process behavior for EMS/SCADA systems.

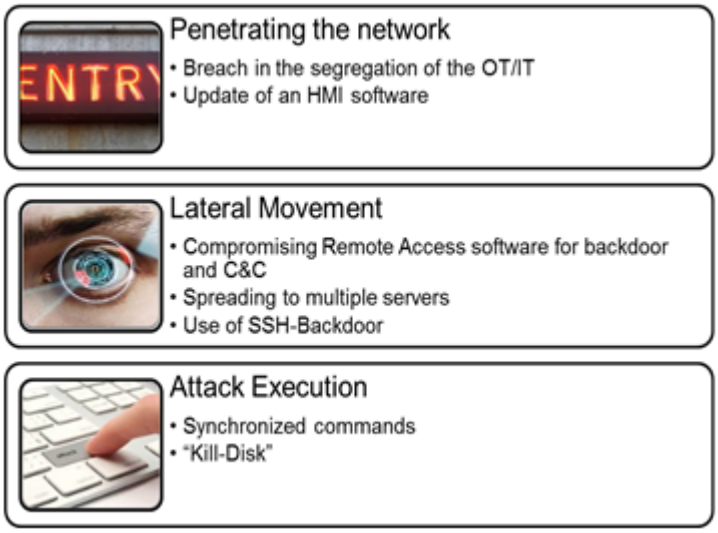
Future editions of Market Trends Digest will include occasional guest articles if our readers find the information to be relevant to their needs.

Mitigating the Risk of Cyber Attacks on Power Substations

by Guest Contributor Radiflow

The 2015 Ukraine Outage

The worldwide power industry received a wakeup call just days before Christmas 2015, when multiple western Ukraine power utility sites were cyber-attacked, causing a severe outage which left 80 thousand customers without power for hours. The attackers targeted specific servers on the utilities' operational networks and managed to delete their attack paths, which delayed the prompt reaction to the cyber attack. Evidently, the attackers used compromised HMI software, as well as remote access to interact with the network during the attack.



The attackers disconnected seven 110kV substations and twenty-three 35kV substations. During the blackout, the attackers also launched a Denial of Service (DoS)-type attack on the dispatch center, and blocked calls from customers trying to report on the power outage.

Could such an attack be prevented?

The Ukrainian outage could have been prevented at multiple points along the "Kill-Chain." During the Network Penetration phase, effective segregation of the OT network would have enabled detecting the attackers' attempts to penetrate the network. This type of 'ICS Internal Zoning' segregation has already been suggested by the ICS-CERT in August 2014. All it requires is deploying firewall protection between disparate sites (preferably a Deep-Packet-Inspection (DPI) Industrial Firewall), and implement an extensive VPN and authentication mechanism.

That said, while network segregation is an extremely important measure, as it would have enabled detecting and preventing the next attack phases, even without it, the Ukrainian operators could have still detected the attack.

An even higher level of protection would be provided by using Industrial IDS. Using network visualization, the Ukrainian operators would have been able to see that the attackers had opened an SSH connection between different stations in their network. In addition, the operators could have detected the communication channel to the attackers' Command-and-Control servers.

Another important measure is signature-based detection for detecting known malware communicating inside the network. It is known that the Ukraine attackers used the Black-Energy malware as well as known SSH-Backdoors. Both have signatures, and both could have been detected.

Finally, at the attack stage, the operator could have seen the exact commands that were sent by the attacker. In the aftermath of the Ukraine attack, researchers found it difficult to conduct forensic research due to lack of data. With an Industrial IDS the operators could have analyzed the traffic that caused the outage and track all of the attackers' actions. This would have made the forensics and the mitigation stages much easier and shorter.

Summary

Preventing cyber attacks on control systems which manage critical infrastructures is possible and feasible. Upon detecting an attack, power utility operators can instantly activate preset cyber defense actions. Utilities which are "well-prepared for the unexpected" already use industry-specific add-on hardware and software to mitigate the risk of cyber attack on their facilities.
For further information about effective processes and solution adopted by power utilities worldwide, please visit
www.radiflow.com

Development Field Testing for Asset Management and Integration of Renewables

by Guest Contributor Paul Leufkens

We read with interest "T&D Testing Topics" *(Market Trends Digest – Jan 2016, p.2)* about its importance to the electrical power industry. Now we look ahead to areas of equipment testing in which we expect significant development in 2016, especially for utilities.

Asset Management (AM) is the biggest interest: better methods must be found to determine the remaining life of equipment and to develop targeted maintenance programs based on testing experience and condition assessment. When considering the integration of renewables (including ESS), effective testing of the variability of equipment must be demonstrated. Most importantly, testing of integrated systems locally needs to be addressed. "Big Data" generated by the new Smart Grid applications need "Big Effort" to process, but, in turn, will provide "Big Opportunities" for better Asset Management.

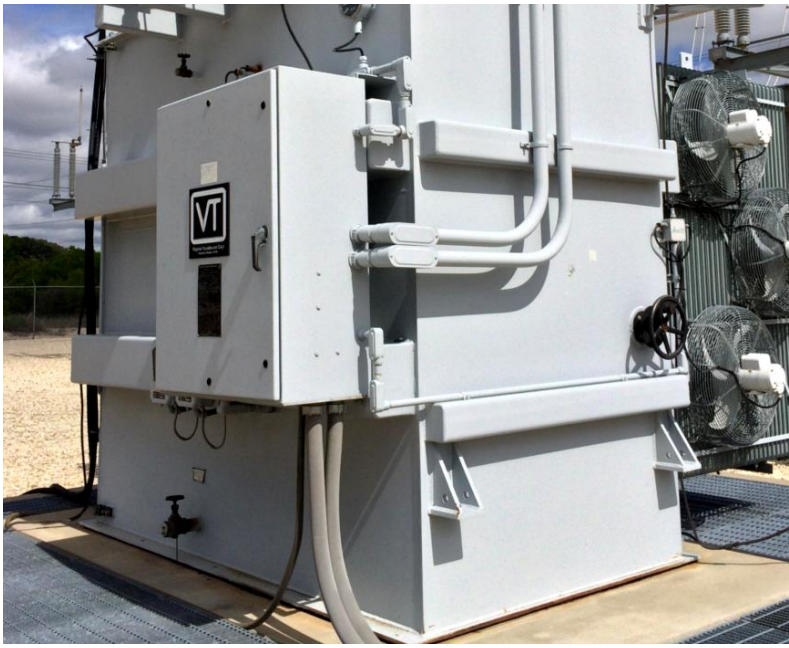
The primary interest of grid operators is to offer a maximally available well-functioning network at minimum costs. Asset Management (AM) is the name of the game and that means maximizing the lifetime of assets, preventing outages and optimizing the maintenance effectiveness. In addition, utilities have now obtained a newer role: to interconnect renewables safely into the grids, while much is still unknown about lifetime performance or how renewables combine with traditional T&D systems. Additionally, since superstorms Katrina and Sandy, utilities have to provide proper response and demonstrate resilience to abnormal weather conditions.

The first part of AM, acquiring new material, is largely covered by manufacturers' type-tests and effective commissioning tests. The reliability of the assets during usage is dependent upon their age, conditions on the moment of purchase, specific wear, weather circumstances at their location, and maintenance in the field.

Utilities work continuously to leverage their assets. Investor-owned utilities have to grow earnings even when there is no corresponding revenue growth. Suddenly everybody is on his own: no standards, only best practices; always under the strict and severe supervision of a Public Commission, while at the mercy of local circumstances and considerable history. This is made even worse for utilities with an aged infrastructure or missing historical records. What field

testing can be done to predict remaining equipment lifetime and support a maintenance methodology? Investigation and meta-analysis is required. Specific investigation must be done to discover insights concerning weather resiliency of components.

Condition monitoring and maintenance strategies re-inforce reliability. Also, the smart use of loading practices can be an AM solution. Reliability surveys on aged components (Cigré) provide input on failure modes and can thus prioritize maintenance targets.



The rapidly growing Smart Grid applications create another challenge but also provide an opportunity. IT integration requires effort, without always knowing what one can expect to achieve. Furthermore, the Big Data may be so large and complex that traditional data processing applications prove to be inadequate. Challenges include analysis, capture, transfer, visualization, querying and information privacy. Now is the time to develop methods to use Big Data for effective AM.

The integration of renewables currently provides utilities with a new concern. What requirements should be placed on the product when purchasing, as often this is a first generation product? Utilities must make difficult choices between technologies that haven't yet had the opportunity to prove themselves, or when interoperability with the existing environment is questionable. For instance, it is not yet clear whether the best choice for storage is lithium ion or flow batteries. Testing technology needs to develop together with the product manufacturing technology itself but testing techniques often lag the product development cycle. Moreover, the multi-MW size of renewables makes field testing quite expensive, requiring significant investments.

Part of the solution to these problems can be found in a “telescope” approach: test on a smaller scale what you can, and work in modules. This way, only testing of the reliability of integrated modules is necessary. Two considerations arise. One is that proper functioning of power electronics is strongly related to interaction in an immediate grid vicinity. This condition can only be tested at a specific location and under various loading conditions. The second problem is that proper functioning of inverters is highly influenced by their controls and software which again is a function of the local grid interaction.

The year 2016 without question brings a demand for market research into the areas of field testing and the processing of its output into Asset Management programs.

Paul Leufkens, President of the consulting firm Power Projects
Leufkens, has 35 years’ experience in the power sector. He has developed products for the T&D cable industry and for switchgear manufacturers. More recently, he has worked internationally in Business Development and Management for consulting and testing companies, including 13 years with KEMA in the Netherlands and in Chalfont, PA.

While involving support from a network of experts in related areas, Leufkens provides Consulting, Professional Services and Coaching in:

- *International business development and marketing,*
- *Innovation of products, services and processes*
- *Project and executive management*
- *High voltage and power technology, components, engineering, and testing*

Protecting The Power Grid Against Cyber Attacks

by Guest Contributor ICS²

Introduction

Utility control experts agree that widely used cyber defense measures such as SCADA-aware firewalls, DMZ, Antivirus and standard IDS are all effective, but have technology limitations when applied for power grid defense. The legacy type EMS /DMS were built for operational performance reliability and safety, and cyber defense was not specified as a requirement. Existing systems are often using 10-15 years old hardware and software, and adding cyber defense shall be done without system architecture changes. New technologies utilizing Process Behavior Analysis that use Big Data technology deliver an effective solution to these challenges.

Source of Information

Detecting unusual conditions in a control system, resulted from a process disruption, sensor failure, operator mistake or cyber-attack is not an easy task. In order to detect undesirable events, the system must analyze a large amount of data collected by the control computers and historian databases and perform fast data analysis.

Detection Versatility

In order to effectively dealing with such unexpected threats and risks, cyber defense measures must be capable detecting both internally as well as externally generated attacks. It can be done by utilizing unique algorithms that besides detecting cyber attacks are capable to identify operator faults, misconfigurations and sensor malfunctions, and to minimize unplanned outages and prevent equipment damage.

More Effective than Antivirus

Relying only on the Antivirus is a problematic approach, because control systems are rarely upgraded with new signatures. Any software change represents a risk to the safety and reliability of the control process and therefore deployment of any type of new software code takes months after its release.

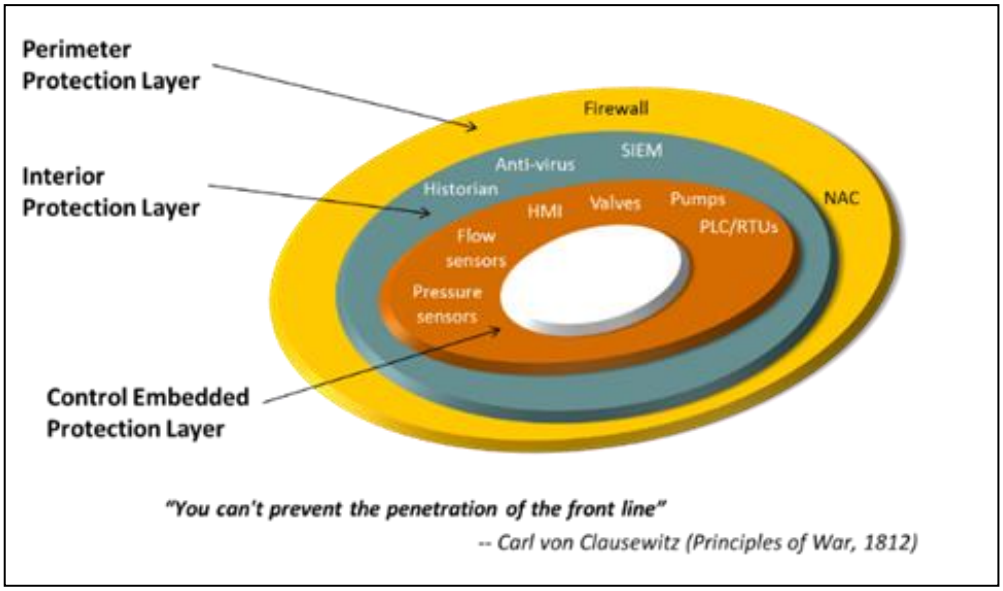
Broad coverage of detected anomalies

The cyber defense for EMS/DMS must deal with a range of anomalies while the baseline for detection is constantly tuned through a self-learning process. This makes the process highly efficient and effective for at detecting a broad range of malfunctions and cyber attack vectors.

Enhanced detection
Deployment of a cyber defense process which does not interfere with the control operation is a critical and a "must" requirement. Process behavior analysis is a reliable approach for modern and legacy type EMS/DMS, and is called an Industrial Intrusion Detection System (IIDS). It performs analysis on raw data, alert on any anomalies and provide tools for cyber threat detection and root cause analysis.

Data Collection across the ICS
Cyber defense solutions adapted for EMS/DMS systems utilize a powerful computing platform and capable of performing threat detection based on available data. Upon requirement to upgrade the defense and detection capabilities, additional computer-power shall be added thus enabling the IIDS operation in new conditions.

Summary
Process behavior analysis is dealing with a range of threats and malfunctions caused by computer hardware failure, damaged sensors, software flaws and communication problems, and cyber attacks. This technology is considered as a suitable solution for defending critical infrastructure. IIDS systems used by EMS/DMS shall combine anomaly behavior analysis deployed for cyber defense, and shall utilize patented algorithms providing cutting edge performance. For information on ICS^2 technology based IIDS, please refer to www.ICS2.com or contact us on info@ics2.com



Upcoming Conferences and Exhibitions

by Chuck Newton

The 2016 DISTRIBTECH Conference kicks off a big year for conferences both in North America and internationally. Over my career in energy-related research, I have been privileged to attend and speak at many conferences around the world. This year being an even-numbered year, mean that three bi-annual world-class conferences will be held. These include the spring IEEE T&D Conference in Dallas, the summer CIGRE Conference in Paris and the autumn CEPSI conference being held in Bangkok. Another important Asian conference on Electric Power Distribution Networks is CICED, planned for Xi'An, China in August. Newton-Evans is hopeful of being represented at each of these, as well as at the UTC conference, CIGRE and various IEEE sessions.

www.newton-evans.com maintains one of the more extensive calendars of energy-related events of major interest. The 2016 listing of events on our website includes more than 50 domestic and international conferences of note, many sponsored by technical associations and a few by universities or private event organizations. Each day, visitors from around the world visit our Events page to learn about upcoming conferences. Events marked with * indicate that Newton-Evans staff will possibly be in attendance.

Distributech Conference and Exhibition 2016
February 9-11, 2016
Orange County Convention Center
Orlando, Florida USA
www.distributech.com

National Hydropower Conference
April 25-27 2015
Washington, D.C.
www.nationalhydroconference.com

2016 IEEE PES Transmission & Distribution Conference & Exposition
May 3-5, 2016
Dallas, Texas
www.ieeet-d.org

UTC Telecom and Technology Conference and Expo
May 3-6, 2016
Denver, Colorado USA
http://utctelecom.org

2016 EIA Energy Conference
July 11-12, 2016
Washington, D.C.
www.eia.gov/conference

2016 IEEE PES General Meeting
July 18-21 2016
Boston, Massachusetts USA
www.ieee-pes.org

CICED 2016 – China International Conference on Electricity Distribution
10-13 August 2016
Xi'An, CHINA
www.ciced2016.org.cn

CIGRE Session 2016
21-26 August 2016
Palais des Congres
Paris, FRANCE
www.cigre.org/Events/Session/Session-2016

EMMOS 2016
Energy Management and Market Operations Systems Users Conference
September 11-14, 2016
Phoenix, Arizona USA
www.emmos.org

CEPSI 2016 Conference and Exposition
23-27 October 2016
Bangkok, THAILAND
www.cepsi2016bangkok.org

Power-Gen International Conference and Exhibition 2016
December 13-15, 2016
Orlando, Florida USA
www.power-gen.com