http://www.cigre.org

2012 Paris Session

Study Committee B5: Protection and Automation
Preferential subject PS2: Utilization and Application of Remote Access for Protection and Automation Systems

Automated Data Retrieval, Analysis and Operational Response Using Substation Intelligent Electronic Devices

M. KEZUNOVIC[1], M. DATTA-BARUA[2], D.R. SEVCIK[2], B. FARDANESH[3], J. WALIGORSKI[4], T. POPOVIC[5]
Texas A&M University[1], CenterPoint Energy[2], New York Power Authority[3], First Energy[4], TLI, Inc.[5]
USA
kezunov@ece.tamu.edu

SUMMARY

Availability of a multitude of substation Intelligent Electronic Devices (IEDs) has created a challenge in utilities of how to manage the abundance of data recorded by such devices during various types of events. The paper explores the goals, objectives and deployment aspects of field solutions that are aimed at data retrieval, analysis and decision support for operators.

The goals of utilizing IED data are in general driven by the cost benefit in utilizing more data and better information to improve reliability, quality of service, personnel productivity, regulatory compliance, and utilization of assets. The objectives are to develop such solutions through seamless integration with legacy solutions hence assuring continuity of existing and introduction of new practices. Hence the deployment approaches have to be based on interoperability and open platform solutions that assure upgradability, testability and amenability to global standard adoption while meeting the cybersecurity requirements.

To illustrate different requirements for data retrieval and analysis, as well as different aspect of the operational uses, several applications are explored: cause-effect analysis of protective relay operation, optimization of fault location calculation, intelligent alarm processing , and utilization of the field data for troubleshooting tests. For each application an example of how the data processing may be implemented is given and improvements criteria are established.

To illustrate the best practices this paper starts with discussion of new requirements for such solutions. In all instances the end users have to be identified and their needs have to be clearly articulated through development of well-structured use case scenarios. After the approaches to the deployment specification are discussed, the paper illustrates various implementations undertaken by several utilities. For each case the applications of interest are outlined, specific deployment scenarios are explained, and expected benefits are summarized. Last but not least, interoperability concept based on the Grid Wise Architecture Council's stack [1], an interoperability context-setting framework, is mentioned as it applies to the types of applications discussed in this paper.

KEYWORDS

Disturbance analysis, automated retrieval, protection, maintenance, fault location

GOALS AND OBJECTIVES

To emphasize different aspect of the value proposition for such solutions, the associated goals and objectives are classified in the following categories: reliability, productivity, capital investment, regulatory compliance and standardization. For each of the categories, further details explaining the expectations that need to be met to get full value of the proposed solutions are illustrated in Table 1.

Table 1: Goals and Objectives

Goals	***Objectives***
Reliability	• Reliability of assets is improved based on condition-based data • Resilience to random events is enhanced through better analysis • Reliability of operating decisions is made with reduced risk • Robustness of system wiring and data is checked using redundancy
Productivity	• Data integration is automated • Data analysis is facilitated • Data viewing is made more comprehensive • Data archiving is made more efficient • Event reporting is made more timely
Capital Investment Utilization	• While obtaining new data requires new investments, existing data can be widely shared providing additional benefit with minimal cost • Substation data analysis software is not as costly to install as hardware, hence value added features are coming at less cost • Hardware may get stranded due to inability to produce useful data while the software is transferable over the platforms
Regulatory Compliance	• NERC non-compliance fines may be avoided • FERC recommendations for improved reliability can be achieved • PUC criteria for the benefits to the customers are met • Reliability coordinators can have timely reports on main events • Large customers get a way to track and prove their compliance

NEW IMPLEMENTATION REQUIREMENTS

Interoperability. The most relevant aspect of interoperability requirements, as defined by the Smart Grid Interoperability Panel's Architecture Committee reference model, and Test and Certification Committee conformance and interoperability testing requirements, are critical to the system solutions being easily upgradable in the future as the systems grows [2] . Finally, the impact of North American Reliability Corporation's Critical Infrastructure Protection (CIP) standards and Protective Relaying and Control (PRC) requirements needs also to be carefully taken into account as such documents get updated [3,4].

The interoperability is defined as "the capability of two or more network, systems, devices, applications, or components to exchange information between them and to use the information so exchanged." [5]. Informational interoperability covers the data content, semantics and format. The Grid Wise Architecture Council (GWAC) proposed framework [1] organizes concepts and terminology to identify interoperability issues. The framework recognizes that interoperability is only achieved when agreement is reached across many design layers of concern. These layers cover the details from the technology involved to link

systems together, to the understanding of the information being exchanged. When substation data collection, integration, management, analysis and visualization are considered, the proposed interoperability layers need to be well understood and defined.

Standards. The syntax layer for data from substation IEDs is well covered by the existing standards such as COMTRADE [6,7] or COMFEDE [8], but the semantics layer is not uniquely defined yet. Two competing standards in this area are IEC 61850 and 61970 [8,9], which both have their own way of defining semantics for substation data. Recent NIST efforts through the Smart Grid Interoperability Panel (SGIP) are addressing the issue of harmonizing the two standards and getting one solution for the semantic descriptions needed for substation data handling. In the meantime, the solutions that are being developed for automated analysis of substation data will have to adopt either IEC 61850 Substation Control Language (SCL) semantics [9] or the IEC 61850 Common Information Model (CIM) semantics [10]. Further details of such issues may be found on SGIP TWIKI website, which contains detailed reports from the working groups dealing with such issues [2]. The proper understanding and use of available standards is critical when implementing end-to-end solutions that will enable expansions and continuous growth. The standards should be considered frequently and evaluated continuously so that the proper application of standards is possible and timely.

Semantic Data Integration. Once data sources for a substation event are identified and communication infrastructure is established comes the challenge of substation data integration across different enterprise domains as shown in Fig. 1. The integration of data from different sources (IEDs) includes file format conversion, handling of IED configuration settings, and data warehouse arrangement. The section discusses the need for proper use of standards and recommendations, which in turn results in re-usability of integrated data. In spite of the fact that there are standards (IEEE and IEC) for substation event data representation, most of the installed IEDs are configured to keep the data in proprietary, vendor specifics formats.

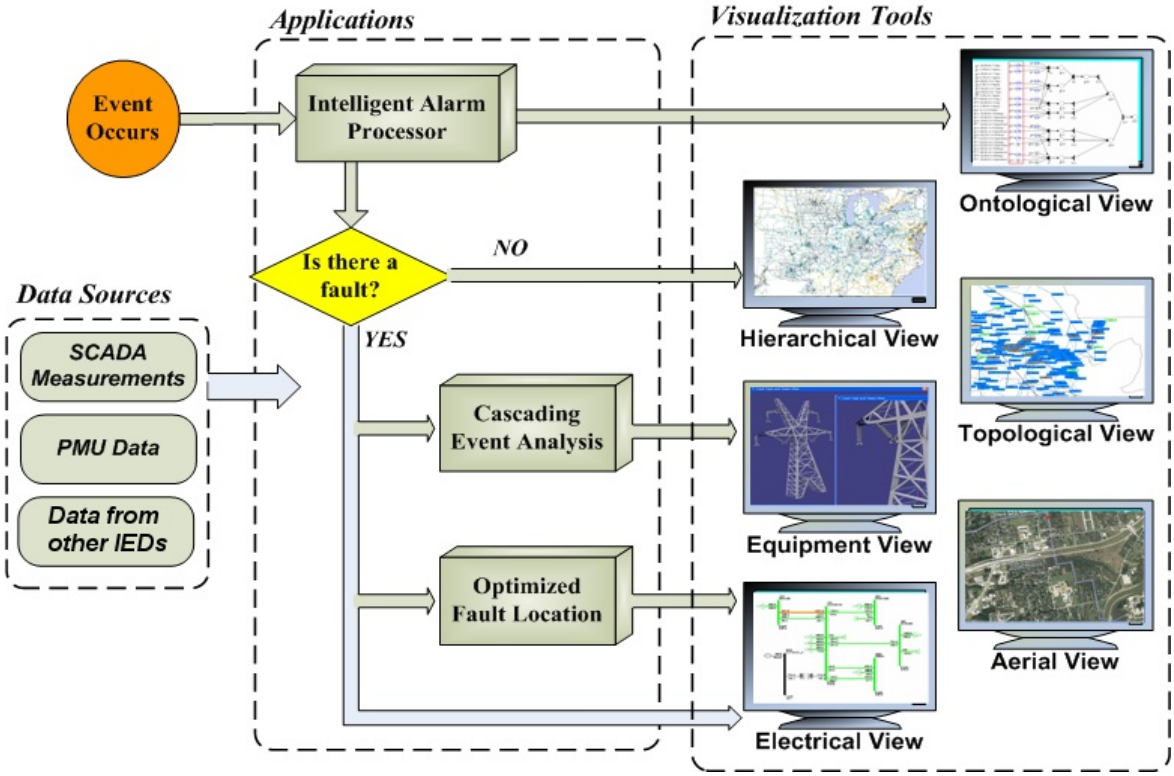

Figure 1. Data integration framework

One of the first steps is to identify IEDs and their configurations, as well as to identify capabilities of vendor support software with respect to data retrieval and conversion to COMTRADE. Where possible, it is recommended to configure IED hardware and software to utilize non-proprietary and standard file formats [6]-[10]. Where that is not possible, it is important to verify which format is supported and configured and to keep track of possible changes so that an automated conversion with third-party tools can be enabled. The latest development in applicable standards includes COMFEDE, and it should definitively be considered as an option for substation event data conversion [8].
Besides the IED data, the database has to contain system configuration data, which describe: a) system components and their relationship (transmission lines, buses, circuit breakers, switches, relays, CTs, VTs, etc.); and b) IED channel assignments and mapping/calibration to specific system components (line/bus voltages, line currents, status signals). The system configuration data enables automated IED data conversion into standard formats and integration into the database thus making the data available for data analytics functions. It is important to note that semantic data integration includes data from various sources, integration of data analytics functions, configuration settings, and finally, viewing as shown in the example in Fig. 1.

Cybersecurity. Another relatively recent development that needs to be taken into account is the contribution of Cyber Security Working Group formed by the NIST Smart Grid Interoperability Panel (SGIP). There is lots of useful information provided in their Guidelines for Smart Grid Cyber Security (NIST IR 7628) document [11]. According to the document the main components of cyber security strategy are:
a) Prevention: Actions taken and measures put in place for the continous assessment and readiness of necessary actions to reduce the risk of threats and vulnerabilities, to intervene and stop an occurrence, or to mitigate effects;
b) Detection: Approaches to identify anomalous behaviors and discover intrusions, detect malicious code, and other activities or events that can disrupt electric power grid operations, as well as techniques for digital evidence gathering;
c) Response: Activities that address the short-term, direct effects of an incident, including immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes;
d) Recovery: Development, coordination, and execution of service- and site-restoration plans for affected facilities and services; reconstitution of Smart Grid operations and services through individual, private-sector, nongovernmental, and public-sector actions.

Open source. In addition to and relevant to both interoperability and standardization should come exploration and utilization of open source solutions and philosophy [12]. In the industry we witnessed way to many closed solutions that failed due to lack of motivation and funds needed to implement and maintain closed solutions. There are several platforms, development tools, as well as engineering tools that are now available as open source. These tools have several benefits such as freedom to use, explore, customize, and share with others. There are several benefits inherited from the nature of open source and our requirements for interoperability. Also, the industry could greatly benefit from adopting the open source philosophy, where the developed solutions could be used, explored, improved, and shared by the industry.

SELECTED APPLICATIONS

Cause-effect analysis of protective relay operation. Fig. 1 shows a data processing block needed to answer the question "Is there a fault". This may be accomplished through automated analysis of data from digital protective relays (DPRs) or digital fault recorders (DFRs). The best example for how data parsing and information extraction may be done is illustrated though automated processing of DPR data (Fig. 2). A DPR can provide several event file formats and it is important to properly select a format option and configure the file format conversion. Most new DPRs offer data in raw or filtered form. In addition, there are usually options to save event data in high or low sample rate as well as to make a choice between a proprietary and a non-proprietary file format. For the data integration intended for further automated analysis it is a good choice to keep raw records with highest possible sampling rate and make those records available for later reuse.

Assuming that downloaded DPR files reside on a network shared folder, which is a typical outcome of DPR data communication and download solution, one can anticipate two possible approaches to automated processing and analysis: a) one that only includes file format conversion and parsing of relay reports to extract fault information of interest (for example, fault type and location); and b) another one that in addition performs calculations and analysis in the same fashion as it is done for digital fault recorder (DFR) files. The later provides for more redundancy in the information obtained from DPRs, but requires additional handling of configuration data.

Typical design of modern digital protective relays is based on a concept of functional elements. The elements handle inputs, outputs, protection, control, and pilot schemes. The statuses and timing of each element are recorded in various reports and such relay files define external and internal operational behavior of relays. File formats and names of relay files and reports can vary from vendor to vendor. In general, each digital protective relay generates the following files: event/fault reports, oscillography file, and setting file.

Event/fault report files contain information on fault type, fault location, phasor values of voltages and currents in pre- and fault-periods as calculated by the relay. These files also contain log of logical element status changes with time stamps and in chronological order so both the external operation and internal states can be observed. Oscillography file contains samples of both analog values (three-phase voltage and current signals) and digital status data corresponding to the relay elements. The oscillography file is in its nature similar to recordings obtained using DFRs, only in this case just the signals related to the protected circuit are being monitored.

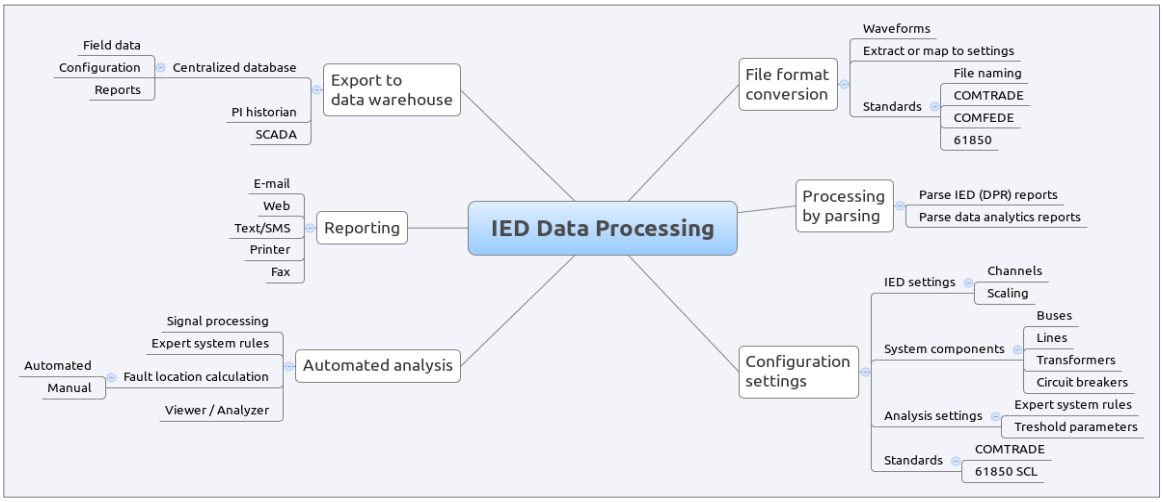

Figure 2. An example of IED data processing

Detection and classification of cascading events. This application is depicted in Fig. 3. As it may be observed, the application is implemented at two locations: system monitoring and control at the energy management system (EMS) level and local monitoring and control at the substation level. The EMS level application monitors system conditions and determines possible vulnerable elements in the system and then arms the local function to determine whether a cascade involving vulnerable elements has been detected and classified. Once a cascade is detected and classified, the system-level control is executed to mitigate the cascade [13]. The importance of this application is the fact that local application uses extensive synchronized sampling data collected by DPRs or DFRs. The algorithm that uses such data calculates very accurately fault location, and if the algorithm does not find one after the line has opened, it informs the system level function that such line is available for being restored since it was not tripped for the reason of having a fault. The algorithms to determine this are rather involved and require use of multiple techniques [14].

Optimization of fault location calculation.
This application is selected to illustrate how data from substation IEDs such as DFRs, DPRs or phasor measurement units (PMUs) may be automatically integrated with data from remote terminal units (RTUs) of supervisory control and data acquisition (SCADA) system to obtain better result for fault location than what is possible through manual data manipulation means.
As described in Fig. 4, field measurements are processed to extract phasors, and then a short circuit program is executed by moving fault location in the program and comparing the simulated phasor values from the short circuit program to the measured phasor values obtained from field devices. An optimization algorithm is developed to find the optimal match, which then points to the fault location used in the short circuit program as being the actual one. In order to make sure the short circuit program model is tuned to the prevailing system conditions at the time of the fault, the load flow results obtained by the program are compared to the corresponding SCADA measurements for the topology confirmed through the topology processor. The automation of such an application has been proven feasible and results obtained through this method are much better and faster than what is possible through manual means [15].

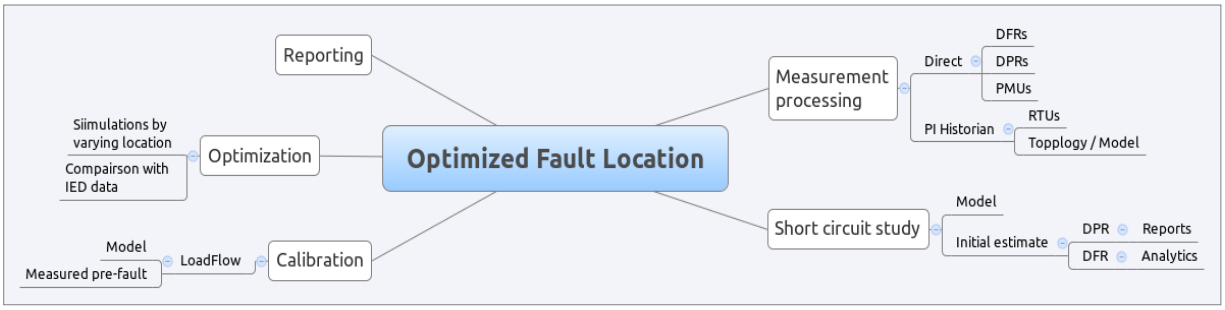

Figure 4. Optimization of fault location calculation

Intelligent Alarm Processing. This application, illustrated in Fig. 5, is developed as an improvement to the traditional Alarm Processor by providing two important enhancements: additional data from substation IEDs other than RTUs, and additional processing capability based on fuzzy reasoning Petri nets (FRPN) [16]. The new data is combined with data from SCADA to improve the modeling capabilities of the cause-effect analysis. Such improved model is represented using Petri nets, and the reasoning is based on fuzzy variables associated with the measurements coming from the combined data base of RTU and IED data. The benefits of this approach are multiple with the most important one being the ability to differentiate multiple alarms caused by a simple event hence dramatically improving alarm

filtering during complex network disturbances where hundreds of alarms may be occurring while only a few actual power systems events may be unfolding.

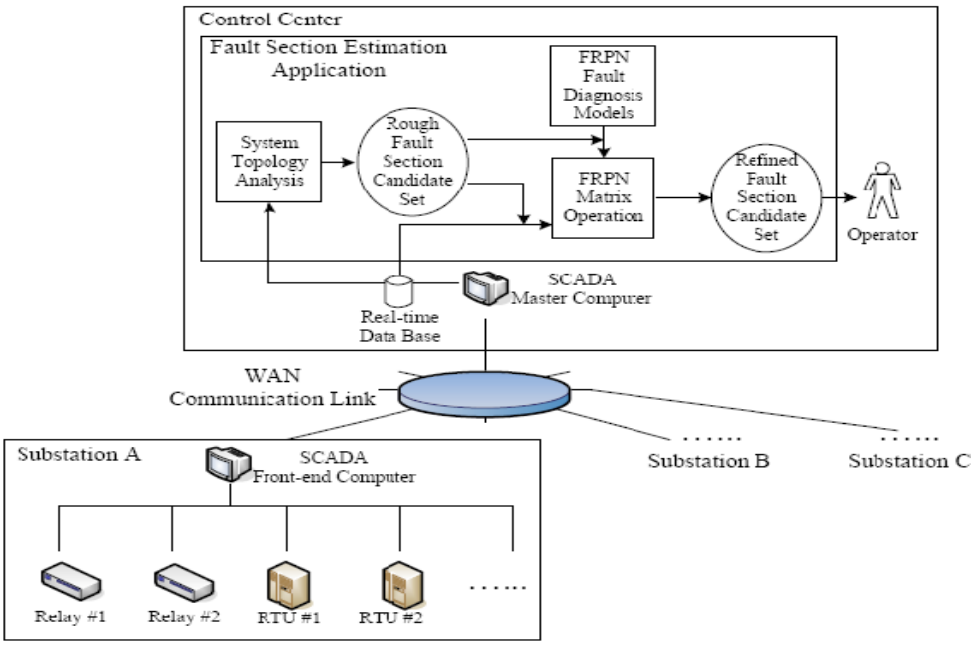

Figure 5. Intelligent Alarm Processing

Utilization of the field data for troubleshooting tests. Automated data collection and data analytics of the field-recorded waveforms is essential for expediting the troubleshooting of protective relay operations. Automated retrieval, processing, and analytics are important for quick identification and classification of the recorded waveforms. Fault playback is important for repeating the problem in the lab and sometimes in the field conditions. The playback methodology utilizes digital simulators or tests sets with fault waveform replay capability. The equipment under test is exposed to conditions with the intention to repeat and "catch" undesired operations so that those can be understood and fixed. Field-recorded data and analytics output can be essential for calibrating and tuning the system model used in simulation.

Combining the automated data retrieval, analytics, and testing methodologies can dramatically expedite process of selecting the field-recorded data that can be used for fault playback or calibration of the system models. This approach allows for quick assessment and evaluation of the protection equipment, which helps further tuning of the settings. All the data together with the analytics reports are available in a centralized database.

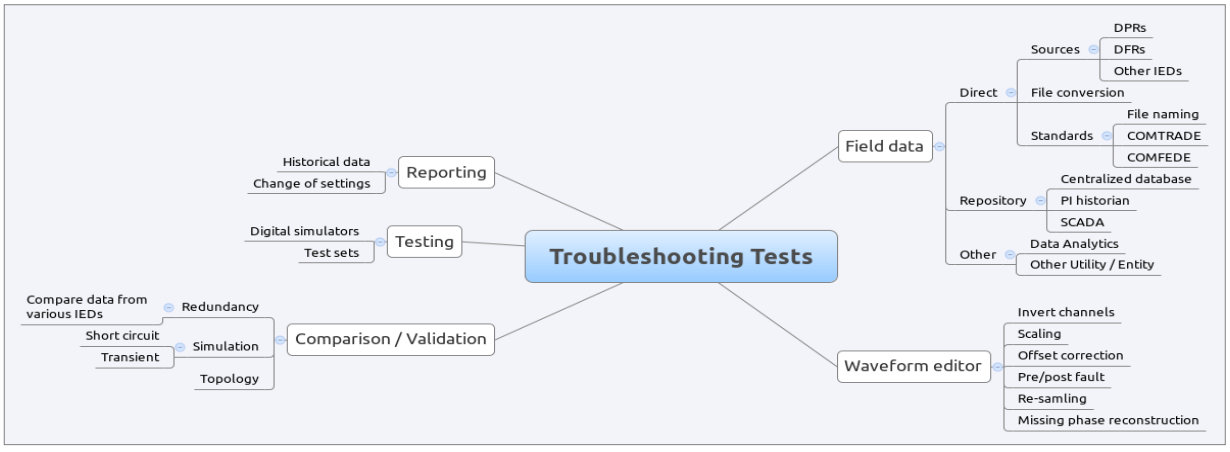

Figure 6. Utilization of the filed data for troubleshooting tests

CONCLUSIONS

This paper illustrates a few important issues related to automated data retrieval, analysis and decision support for operators:

- The goals and objective of automating the data analysis process have to be related to improvements in reliability, savings in personnel time, better utilization of capital investment in the data acquisition and processing equipment, and ability to respond to regulatory requirements for accurately reporting system disturbances and the causes
- To make such system solution to be cost effective and last for an extended period of time, special attention has to be given to the new implementation requirements such as interoperability, standards, semantic data integration and cybersecurity, none of which were widely observed in the past practice and emerged relatively recently
- The use of automation and availability of new data gives tangible benefits in determining occurrence of disturbances, effectively detecting, classifying and mitigating cascades, accurately calculating fault location, and timely processing alarms, as well as in selecting best waveform replay cases for the purpose of testing

BIBLIOGRAPHY

[1] GWAC, Interoperability Path Forward Whitepaper, Oct 05. [Online] Available: http://www.gridwiseac.org

[2] SGIP TWIKI, [Online] Available: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome

[3] NERC Standard, Cyber Security, CIP-002 through CIP-009, North American Electric Reliability Corp., [Online]Available: http://www.nerc.com

[4] NERC Standard, Protection and Control,PRC-002-1 and PRC-018-1, North American Electric Reliability Corp., 2006-2007“

[5] EICTA Interoperability white paper” European Industry Association, Information Systems Communication Technologies Consumer Electronics, 21 June 2004.

[6] IEEE Std C37.111 “Common Format for Transient Data Exchange”, , 1999.

[7] IEC Std. 60255-24, “Common Format for Transient Data Exchange (COMTRADE) for power systems”, First Edition 2001-05, International Electrotechnical Commission, 2001.

[8] IEEE Std. C37.239 “Common Format for Event Data Exchange (COMFEDE) for Power Systems,” , 2010

[9] IEC Std. 61850, “Communication Networks and Systems in Substations”, work in progress, International Electrotechnical Commission, [Online]. Available: http://www.iec.ch

[10] IEC Std. 61970, “Energy management system application program interface (EMS-API) - Part 301: Common Information Model (CIM) Base”, IEC, Edition 1.0,2003-11.

[11] NIST IR 7628, “Guidelines for Smart Grid Cyber Security”, NIST Computer Security Division – Computer Security Resource Center, [Online]. Available: http://csrc.nist.gov

[12] Open source on Wikipedia, [Online]. Available: http://en.wikipedia.org/wiki/Open_source

[13] H. Song, M. Kezunovic, “A New Analysis Method for Early Detection and Prevention of Cascading Events,” Electric Power Systems Research, Vol. 77, Issue 8, Pages 1132-1142, June 2007.

[14] M. Kezunovic, “Smart Fault Location for Smart Grids,” IEEE Transactions on Smart Grid, Vol 2., No. 1, pp 61-69, March, 2011

[15] M. Kezunovic, “Translational Knowledge: From Collecting Data to Making Decisions in a Smart Grid,” IEEE Proceedings, 2011, Vol. 99., No.6, pp 977-997, June 2011.

[16] Y. Guan and M. Kezunovic, “Grid Monitoring and Market Risk Management using Intelligent Economic Alarm Processor,” IEEE Intelligent Systems,vol.26, no.2, pp.18-21, March-April 2011.