Intelligent Monitoring of the Health and Performance of Distribution Automation

S. E. Rudd*, J. D. Kirkwood†, E. M. Davidson*, S. M. Strachan*, V. M. Catterson* and S. D. J. McArthur*
*Institute for Energy and Environment, University of Strathclyde, Glasgow, United Kingdom
Email: srudd@eee.strath.ac.uk
†Scottish Power Energy Networks, United Kingdom

***Abstract*—With a move to 'smarter' distribution networks through an increase in distribution automation and active network management, the volume of monitoring data available to engineers also increases. It can be onerous to interpret such data to produce meaningful information about the health and performance of automation and control equipment. Moreover, indicators of incipient failure may have to be tracked over several hours or days.**

This paper discusses some of the data analysis challenges inherent in assessing the health and performance of distribution automation based on available monitoring data. A rule-based expert system approach is proposed to provide decision support for engineers regarding the condition of these components. Implementation of such a system using a complex event processing system shell, to remove the manual task of tracking alarms over a number of days, is discussed.

I. Introduction

WHILST the scope of definition for the 'smart grid' is wide and differs across territories, certain visions of how our energy infrastructure is predicted to evolve during the coming decades are shared. It is envisaged in [1] and [2] that information and communications technologies will play a key role in the delivery of future networks.

For the operation of future distribution networks, these visions translate into a number of changes from common practice:

- An increasingly observable network—the proliferation of communications and monitoring equipment on distribution networks will result in greater observability at lower voltage levels.
- Bi-directional power flows, introduced through the connection of distributed energy resources—for networks originally designed for uni-directional power flows, this can lead to congestion and problems regulating voltage.
- Increased use or even reliance on distribution automation and active network management, as a means of providing reliable and cost effective supply of electricity.
- Controllable load through various demand-side management measures.

However, these changes to current practice are likely to result in a number of challenges for the utility personnel tasked with operating distribution networks. One such challenge is the increased volumes of data that such a highly monitored, active distribution system, with widespread use of automation, is likely to produce.

Intelligent systems researchers within the power systems community have long understood the problems associated with deriving meaningful information from power systems data, especially under extreme conditions, such as during storms or other network events. Over two decades of research have produced numerous expert systems [3], [4], [5], [6], [7], and model-based reasoning systems [8], [9], [10], for alarm processing for both transmission and distribution systems. However, the move to more observable distribution networks, which are active rather than passive, leads to a new set of challenges in understanding system behavior, health and performance of distribution automation and active network management schemes on a day-to-day basis.

Arguably, active network management is still in its infancy. Only a handful of schemes have seen deployment around the world [11], and utilities are still learning what the impact on the routine operation of the networks will be and what, from an operational perspective, the widespread roll-out of such schemes is likely to entail.

On the other hand, one area where much more experience has been gained is that of distribution automation. Regulatory pressure in the form of incentives relating to reliability of supply, e.g. customer minutes lost (CML) and customer interruption (CI) in the UK; and the customer average interruption duration index (CAIDI) in the USA, have resulted in utilities investing in distribution automation in a bid to increase their revenue.

Distribution automation to improve customer service, and in doing so meet or exceed regulatory targets, can take various forms: remote terminal unit (RTU) based schemes [12]; automatic teleswitching schemes [12]; and novel peer-to-peer communicating schemes, such as S&C Electric's IntelliTeam2 [13]. However, regardless of the type of distribution automation used, understanding both the performance and health of such schemes is an operational requirement. In order to make a positive impact (and not a negative impact) on reliability of supply, distribution automation schemes must operate when needed. Identifying incipient failures, scheme performance issues or problems with equipment health before they result in failure of the scheme to operate when needed, is an important task: it ensures that schemes perform in such a way that justifies the investment in the first place. This includes the health and performance of the communication systems on which they may rely. Often, such information is

implicit in the power systems data that engineers use to make such assessments. Moreover, the volumes of data produced by a large number of schemes can make manual analysis of the data impractical. Symptoms of incipient failure may be seen over several hours, days or even weeks. Tracking such symptoms can be problematic.

This paper discusses distribution automation in general and the requirement for automatic analysis of data relating to the health and performance of distribution automation schemes. A case study is included, which considers some of the data analysis problems seen by a UK utility after the widespread roll-out of a particular type of distribution automation scheme. This paper outlines some of the decision support requirements from the perspective of the engineers tasked with maintaining and managing such schemes.

In terms of decision support technologies, the paper examines the use of complex event processing and rule-based expert systems as a means of dealing with that data. Example rules for identifying a number of scheme health and performance issues, derived through knowledge elicitation, are presented. How these rules are used within a prototype alarm processing system, currently under development, is described. Future extensions to that prototype are also discussed.

II. Distribution Automation and Smart Grid

The term 'distribution automation' connotes a wide set of technologies and approaches to the remote operation of distribution networks. Distribution automation can be thought of as "a set of technologies that enable an electric utility to remotely monitor, coordinate and operate distribution components in real-time mode from remote locations" [12].

Northcote-Green and Wilson identify three classes of distribution automation [12]:

1) Local Automation—switch operation performed by protection or local logic-based decision-making operation;
2) SCADA (telecontrol)—manually initiated switch operation by remote control with remote monitoring of status, indications, alarms and measurements; and
3) Centralized Automation—automatic switch operation by remote control from central decision-making for fault isolation, network reconfiguration and service restoration.

Examples of all three can be found in the operation of distribution networks in the UK. A fairly high level of telecontrol is commonplace with certain companies, who have made investments in telecontrol due to the CML savings they can achieve on particular classes of circuit.

Restoration via telecontrol can be problematic. Depending on prevailing network conditions, control engineers may not be able to respond and restore customers within three minutes, after which CML start to accrue. During storm conditions or busy periods, it may not be possible for the control engineer to manage large numbers of restorations within that timescale. Human factors aside, restoration via telecontrol is beholden to the availability and performance of communications and telecontrol equipment.

Several utilities in the UK have experience with a centralized approach to automatic restoration. Automation scripts run in the distribution network management system environment, e.g. Korn shell scripts run within GE's ENMAC, can be used to automatically execute a sequence of control actions for restoring customer supply after a fault. For example, a very simple script may do the following after being triggered by the operation of a breaker:

1) check that automation is enabled on a given feeder;
2) check the status of a remotely controllable sectionalizer and normally open point;
3) open the sectionalizer and check for successful operation;
4) close the a normally open point and check for successful operation.

Scripting in the Distribution Management System (DMS) is not without its foibles. Scripts may not cover all possible operating states and thus exit early when experiencing unusual conditions. Time-outs due to communications delays can also cause scripts to terminate before restoration is complete. For example, a script may wait 20 seconds for confirmation of the status change of a switch. Communications delays may cause that confirmation to take over 20 seconds to arrive at the control room; however, by then the script will have terminated early. So, like restoration via telecontrol, centralized automation is also beholden to the availability and performance of communications and telecontrol equipment.

Other utilities also use local automation schemes, sometimes in addition to the centralized approach. These can range from non-communicating automation schemes, such as the use of automatic sectionlizing links including 'smart fuses' and autoreclosers [12], to a communicating RTU-based automation scheme such as that described in section III. Recent years have also seen the first trials of peer-to-peer network restoration schemes, such as trials of S&C Electric's IntelliTeam2 on the Isle of Wight [13], although IntelliTeam2 has seen a large number of other deployments around the world.

In relation to the 'smart grid', distribution automation can play a role in achieving the oft-mooted 'self-healing' functionality. Financial incentives to improve reliability of supply can drive distribution network operators to invest in distribution automation to that end.

However, increasing levels of distribution automation lead to a requirement for ways of analyzing the data related to scheme health and performance. In this paper, an industrial case study is presented from a utility in the UK which currently employs all three types of automation discussed above.

III. An Industrial Case Study

A key building block in the utility's distribution automation infrastructure is what is termed a Network Controllable Point (NCP). An NCP is an item of 11kV secondary equipment that can be controlled remotely, such as a remote terminal unit (RTU) controlling a circuit breaker. Figure 1 illustrates a typical underground urban network, showing the installment of RTUs, which provide the interface that controls the switchgear.

Modern equipment can also be accessed directly with an intelligent electronic device (IED). The utility have over 2800 NCPs installed on the network, with plans to increase to a number approaching 5300.

NCPs have a dual purpose. One is to enable remote control of the distribution components by the engineer manually initiating a command in the control room via the distribution management system (DMS). Alternatively, some NCPs form part of the 235 automatic restoration schemes that the utility has installed on the network. It is therefore necessary that NCPs are in a healthy condition and ready to contribute to both automated and remote control of switchgear.

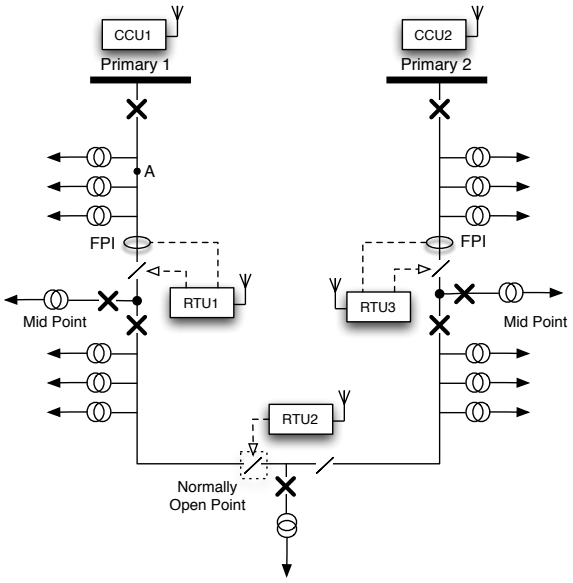

Fig. 1. Network diagram highlighting the placement of Fault Passage Indicators, Central Control Units and RTUs for automatic restoration schemes

Automatic restoration can be achieved by placing fault passage indicators (FPIs), central control units (CCUs) and RTUs on the network to monitor and remotely control the actuators at switches and normally open points (NOP) (Figure 1). Each RTU uses VHF digital radio equipment to communicate with the primary CCU, which remotely controls the remote equipment attached to that primary. When a fault occurs in a section of the network, a circuit breaker will trip and isolate the fault. Decision-making logic incorporated either at the control room or the source primary can automatically restore those disrupted customers who are not permanently affected by the fault, through network reconfiguration and service restoration.

For example, if a fault were to occur at point A in Figure 1, the circuit breaker at primary 1 trips, taking all customers from primary 1 to the NOP off supply. Communication occurs between CCU1, RTU1 and RTU2 to identify the passage of fault current and voltage changes at these points. Since no fault current would have been seen at RTU1, it opens the sectionalizer. RTU2 will then close the NOP, restoring supply to the customers between the mid point and NOP.

The DMS, along with the SCADA system's communication infrastructure and controllable protection equipment, forms the architecture required to perform distribution automation (Figure 2). The PS Alerts database stores NCP SCADA alarms in real time that can indicate potential issues associated with NCP equipment health.

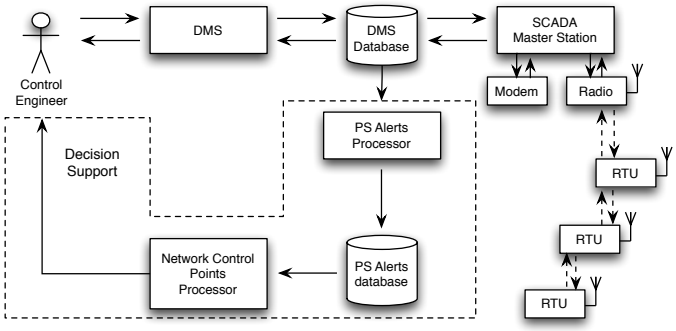

Fig. 2. Distribution automation with respect to the SCADA system.

The SCADA and communication infrastructure shown in Figure 2 allows the status updates and alarms associated with each NCP to be sent back to the control room. It is then the task of the control engineer to examine a series of alarms to identify any important information. Monitoring the alarms of each NCP manually has the following disadvantages:

- An onerous amount of data is presented to the operator from all the protection devices, as well as the RTUs.
- Moving to a smarter grid will increase the amount of monitoring data further, with alarms being generating from equipment that was previously unmonitored.
- Shift changes of the operators, as well as alarms spanning a number of days, can lead to operators missing previous alarms, which might have given an insight into the NCP equipment's present condition.

During knowledge elicitation with experts, five scenarios were highlighted as problems with the NCP's health, which could affect its performance:

1) Every six hours, the CCU polls the RTUs to check if they are still online. An alarm will be generated by SCADA if the condition of that RTU changes state ("comms fail ON" or "comms fail OFF"). There are two general situations that engineers look for. The first is an intermittent problem with communications, indicated by a sequence of alarms such as comms ON, comms OFF, comms ON, comms OFF within a 24 hour period. The second is the more serious case of a comms ON alarm that stays on permanently for 48 hours. Due to a significant number of alarms being presented to the control engineer over a number of days, it can be difficult to keep track of the status of each RTU, and the single alarm that corresponds to a permanent communications failure could easily be missed.
2) A common problem associated with RTU operation is a loss of power supply. A ground mounted RTU has an associated power supply unit (PSU), which derives its

auxiliary power supply from the LV network. Within the PSU there is a battery backed power supply designed to last at least 24 hours. A loss of LV supply to the RTU sets off a chain of events:

- First, if the LV supply is lost, through human intervention or other errors, then a "loss of volts" alarm is generated by SCADA.
- If the LV supply is not restored within 1–3 days, then the battery will have discharged to the point that it will generate a "battery alarm" by SCADA. This is because if the sealed lead acid battery is allowed to go below a nominal voltage it reverses cell polarity and is damaged.
- Finally, if LV supply is still not restored, the battery goes into deep discharge protection and shuts itself off. This means that during the six hour health check between CCU and RTU, the RTU will not reply and a "comms fail ON" will be generated by SCADA.

3) When a control engineer tries to control an object a 20 second timer is started. If this time is exceeded and the object has not changed state then a "scan task timeout" is generated by SCADA indicating that the object has not opened/closed within the allotted time. However, due to different ways in which the signal may propagate through the network, the confirmation of successful operation may feasibly take longer than 20 seconds. It is therefore necessary to identify if objects did in fact operate after they were commanded to do so, and calculate how much longer than the 20 seconds they took. This would allow the object's timer to be set with respect to how the comms system actually behaves, and reduce the number of unnecessary alarms presented to the control engineer.
4) If the state of an actuator is unknown then a "DBI (double bit indication) alarm" is generated by SCADA. The positional indication of remote plant is derived from a double bit I/0 state. If this state is illegal or transitional i.e. DBI 00 or DBI 11, then it cannot be remotely controlled because it is unknown whether it is in an open or closed position. This condition may have been caused by third party intervention on site and requires further investigation.
5) Once an automation scheme has successfully operated, it goes into an "auto off and complete" or an "auto off" state. Although automation has restored supply to customers on part of the network that is unaffected by the initial fault, the network remains in an abnormal condition until it is repaired. Only once this has happened can the automation scheme be manually re-enabled. As the "auto off" alarms reside as historical events there is no immediate reminder to reset the automation, therefore, if not reactivated, the distribution automation scheme cannot respond to any subsequent fault events that may occur.

Although these five scenarios represent some of the expert's knowledge regarding the health and performance of NCPs, it should be noted that further issues may arise over time, which the NCP experts are presently unaware of or have not been discussed above. The authors are developing an extensible and flexible system to automate the interpretation of SCADA alarms, shown in the dashed section in Figure 2. This system is intended to provide decision support to the control engineer regarding NCP performance and health, and aims to minimise unnecessary loss of supply, as well as reduce CIs and CMLs attributed to faulty NCP equipment.

IV. Intelligent Monitoring

Within the power industry, there has been a wealth of research into the use of intelligent system techniques for alarm processing. Since each utility has different needs and requirements based on their infrastructure for network monitoring, over the years a variety of approaches have been investigated [3], [4], [5], [6], [7], [14], [8], [9], [10].

This history of research means that the strengths and weaknesses of each technique are well-understood. For example, the "knowledge bottleneck", or intensity of time and effort required for knowledge-capture or building of models means that rule-based and model-based systems have limited penetration in the control room beyond some key installations. On the other hand, data-driven techniques such as neural networks require re-training whenever the network topology changes, and cannot present engineers with an explanation of their results, meaning that engineers are wary of the solutions they offer.

While networks remain largely passive and centrally-managed, alarm processing can be managed by engineers supported by expert systems. However, with the move towards smarter grids, with associated increases in monitoring data and the need for systems which are more self-healing and self-diagnosing, the case for automated alarm processing becomes more pressing. The broader application is not new, but there are new drivers creating a requirement for a distribution automation alarm processor.

Model-based alarm processing is possible in situations where a first principles understanding exists of the relationship between function and structure of components of the system to be diagnosed and the SCADA data, and that knowledge can be easily be encoded as a model.

When knowledge is associational, like in the 5 cases shown above, production rules or causal models can be an appropriate form of knowledge representation. The up-front effort required for knowledge elicitation is more than compensated for by the information such a technique can provide, and production rules map well to the way the engineer considers the problem.

A related technique is Complex Event Processing (CEP) [15], which has been deployed successfully in industries such as banking and finance. Microsoft see clear parallels between these applications and those faced by the smart grid, publishing a smart grid reference architecture (SERA) [16] with CEP at its core. An EU Framework 7 project is currently

investigating CEP for detecting security breaches in SCADA systems [17].

According to luckman [15], CEP consists of a mixture of techniques, some old and some new. For example, one form of CEP uses knowledge-based expert systems with a knowledge modelling formalism that explicitly groups temporal data into events. Drools Fusion is one such CEP toolkit [18], an iteration on the popular Drools Expert expert system shell. Both Drools Fusion and Expert employ the Rete engine for inference, with the main difference being that the Fusion rule language contains temporal predicates, such as 'before', 'overlaps', 'starts', and 'coincides'.

The nature of the alarm processing problem is such that temporal relationships between alarms are key for correct interpretation of the situation. The presence or absence of particular alarms in sequence is indicative of the type and location of incidents in the monitored system. This means that many rule-based expert systems developed to address alarm processing include some method of temporal reasoning. For example, one post-fault analysis system [7] has explicit concepts for events and incidents: SCADA alarms are first grouped into events, then related events are linked to form an incident. The investigation of an incident involves analysing the sequence of events to determine whether secondary analysis of further datasets is required.

This suggests that the power systems community may have been performing CEP-style analysis all along, by using rule-based expert systems for processing of temporal alarm streams. While CEP may not represent a novel concept in the context of alarm processing, the benefit of wider deployment of CEP applications is that a set of tools and standard approaches to modeling events is now available, such as Drools Fusion.

As a result, the authors have explored the use of CEP for monitoring of the distribution automation system. The authors believe that the benefits of knowledge-based systems, including explainability and validation of the knowledge, can be coupled with the CEP approaches to modelling temporal constraints, to produce a system that meets the needs for a distribution automation monitoring system. The following section considers how this could be achieved.

V. Using CEP for Monitoring Health and Performance of Distribution Automation

In 2008, research within the authors' research group developed a prototype system using the knowledge-based expert system shell Drools to diagnose the health of NCP equipment. However, one of the main challenges for this system is in dealing with the temporal aspect of the NCP SCADA alarms, which can span days. Utilizing a knowledge-based approach to process the SCADA alarms means that such alarms are required to be held in working memory for a number of days. Additional rules were therefore required regarding the maintenance of facts in working memory; if after a predefined time certain facts were still in working memory, they were deleted reducing the memory intensity. This added to the complexity of the rule-base.

The authors have since begun exploring a CEP approach. This type of approach removes the requirement of additional timing rules by making each alarm an event and triggering response actions in real time. Drools Fusion offers a CEP framework to handle this reasoning over days/weeks, using the architecture shown in Figure 3 to process the SCADA alarms and diagnose the condition of the NCP equipment.

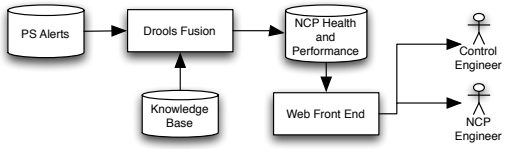

Fig. 3. Flow of CEP.

Knowledge engineering techniques are still required to construct domain knowledge rules if using CEP. The following example shows the rules to handle the alarms shown in Table I, which will be hidden in amongst tens of thousands of alarms within that time period. These alarms are associated with a loss of mains supply to the RTU, which triggers a series of events explained in section III, scenario 2.

If *Alarm Name = Loss of Volts ON*
And *Exists for > 4 hours*
And *Alarm_District_Zone != test zone*
Then *This equipment has lost its LV supply and must be visited, inform LV operational support immediately.*

Fig. 4. Rule for stage 1.

If *Alarm Name = Loss of Volts ON*
And *Alarm Name = Battery Alarm ON (for the same substation name)*
And *Alarm_District_Zone != test zone*
Then *This equipment has lost its LV supply and the battery is in discharge condition. This NCP is about to lose telecontrol and must be visited, inform LV operational support immediately.*

Fig. 5. Rule for stage 2.

If *Alarm Name = Loss of Volts ON*
And *Alarm Name = Battery Alarm ON (for the same substation name)*
And *Alarm Name = Comms Fail ON (for the same substation name)*
And *Alarm_District_Zone != test zone*
Then *This equipment has lost its LV supply, the battery has gone into deep discharge and has shutdown the NCP. Inform LV operational support and NCP team immediately.*

Fig. 6. Rule for stage 3.

Noticeable from the first rule (Figure 4), there is a waiting time of 4 hours. This allows an engineer to visit site and put the RTU back online. It is therefore necessary to handle this rule over a 4 hour period, checking if the loss of volts alarm goes OFF. If this alarm goes unnoticed and the LV supply is not restored, then 2 days later the battery alarm ON will be generated, meaning that the first alarm is required to be stored in working memory for two days, prior to the second rule (Figure 5) firing on receipt of a battery alarm ON. The

TABLE I
EXAMPLE OF ALARMS TRIGGERED FROM LOSS OF AUXILIARY SUPPLY.

STAGE	EVENT_TIME	ALARM_SUBSTATION_NAME	ALARM_CIRCUIT_NAME	ALARM_NAME	ALARM_TEXT
Stage 1	09 Dec 2010 13:17:35.360	EVERGREEN TERRACE	EVERGREEN TERRACE → YELLOW BRICK ROAD	LOSS OF VOLTS	ON
…	…	…	…	…	…
…	…	…	…	…	…
…	…	…	…	…	…
Stage 2	11 Dec 2010 15:49:39.260	EVERGREEN TERRACE		BATTERY ALARM	ON
…	…	…	…	…	…
Stage 3	11 Dec 2010 22:25:19.470	EVERGREEN TERRACE		COMMS FAIL	ON

temporal effect of this series of alarms is seen in Table I, where the time between the first two alarms is 2 days, 2 hours, 32 minutes and 4 seconds and the time between the second and third alarm is 6 hours, 35 minutes and 40 seconds. Since each later rule is dependent on the previous alarms, the alarms may be required in the working memory over a number of days.

Figure 7 shows the CEP implementation of rule 4 explicitly allowing the reasoning of the absence of events over a defined time period. In this case a waiting time of 4 hours is required to test if the "loss of volts" alarm goes OFF prior to informing the control engineer regarding the loss of LV supply. This constraint can be seen in the "when" part of the rule in Figure 7.

```
declare Alarm
    @role(event)
end

rule "Lost LV Supply"
no-loop false
        when
                $lofv : Alarm(alarmName == "loss of volts", $s:subName,
                alarmText == "ON")
                not (Alarm(this after[0s, 4h] $lofv, alarmName == "loss of volts",
                subName == $s, alarmText =="OFF"))
        then
                insert(new Event("lost LV supply, supply has not been restored after 4
                hours, engineering staff should be informed of this situation", $s));
end
```

Fig. 7. Example drools coding of rule 4.

VI. DISCUSSION AND CONCLUSIONS

Through an industrial case study, this paper has explored some of the issues surrounding the widespread roll-out of distribution automation. The experience of a distribution network operator in the UK illustrates the requirement for automatic analysis of data and the role intelligent systems could play. The five scenarios presented in this paper are only a subset of problems domain experts currently see or anticipate seeing in the future. As a result the authors are taking an incremental approach to building this intelligent monitoring functionality with the aim of extending the scope of the rule base.

The prototype system, currently being developed by the authors, demonstrates that previous research into alarm processing is valid in the context of dealing with the sort of data analysis challenges the smart grid is likely to present.

While new tools for alarm processing, such as the CEP toolkits that are both freely and commercially available, may aid in some aspects of the development of alarm processors, the fundamental challenges of knowledge capture and representation in a domain where data may be uncertain or even conflicting, still apply.

REFERENCES

[1] SmartGrids, "Vision and strategy for Europe's electricity networks of the future," Available: http://www.smartgrids.eu/.

[2] IntelliGrid, "Smart power for the 21st century," Available: http://intelligrid.epri.com/.

[3] K. Tomsovic, C.-C. Liu, P. Ackerman, and S. Pope, "An expert system as a dispatchers' aid for the isolation of line section faults," *Power Delivery, IEEE Transactions on*, vol. 2, no. 3, pp. 736 –743, Jul. 1987.

[4] T.-K. Ma, C.-C. Liu, M.-S. Tsai, R. Rogers, S. Muchlinski, and J. Dodge, "Operational experience and maintenance of online expert system for customer restoration and fault testing," *Power Systems, IEEE Transactions on*, vol. 7, no. 2, pp. 835 –842, May 1992.

[5] J. R. McDonald, G. M. Burt, and D. J. Young, "Alarm processing and fault diagnosis using knowledge-based systems for transmission and distribution network control," *IEEE Trans. Power Syst.*, vol. 7, no. 3, pp. 1292–1298, Aug. 1992.

[6] Z. A. Vale, M. F. Fernandes, C. Rosado, A. Marques, C. Ramos, and L. Faria, "Better KBS for real-time applications in power system control centers: Experience from the SPARSE project," *Computational Intelligence*, vol. 37, pp. 97–111, 1998.

[7] J. A. Hossack, G. M. Burt, J. R. McDonald, T. Cumming, and K. Stokoe, "Progressive power system data interpretation and information dissemination," in *IEEE/PES Transmission and Distribution Conference and Exposition*, Oct. 2001, pp. 907–912.

[8] M. Pfau-Wagenbauer and W. Nejdl, "Integrating model-based and heuristic features in a real-time expert system," *IEEE Expert*, vol. 8, no. 4, pp. 12 –18, Aug. 1993.

[9] A. Beschta, O. Dressler, H. Freitag, M. Montag, and P. Struss, "A model-based approach to fault localisation in power transmission networks," *Intelligent Systems Engineering*, vol. 2, no. 1, pp. 3 –14, 1993.

[10] P. Baroni, G. Lamperti, P. Pogliano, and M. Zanella, "Diagnosis of a class of distributed discrete-event systems," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 3, no. 6, pp. 731–752, Nov. 2000.

[11] R. McDonald, R. A. F. Currie, and G. W. Ault, "Active networks deployment register," Available: http://www.ensg.gov.uk/assets/anm_deploymen_register_report_-_january_2008_final.pdf, 2008.

[12] J. Northcote-Green and R. Wilson, *Control and Automation of Electrical Power Distribution Systems*. CRC Press, Taylor and Francis Group, Florida, 1997.

[13] D. Macleman, W. Bik, and A. Jones, "Evaluation of a self healing distribution automation scheme on the Isle of Wight," in *Electricity Distribution - Part 1, 2009. CIRED 2009. 20th International Conference and Exhibition on*, Jun. 2009.

[14] M. Negnevitski and V. Pavlovsky, "Neural networks approach to online identification of multiple failures of protection systems," *IEEE Trans. Power Delivery*, vol. 20, no. 2, Apr. 2005.

[15] D. C. Luckham, *The power of events: an introduction to complex event processing in distributed enterprise systems*. Addison-Wesley, 2002.

[16] Microsoft, "SERA White-paper," Available from http://download.microsoft.com/download/0/C/2/0C2F64B1-241D-4433-9665-5F802E7510D6/Microsoft2010.

[17] INSPIRE, "INcreasing Security and Protection through Infrastructure REsilience," Project home: http://www.inspire-strep.eu/, 2011.

[18] JBoss, "Drools fusion," Available from http://www.jboss.org/drools/drools-fusion.html, 2010.