A Control and Communications Architecture for a Secure and Reconfigurable Power Distribution System: An Analysis and Case Study

Anthony M. Giacomoni*, S. Massoud Amin*, and Bruce F. Wollenberg*

*Department of Electrical and Computer Engineering,
University of Minnesota, Minneapolis, MN 55455 USA
(e-mail: {giaco013, amin, wollenbe}@umn.edu)

Abstract: The transformation of the end-to-end power grid to a digitalized, intelligent, self-healing system presents many new modeling, sensing, communications, and control challenges that must be addressed before extensive deployment can begin. Increasing the security, robustness, and efficiency of electric power infrastructure requires utilizing these automation technologies in order to continually assess and optimize system performance. In this paper, an intelligent distributed secure control architecture is presented for distribution systems to provide greater adaptive protection, with the ability to proactively reconfigure, and rapidly respond to disturbances. Detailed descriptions of functionalities at each layer of the architecture as well as the whole system are provided. Applying this comprehensive systems' approach, performance results for the IEEE 123 node test feeder are simulated and analyzed. The results show the trade-offs between system reliability, operational constraints, and costs involved. This work represents a novel strategy toward developing an analytical and multi-domain methodology to assess the effects of smart grid technologies on distribution system operations and performance.

Keywords: Power Systems, Power Systems Control, Power Systems Distribution, Smart Power Applications, Smart Grids

1. INTRODUCTION

Planning has already begun to replace much of the antiquated electric infrastructure of the existing power-delivery system with digital systems providing the grid with the capability to reconfigure itself and prevent widespread outages. Often, this collection of digital overlaid systems is referred to as smart grid. Upgrading the power grid, however, will present many new security challenges that must be dealt with before extensive deployment and implementation of smart grid technologies can begin. The digitalization of the electric grid may enable remote attacks to grow rapidly, potentially spanning countries or even continents (McDaniel & McLaughlin, 2009). Moreover, it is rapidly becoming easier to compromise computer systems due to the increased availability of hacker tools on the Internet and the decrease in technical knowledge required to use them to impose significant damage (Kropp, 2006). While digitalization of the electric grid will present many new security challenges, it will also provide the gird with increased flexibility to prevent and withstand potential threats.

In this paper, an intelligent distributed secure control architecture is presented for distribution systems to provide greater adaptive protection, with the ability to proactively reconfigure, and rapidly respond to disturbances. Section 2 provides an overview of distribution automation systems (DAS), Section 3 includes detailed descriptions of the functionalities at each layer of the architecture as well as the whole system, and Section 4 formulates the distribution system reconfiguration problem. Finally, Section 5 simulates and analyzes performance results for the IEEE 123 node test feeder, and Section 6 states some conclusions.

This work was supported by the National Science Foundation under grant number 0831059.

2. DISTRIBUTION AUTOMATION SYSTEMS

Due to its size, complexity, and cost, the transformation of the existing electrical grid to a smart self-healing system will need to occur in several stages over time. Since almost 90% of all power outages and disturbances have their roots in the distribution network, the transformation must begin at the distribution level (Farhangi, 2010) where customers will see the greatest increase in performance. In the United States, initial investments in smart grid technologies have highlighted this fact. Of the $3.4 billion awarded by the American Recovery and Reinvestment Act (ARRA) Smart Grid Investment Grants (SGIGs), announced in October 2009, only $148 million went to transmission related projects (Horowitz et al., 2010). Nearly all the rest went to distribution related projects.

A first step in the transformation will be in the development and wide-scale deployment of DAS. Currently, only a small minority of distribution systems worldwide are equipped with such capabilities. Even in North America, home of one of the world's most advanced power systems, less than a quarter of the distribution system is equipped with information and communications systems, and only about 15% to 20% of the system at the feeder level. As a result, many utilities believe that initially investing in distribution automation will provide them with increasing capabilities over time.

DAS are equipped with information and communications systems to provide system dispatchers with support for day-to-day operations. According to Bassett et al. (1988), common functions include:

- Automatic bus sectionalizing
- Feeder deployment switching and automatic sectionalizing
- Integrated volt/var control
- Substation transformer load balancing
- Feeder load balancing
- Remote metering
- Load control.

3. INTELLIGENT DISTRIBUTED SECURE CONTROL

The control of DAS can be either centralized or decentralized. In centralized control, all computing and control functions are based in one centralized location, while in decentralized control computing and control functions may be dispersed in many different locations. Centralized control, while easier to implement than decentralized control, is unable to respond quickly to adverse events at centralized control points. Decentralized control is able to respond quicker to adverse events, but the lack of information exchange may lead to unreliable or biased decision making.

For deeper and layered protection, an intelligent distributed secure control is required, which would enable parts of the network to remain operational and even automatically reconfigure in the event of local failures or threats of failure. With distributed intelligence and components acting as independent agents, those in each isolated area would have the ability to reorganize themselves and make efficient use of whatever local resources remain to them in ways consonant with the established global goals to minimize adverse impacts on the overall network. Local controllers would then be able to guide the isolated areas to operate independently while preparing them to rejoin the network, without creating unacceptable local conditions either during or after the transition.

Numerous sources in the literature proclaim how future distribution systems will employ control and communications technologies to achieve such goals. They discuss numerous operating capabilities such as how "the switches will communicate with each other and, using preset conditions, or even artificial intelligence, will operate without human intervention" (Bouford & Warren, 2007). The literature, however, provides few descriptions or models of how such objectives will be achieved and no analysis of the effects such technology will have on system operations.

3.1 Architecture

To achieve the desired goals stated above for distribution systems, an intelligent distributed secure control architecture was developed. The model was based upon the Strategic Power Infrastructure Defense (SPID) system control architecture produced by the EPRI/DOD Complex Interactive Networks/Systems Initiative (CIN/SI) for systems with intelligent wide-area sensing, protection, and reconfiguration capabilities (Electric Power Research Institute, 2002). Several concepts central to the SPID system were utilized in the design. A diagram of the resulting control architecture is shown in Fig. 1.

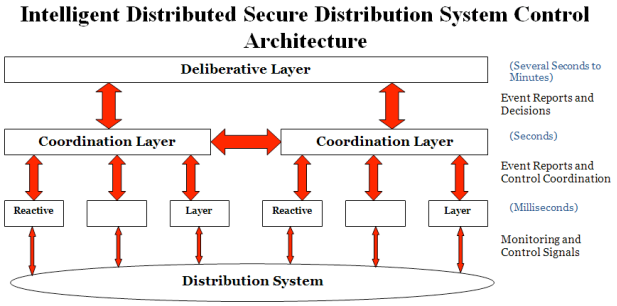

Fig. 1. Intelligent distributed secure distribution system control architecture (adapted from Electric Power Research Institute (2002)).

The model utilizes three layers composed of numerous independent, intelligent agents. A thorough description of what intelligent agents are and how they operate is provided in Amin & Ballard (2000). The agents gather and exchange information with each other in real-time or near real-time in order to provide coordinated protection and to optimize system performance.

A diagram of example control functions and signals being sent between different agents at each layer of the control architecture is shown in Fig. 2. In the diagram, each block represents the control functions for the agents at that layer, with the bottom block representing the reactive layer, the middle block representing the coordination layer, and the top block representing the deliberative layer.

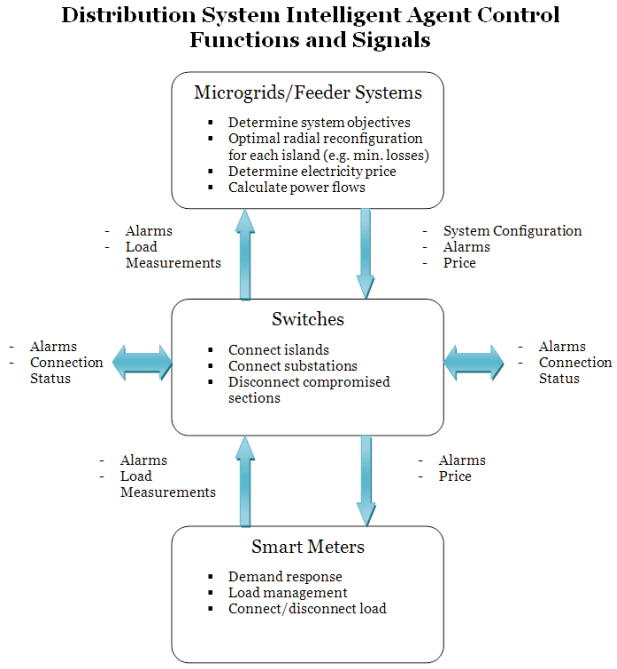

Fig. 2. Distribution system intelligent agent control functions and signals.

3.2 Reactive Layer

At the lowest control level, the reactive layer is composed of agents located at each smart meter, substation, and distributed energy resource in the system. The agents gather and

exchange information with adjacent coordination level agents. They respond to incoming price signals and alarms by performing demand response and load management functions, such as shedding load or shifting load to lower price times, and connecting or disconnecting load from the distribution system in response to attacks or natural disasters. In return, load measurements and alarm signals are sent back up to the coordination layer.

3.3 Coordination Layer

The coordination layer is composed of agents located at each tie-line or switch in the system. The agents exchange information with each other as well as forward signals sent by the reactive and deliberative layer agents to their appropriate destinations. They make decisions regarding their connection status, and take quick action if faults or attacks are detected. They have the ability to recognize if they are islanded from the rest of the system and to utilize whatever local resources are available to them. In addition, they implement optimal system configurations as determined by the deliberative layer agents.

3.4 Deliberative Layer

Finally, the deliberative layer is composed of agents located at the microgrid or feeder system level. The agents gather and exchange information with adjacent coordination layer agents and determine the overall system objectives such as increased network reliability or minimized line losses. They also determine the optimal system configuration for each island in their system based on the chosen system objectives and send these control signals down to the coordination layer agents for implementation. Furthermore, they perform analysis on their systems to determine if all operating constraints are met and aggregate system load in order to submit bids into real-time electricity markets at the transmission system level.

4. DISTRIBUTION SYSTEM RECONFIGURATION

Distribution system reconfiguration is one of the most important tasks of DAS. The objective is to determine the status of switches on the network in order to optimize system performance. The types of switches include both sectionalizing switches (normally closed) and tie-switches (normally open), and large feeder systems can contain several hundred switches. Normally, distribution system reconfiguration is performed for the following reasons: 1) to reduce line losses, 2) to alleviate network overloads, 3) to restore service to as many customers as possible following a fault on the system, or 4) to increase network reliability, with the majority of past work focusing on minimizing line losses (Ahuja et al., 2007), (Jazebi et al., 2008), (Karthikeyan et al., 2008), (Shirmohammadi & Hong, 1989).

Distributed intelligent secure control, however, provides the grid with the ability to dynamically optimize its configuration in the event of local failures or the threat of failures. Thus, new objectives can be developed for distribution system reconfiguration to take into account current system conditions.

4.1 Objective Function

A simple objective function is proposed to minimize the expected impact of cyber and physical disturbances on a system by taking into account its reliability, and the availability of its sensing, communications, and control systems. The latter is accounted for using the availability of each intelligent agent, which is continually changing due to the effects of cyber and physical attacks. The availability of each agent is calculated by finding the percentage of time it is operating in the up state over the total time being measured. Such values can be determined from operating records for each individual agent.

The expected impact of disturbances on a system is measured by computing the loss of energy expectation (LOEE) for a given configuration. The LOEE is calculated by finding the sum of the probabilities that the path from each load to its source is unavailable weighted by its load. The probability of each path being unavailable is one minus the product of the reliabilities and availabilities of each line and intelligent agent respectively encountered in the path. The LOEE and the path availability calculations are shown in (1) and (2) respectively.

$$LOEE = F\left(N, P_{load}, T\right) = \sum_{\forall i \in B, i \neq s} \left(1 - N_{is}\right) \times P_{load_i} \times T \qquad (1)$$

$$N_{is} = \prod_{\forall j,k \in L_{is}} R_{jk} \times \prod_{\forall l \in D_{is}} A_l \qquad (2)$$

Where:

- F - system LOEE
- B - set of all buses
- P_{load} - set of all real power loads
- P_{load_i} - real power load at bus i
- N - set of all path availability probabilities
- N_{is} - path availability probability from bus i to source bus s
- T - length of time period being measured
- L_{is} - set of all lines in the path from bus i to source bus s
- R_{jk} - reliability of the line from bus j to bus k
- D_{is} - set of all intelligent agents encountered in the path from bus i to source bus s
- A_l - availability of intelligent agent l

4.2 Problem Formulation

Constraints are added to the problem to ensure that all operating conditions are met. To maintain standard utility operating practices, the system is required to remain radially connected, and all scheduled loads must be served if possible. Radial system configurations are characterized by having a set of series components between a substation and each load point. Such configurations account for over 99% of all distribution systems in North America (Willis, 1997).

The resulting formulation for the distribution system reconfiguration problem is shown in (3)-(8).

$$\min F\left(N, P_{load}, T\right) \qquad (3)$$

s.t.

$$\left(P_{gen_i} - P_{load_i}\right) - \text{Real}\left\{V_i \left(\sum_{k=1}^{B_N} Y_{ik} V_k\right)^*\right\} = 0 \quad \left(\forall i \in B\right) \quad (4)$$

$$\left(Q_{gen_i} - Q_{load_i}\right) - \text{Imag}\left\{V_i\left(\sum_{k=1}^{B_N} Y_{ik}V_k\right)^*\right\} = 0 \quad \left(\forall i \in B\right) \quad (5)$$

$$\left|V_i\right|^{\min} \le \left|V_i\right| \quad \left(\forall i \in B\right) \quad (6)$$

$$S_{ij} \le S_{ij}^{\max} \quad \left(\forall i, j \in L\right) \quad (7)$$

System is radially connected (8)

Where:

P_{gen_i} - real power generation at bus i
Q_{gen_i} - reactive power generation at bus i
Q_{load_i} - reactive power load at bus i
B_N - number of buses
Y_{ik} - i,k term of the bus admittance matrix
V_i - complex voltage at bus i
$|V_i|$ - voltage magnitude at bus i
$|V_i|^{min}$ - minimum voltage magnitude limit at bus i
S_{ij} - complex power flow on line from bus i to bus j
S_{ij}^{max} - maximum complex power flow limit on line from bus i to bus j
L - set of all lines

Constraint (4) represents the real power equality constraints, (5) the reactive power equality constraints, (6) the bus voltage magnitude limits, and (7) the line complex power flow limits. To implement constraints (6) and (7), they are added as penalty factors to the objective function. The penalty factor formulations used for the bus voltage magnitude limits and the line complex power flow limits are shown in (9) and (10) respectively.

$$\text{voltage mag. limits penalty factor} = \sum_{i \in B} \max\left[\frac{\left|V_i\right|^{\min} - \left|V_i\right|}{\left|V_i\right|^{\min}}, 0\right] \quad (9)$$

$$\text{line flow limits penalty factor} = \sum_{i,j \in L} \max\left[\frac{S_{ij} - S_{ij}^{\max}}{S_{ij}^{\max}}, 0\right] \quad (10)$$

4.3 Annealed Local Search

Distribution system reconfiguration represents a discrete optimization problem. Since typical distribution systems can include hundreds of switches, exhaustive enumeration of all possible combinations (2^n) would quickly become computationally infeasible. This problem is further complicated by the addition of constraints such as those shown in (4)-(8). Nevertheless, the performance of the optimization, and ultimately the potential cost savings, increases dramatically as the number of switches increases (McDermott et al., 1999). Thus, the analysis technique must be able to handle large systems.

Both genetic algorithms (Jazebi et al., 2008) and simulated annealing have been applied to similar discrete optimization problems, but they encounter difficulty with the radial structure of distribution systems. Brown (2001) states two reasons for this being that: "1) most of the generated switch position combinations will not represent feasible solutions, and 2) generating a new radial tree structure for each combination of switch positions is computationally intensive." In addition, branch-and-bound methods have been attempted by Shirmohammadi and Hong (1989), but they provide no assurance that convergence will be reached, and for the cases where convergence is reached the computational burden to solve them is extremely high.

To determine the optimal radial configuration for the problem formulation described in Section 4.2, annealed local search (ALS) was used. ALS takes advantage of the radial structure of distribution systems and overcomes the shortcomings encountered by genetic algorithms and simulated annealing. The algorithm used was based on the one described by Brown (2001) for distribution system reliability optimization problems, which had been successfully applied to topologically diverse systems with up to 345 switches.

To adapt the algorithm for the current problem, a few modifications were made. The original algorithm made use of the *tie switch shift*, where a normally open switch was closed and a nearby upstream switch was opened, to make incremental changes to the radial system structure. However, to ensure that all feasible switch combinations were searched utilizing intelligent distributed secure control, search tables comprising the switches currently in the closed position, and those available in the opened position were generated. Each of the feasible switch combinations was then searched. The resulting method was found to be efficient, and straightforward to implement.

5. NUMERICAL CASE STUDY

To investigate the performance of the intelligent distributed secure control architecture described in Section 3 with ALS described in Section 4.3, the IEEE 123 node test feeder was simulated using MATLAB. Results were compared to those obtained using the sequential switch opening (SSO) method, a prevalent minimum loss reconfiguration algorithm for normal operating conditions, and decentralized and centralized control architectures as shown in Fig. 3 and Fig. 4 respectively. The SSO method is described by Shirmohammadi & Hong (1989).

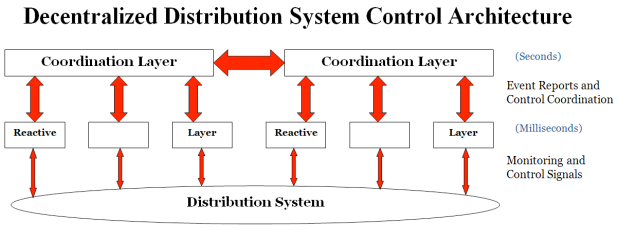

Fig. 3. Decentralized distribution system control architecture.

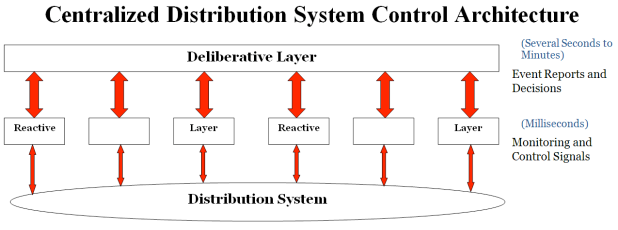

Fig. 4. Centralized distribution system control architecture.

The decentralized control architecture does not utilize deliberative layer agents for centralized decision-making. Thus, coordination and reactive layer agents utilize only local information and reconfiguration is performed using preprogrammed switching priorities. For the simulations, switches were prioritized by 1) being in the minimum loss

configuration and 2) from node. In contrast, the centralized control architecture does not utilize coordination layer agents for distributed decision-making. Thus, reconfiguration capabilities are not available in real-time, and can only be implemented with advanced planning, such as for maintenance or planned outages.

5.1 Test Case

A one-line diagram of the IEEE 123 node test feeder is shown in Fig. 5, and key system characteristics are listed in Table 1. Data for the IEEE 123 node test feeder and other test feeder cases are available from Kersting (2001).

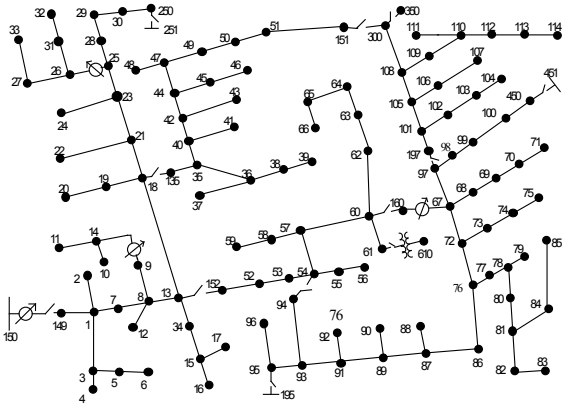

Fig. 5. IEEE 123 node test feeder one-line diagram (Kersting, 2001).

Table 1. IEEE 123 Node Test Feeder Key System Characteristics

	Value
Substations	4
Switches	12
Lines	118
Load (kW)	761.25
Base Voltage (kV)	4.16
Base Complex Power (MVA)	10

It was assumed that all elements were balanced in both impedances and loadings, which has traditionally been chosen as the best compromise between available resources and required results for such an analysis (Willis, 1997). Each line was set to have a reliability of 97%, each tie-line/switch was set to have a reliability of 100%, and the initial availability of each intelligent agent was set to 100%. The minimum bus voltage magnitude for each bus was set to $0.94\ pu$, and the maximum complex power flow for each line was set to $2{,}496kVA$ based on the standard practice by electric utilities of designing main feeder lines with an emergency rating of $600A$ (Short, 2004).

5.2 Customer Load Model

Each customer was modeled to have the load demand curve shown in Fig. 6, which is divided into three levels. The lowest level represents load that a customer absolutely requires in order to maintain basic living functions or critical business operations. It is assumed that this type of load comprises one-tenth of a customer's total electricity demand, and it is served regardless of electricity price.

The next level represents nondiscretionary load. It includes load that is necessary for a customer to maintain his or her basic quality of life or normal business operations, but it can

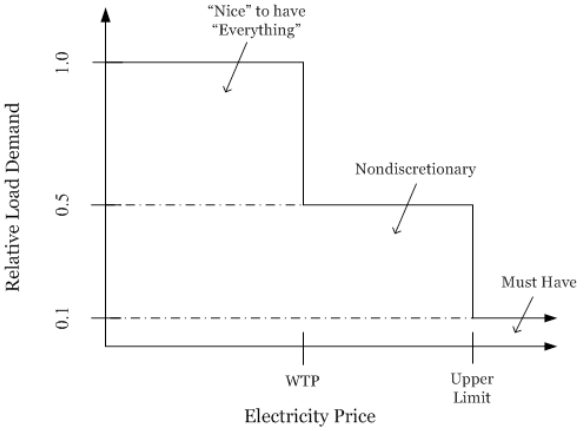

Fig. 6. Customer load demand curve.

be done without for short periods or in the event of an emergency. It is assumed that this type of load comprises four-tenths of a customer's electricity demand, and it is served as long as the electricity price is below some upper price limit, which is the same for all customers.

The last level represents discretionary or supplemental types of load that can be scheduled in advance or are unnecessary to maintain one's basic quality of life or normal business operations. This type of load is assumed to comprise one-half of a customer's electricity demand and it is served only if the electricity price is below one's willingness to pay (WTP). The WTP for each customer was randomly generated from a uniform probability distribution in the range $[0{,}100]\ \$/MWh$ and remained constant throughout the simulations.

5.3 Smart Meter Agents

Each smart meter agent is designed with demand response capabilities to shift discretionary and supplemental load from periods when the electricity price is above its owner's WTP or is unavailable to periods when the electricity price is below its owner's WTP and service is available. Furthermore, several protective measures were built into each smart meter agent to combat key threats to the smart grid as described by Winkler (2009).

To prevent abnormal loads from overburdening the system, each smart meter caps its owner's load demand during each hour to three times its average peak load based on past data. If an owner's initial load demand for one hour is below this limit, then additional load may be shifted to that hour until the limit is reached, as long as the electricity price is below his or her WTP.

To prevent brownouts from occurring, each smart meter is programmed to serve only necessary or "Must Have" load as shown in Fig. 6 when the price of electricity rises above some predefined upper limit set by the local electric utility or public utilities commission. The above actions help prevent adversaries from compromising the system and ultimately undermining consumer confidence.

5.4 Simulations

Simulations were executed for a length of 1,368 hours, and the electricity price and load demand curve data were

obtained from the Midwest Independent Transmission System Operator (MISO) (Midwest ISO, 2010). The electricity prices used were the real-time market clearing prices (MCPs) for each hour during the period from July 6, 2009 - August 31, 2009, and ranged from 1.79 $\$/MWh$ to 78.85 $\$/MWh$. An electricity price of 75 $\$/MWh$ was set as the upper price limit as shown in Fig. 6. The load demand curve for each customer was generated using the MISO actual load curve from July 6, 2009 - August 31, 2009 scaled to the value of each customer's peak load. The smart meters were enabled to shift discretionary or supplemental load as described in Section 5.3, and also to serve all discretionary load in the first available period regardless of price, as is the case in conventional distribution system operations.

Furthermore, random cyber attacks were enabled to occur for each reactive layer agent during each hour with a probability of 20%, and for each coordination layer agent during each hour with a probability of 10%. The probability of a reactive layer agent cyber attack was set to be greater than that of a coordination layer agent cyber attack because of their larger numbers and their increased vulnerability due to their tendency to be located in less secure areas. Because of the critical functions provided by the deliberative layer intelligent agent, which must be secured to ensure 100% uptime, it was assumed that it was protected to withstand all cyber attacks.

A successful cyber attack on a coordination layer agent or a reactive layer substation agent was assumed to immobilize the agent for the hour during which the attack occurred, while a successful cyber attack on a reactive layer smart meter agent was assumed to trigger the agent into emergency operation mode where only critical load is served as shown in Fig. 6 for the hour during which the attack occurred. In addition, line failures were enabled to occur, and a line failure was assumed to remove the line from operation for the hour during which the failure occurred.

In order to account for the variance in each simulation due to random cyber attacks and line failures, ten trials were performed, and the mean results were used for analysis. In addition, all simulations utilized initial configurations with minimum line losses.

5.5 Results

The simulation results are shown below. Fig. 7 shows the change in the LOEE for the different algorithms and control architectures simulated, Fig. 8 shows the change in line losses, Fig. 9 shows the cumulative sum of the voltage violations, and Fig. 10 shows the cumulative sum of the line flow violations. In addition, Table 2 shows the average discretionary, nondiscretionary, and total energy costs with system reconfiguration, with system reconfiguration without optimization, without system reconfiguration, and with and without demand response capabilities enabled. The intelligent distributed secure control architecture utilizes system reconfiguration capabilities, the decentralized control architecture utilizes system reconfiguration capabilities without optimization, and the centralized control architecture does not utilize any system reconfiguration capabilities.

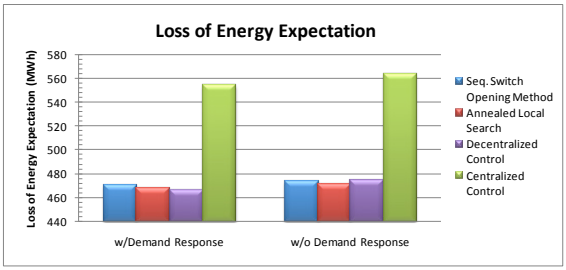

Fig. 7. Loss of energy expectation comparison.

Fig. 8. Line losses comparison.

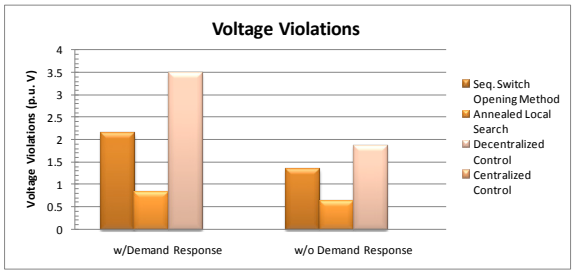

Fig. 9. Voltage violations comparison.

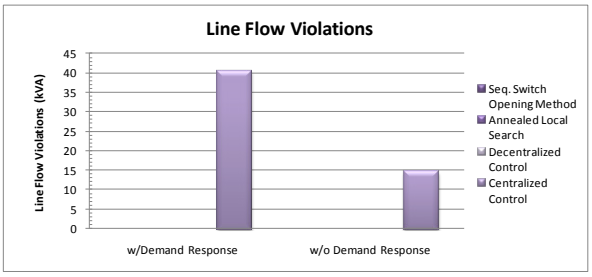

Fig. 10 Line flow violations comparison.

Table 2. Average Energy Costs

($\$/MWh$)	*w/DR*	*w/o DR*
Discretionary		
w/Reconfiguration	10.56	11.46
w/Reconfiguration (w/o opt.)	10.56	11.43
w/o Reconfiguration	10.51	11.45
Nondiscretionary		
w/Reconfiguration	11.41	11.46
w/Reconfiguration (w/o opt.)	11.42	11.45
w/o Reconfiguration	11.39	11.47
Total		
w/Reconfiguration	10.93	11.46
w/Reconfiguration (w/o opt.)	10.94	11.44
w/o Reconfiguration	10.82	11.46

5.6 Discussion

Fig. 7 shows that the intelligent distributed secure control architecture using both the SSO and ALS methods and the decentralized control architecture greatly improved the reliability and availability of the test system compared to the centralized control architecture due to the advanced reconfiguration capabilities enabled. Because of these

capabilities, however, Fig. 8 and Fig. 9 show that the amount of line losses and the severity of voltage violations greatly increased. Line flow violations did not have any measured effect on system operations except for the cases where the centralized control architecture was used as shown in Fig. 10. Comparing the ALS method to the SSO method, it can be seen from Fig. 7 - Fig. 9 that while the ALS method further improved the reliability and availability of the system, and decreased the severity of voltage violations, it resulted in an increase in line losses.

Table 2 shows that the use of demand response significantly decreased the average cost of discretionary energy served, and Fig. 7 and Fig. 8 show that it decreased or had no appreciable effect on the LOEE and line losses respectively for all algorithms and control architectures simulated. However, it resulted in an increase in the severity of voltage violations for the intelligent distributed secure control architecture using both the SSO and ALS methods, and the decentralized control architecture as shown in Fig. 9. It also increased the severity of line flow violations for the centralized control architecture as shown in Fig. 10.

Thus, for the test system, the price for minimizing cyber and physical disturbances using the intelligent distributed secure control architecture is increased line losses and voltage violations. To determine the most beneficial control architectures and algorithms to implement, the benefits from improved performance must be balanced against the operational costs.

6. CONCLUSION

In order to enhance the reliability, robustness, efficiency, and security of the power grid to meets the needs of today's digital society and those of the future, the end-to-end electric infrastructure must effectively utilize sensing, information, and control systems technologies to continually optimize system performance. The contributions of this paper can be summarized as follows:

1) An intelligent distributed secure control architecture is presented for distribution systems to provide greater adaptive protection, with the ability to proactively reconfigure, and rapidly respond to disturbances.
2) This work represents a novel approach toward developing an analytical and multi-domain methodology to assess the effects of smart grid technologies on distribution system operations and performance.
3) The model integrates aspects of cyber-physical security, dynamic price and demand response, sensing, communications, and dynamic optimization and reconfiguration.
4) Simulation results show the trade-offs between system reliability, operational constraints, and costs involved.

Future work will be focused on further improving the capabilities of the model, and simulating and comparing the effects of additional control architectures and technologies on distribution system operations and performance.

REFERENCES

Ahuja, A., Das, S., and Pahwa, A. (2007). An AIS-ACO hybrid approach for multi-objective distribution system reconfiguration. *IEEE Trans. on Power Systems*, 22(3), pp.1101-11.

Amin, M. and Ballard, D. (2000). Defining new markets for intelligent agents. *IT Pro*, July/August, pp.29-35.

Bassett, D.S. et al. (1988). Distribution automation and the utility system. In *Distribution Automation*, pp.1-6. IEEE Press, Piscataway, NJ.

Brown, R.E. (2001). Distribution reliability assessment and reconfiguration optimization. In *IEEE/PES T&D Conference and Exposition*, 2, pp.994-99.

Bouford, J.D. and Warren, C.A. (2007). Many states of distribution. *IEEE Power & Energy Magazine*, 5(4), pp.24-32.

Electric Power Research Institute (2002). *Complex Interactive Networks/Systems Initiative: Final Summary Report: Overview and Summary Report for Joint EPRI and U.S. Department of Defense University Research Initiative*. EPRI, Palo Alto, CA.

Farhangi, H. (2010). The Path of the Smart Grid. *IEEE Power & Energy Magazine*, 8(1), pp.18-28.

Horowitz, S.H., Phadke, A.G., and Renz, B.A. (2010). The future of power transmission. *IEEE Power & Energy Magazine*, 8(2), pp.34-40.

Jazebi, S., Hosseinian, S.H., Pooyan, M., and Vahidi, B. (2008). Performance comparison of GA and DEA in solving distribution system reconfiguration problem. In *11th International Conference on Optimization of Electrical and Electronic Equipment*, pp.185-90.

Karthikeyan, S.P. et al. (2008). Assessment of distribution system feeder and its reconfiguration using fuzzy adaptive evolutionary computing. In *Annual IEEE India Conference*, pp.240-45.

Kersting, W.H. (2001). Radial distribution test feeders. In *IEEE Power Engineering Society Winter Meeting*, 2, pp.908-12.

Kropp, T. (2006). System threats and vulnerabilities. *IEEE Power & Energy Magazine*, 4(2), pp.46-50.

McDaniel, P. and McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security and Privacy*, 7(3), pp.75-77.

McDermott, T.E., Drezga, I. and Broadwater, R.P. (1999). A heuristic nonlinear constructive method for distribution system reconfiguration. *IEEE Trans. on Power Systems*, 14(2), pp.478-83.

Midwest ISO (2010). *Midwest ISO - Documents*. [Online] Available at: http://www.midwestiso.org/publish.

Shirmohammadi, D. and Hong, H.W. (1989). Reconfiguration of electric distribution networks for resistive line losses reduction. *IEEE Trans. on Power Delivery*, 4(2), pp.1492-98.

Short, T.A. (2004). *Electric Power Distribution Handbook*. CRC Press, New York.

Willis, H.L. (1997). *Power Distribution Planning Reference Book*. Marcel Dekker, Inc., New York.

Winkler, I. (2009). Opinion: The hackability of the smart grid. *Computerworld*, December.