ADAPTATION OF RELAY OPERATIONS IN REAL-TIME

Thomas Nye, Student, IEEE
University of Washington
Seattle, WA U.S.A.
tnye@u.washington.edu

Chen-Ching Liu, Fellow, IEEE
University of Washington
Seattle, WA U.S.A.
liu@ee.washington.edu

Michael Hofmann
Bonneville Power Administ.
Vancouver, WA U.S.A.
mnhofmann1@bpa.gov

Abstract – Relays can degrade power system performance if they fail or are set incorrectly. Reports have shown that this degradation can lead to cascading outages. This paper will show how real-time communication with relays can help prevent these consequences. Through laboratory simulations, it is shown that real-time communication to protective relays can be achieved. This paper reports a new system that adapts automatic relay responses to make the power system more secure. The method of operation is explained.

Keywords: ***Real-time Communication, Adaptation, Power System Security, Wide-area Protection, Power System Protection, Relay Communication, Blackouts, Hidden Failure***

1 INTRODUCTION

The power industry is facing serious threats of major blackouts due to various sources of vulnerability in the grids. Enhancement of the power infrastructure from a technology point of view is an important issue for the years to come. This paper deals with the enhancement of protective systems in the real time environment. Relays are designed to protect the power system, but they can actually degrade the power system performance after an event occurs. An incorrect operation of a relay resulted in 3,000 MW of load shedding during an event in Idaho in 1995. Likewise, the 1977 New York City blackout was partially caused by relay misoperations. [1] The purpose of relays is to clear faults within their intended capabilities before the fault causes the system to become vulnerable. For a distance relay, the zone of protection is also referred to as "reach." By sensing the local voltage and current that are currently on the line in which they protect, relays determine whether or not a fault is present and perform a *pre-determined* function. This characteristic is in fact their limitation. More precisely, they only receive inputs from a small area of the power system to make decisions. Therefore, they are not well-equipped with sufficient inputs to calculate what is best for the power system as a whole. Furthermore, if they fail or are improperly set, they cannot optimally protect their zone. By adding the capability to communicate and analyze relay outputs from a wide area point of view, the effects of unwanted relay operations can be prevented.

The concept of adapting automatic relay operation has been proposed. In [2] the authors propose a novel backup protection expert system that changes present backup protection methods. The system identifies the location of the fault and trips and blocks relays to clear it. This system can reduce the wait period for backup protection. It can also eliminate the need for backup protection to be pre-programmed with automatic operations. Hidden failures have been identified in [3]. The authors identify the modes of failure in each piloting scheme. They also present a method to compensate for hidden failures by providing redundancy with digital relays. Furthermore, a method of adaptively calculating optimal relay settings has been proposed in [4]. These papers present the concept of adapting relay operations by inhibiting, tripping, or changing the automatic response.

Relays can degrade power system performance in two ways. First, the relays or a component inside of the relays may fail. Depending on the severity of the failure, it can either take the relay out of service or go undetected until an event occurs. If a failure is detectable, the relay can be monitored for the failure or be set to trigger an alarm if the failure occurs. Undetectable failures present a more difficult problem and are referred to as *hidden failures*. In [5] the authors provide an example of a hidden failure. They also propose that communication can block the relay from operating. Secondly, relays can be set incorrectly for the current power system conditions or the event that occurs. For example, if the threshold relay setting is set too low on a zone 3 relay, the relay can possibly falsely detect a fault under times of increased load since the voltage sags and the current increases. The relay does not fail in this case because it correctly performs the function that it has been programmed. The authors of [6] give a good example of how the zone 3 problem led to a cascading outage.

This research is a feasibility study to evaluate the idea of real-time communication to prevent the negative effects of relay operations. The main purpose is to study whether communication can adapt and inhibit relay operation in real-time. This paper reports that real-time communication to a relay is realizable and shows that it can adapt automatic relay responses. The real-time constraint will be answered in terms of the requirements and features of a real-time protection system. Papers that explain the theoretical basis for some methods of adapting relay operations have been proposed. However, most of them do not include any mention of how the application can be realized with such rigorous time constraints, on the order of milliseconds, or mention its implementation on the current protection system. In this paper, a simulation environment is set up to demonstrate that a relay can be communicated with in real-time.

2 THE REAL-TIME SYSTEM FOR ADAPTING RELAY OPERATION

An intelligent electronic device (IED) is similar to a computer in that it can receive inputs, process them, and produce an output. Therefore, an

IED can receive relay outputs from multiple relays and process them.

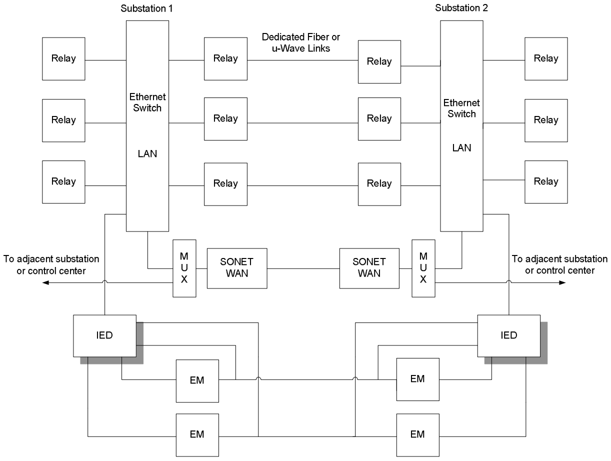

Figure 1: Real-time system for relay adaptation

Once it determines the appropriate actions to take, it can generate outputs to adapt relay operations in real-time. Figure 2 depicts an IED communicating with relays.

A real-time system to adapt relay operations is shown in Figure 1. The digital relays and intelligent electronic device (IED) connect to an Ethernet switch that forms the basis of the substation LAN. A multiplexer then connects the Ethernet switch to a SONET that creates the WAN. Electromechanical relays (EM) cannot connect to a network; their outputs and piloting channels are connected directly to the IED through the EM's communication box. Hence, the IED can send signals directly to the electromechanical relays and knows their operations. The multiplexer also provides the connection to other substations and the control center. The IED is the central control unit that processes the new functions of the network. The other hardware provides the backbone of the communication system.

This protection system incorporates the existing dedicated piloting channels currently deployed on power systems. It adds a network component to the relays that transmits GOOSE messages over either the WAN or dedicated links. GOOSE messages are event driven messages defined in the Utilities Communication Architecture [7]. Main protection keeps the same operation over dedicated links. Backup protection is achieved through the LAN/WAN. Also, the network provides supervision over the main protection schemes. It adds additional logic to aid in the prevention of over-tripping due to main protection failures.

It is important to note that the proposed system is not a replacement of the main or backup protection schemes currently deployed. It only adds an additional layer of communication that adapts automatic relay operations. It is not used as a replacement for main protection because of the uncertainty in message transmission times over the LAN/WAN. In some cases, depending on the level of loading and noises, the IED(s) will be able to transmit messages in a time frame before main protection operates. Therefore, it is capable of supervising the main protection scheme.

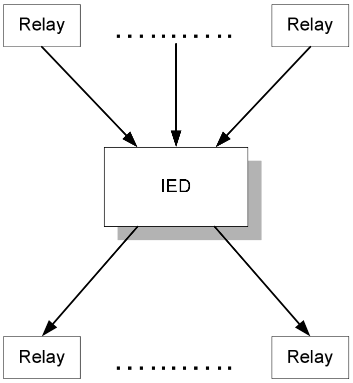

Figure 2: The process of IED control

GOOSE messages propagate through the network with event information. For example, if one of the logic operators in a relay changes state, indicating that a fault is present, the relay will send a GOOSE message over the LAN. It will be received by any IED or relay programmed to receive messages from that relay. The message then propagates over the WAN to other substations. The IED can initiate control signals. It either sends GOOSE messages to digital relays or directs signals to electromechanical relays. Specific examples of message propagation are given in later sections.

The proposed communication network and IEDs will have initiated built-in-test (IBIT) and continuous built-in-test (CBIT). Upon start-up, IBIT will run to make sure that the network is connected properly and that all devices are functioning properly. Throughout operation, CBIT will periodically perform a 'check' of the network. If an IED or communication link fails detrimental to the network, the new system becomes isolated from the old, existing system. Therefore, a fault in the new communication system will not degrade the reliability of the existing system. In terms of reliability, the two systems are isolated – failure modes in the new system do not cause failures in the existing system. Furthermore, the new system will be shown to prevent failures in the existing system from having an effect on the power system through conceptual examples and simulations. Therefore, the new system removes failure mode effects of the existing system. Removing failure mode effects increases the reliability of the protection system.

3 THE NEED FOR REAL-TIME CONTROL

The proposed system is intended to communicate with relays in real-time to inhibit, operate, or adapt the relay. The following sections describe why real-time communication is desirable for critical scenarios.

3.1 Hidden Failures

A *hidden failure* is a permanent defect that will cause a relay or a relay system to incorrectly and inappropriately remove a circuit element(s) as a direct consequence of another switching event [3]. Hidden failures have been identified in electromechanical relays and their sources are fault detectors, relay units, receivers, transmitters, directionality units, and timers. Hidden failures in digital relays have not been identified; it is assumed that they are less prone to hidden failures since they can self-monitor. Relays have a surrounding area termed, *region of vulnerability*, which defines the space that will be affected once a hidden failure has exposed itself. One key characteristic of hidden failures is that they do not affect the power system until an event occurs that makes the hidden failure *visible*, which means the operator can tell that a hidden failure has occurred [5].

Hidden failures can only be identified in the time frame just after an event has occurred. Once an event occurs, the hidden failure can be recognized and real-time communication can prevent its effects. In the real-time system considered in this paper, time is of the essence since some hidden failures can have an effect on the power system within milliseconds of event detection. Real-time control signals must be sent and received before this time elapses.

3.2 Backup Protection

Backup protection is intended to clear faults that main protection relays fail to clear. It consists of zone two and zone three relays that operate on timers set longer than zone one timers to give main protection sufficient time to clear the fault. Furthermore, there are also zone four elements in relays that look in the reverse direction and detect reverse faults. Their function is to inhibit tripping of the relay when a reverse fault occurs.

One of the key limitations of backup relays currently employed on power systems is that they sometimes unnecessarily trip the line in which they are connected. A more logical approach would be for protection to trip the circuit breakers adjacent to the fault. If that does not clear the fault, *then* trip the circuit breakers in the neighboring lines where the zone two and zone three relay elements are located. Secondly, backup protection has been known to false trip even after main protection has correctly cleared the fault. This excessive tripping can further lead to blackouts under stressed power system conditions. Today, backup protection can only see the voltage and current on the line in which it is attached.

Once the location of a fault is known, the appropriate signals can be sent over a communication network to trip and inhibit backup protection. In this sense, the real-time communication network proposed in this study can prevent backup operation from degrading the power system performance. It will supervise backup protection so that no operation occurs if main protection has cleared the fault. When the real-time signal is received, the timer of the zones can be stopped to prevent tripping.

3.3 Inadequate Relay Settings

Relay engineers choose the settings of relays based on information of worst case fault conditions. These settings are then periodically reviewed by the engineers to see if the settings are still applicable. Adaptive relaying applies a continual refinement of the settings as the system state changes. As the system state changes, the measured impedance seen by distance relays changes and if it encroaches on the relay setting, it can cause a false trip. To compound the matter, as the voltage sags and current picks up during times of heavy load, a false trip can cause the system to become unstable and, in the worst case, lead to catastrophic failures. A change in system state has the largest impact on zone three relays. Power system operators want zone three relays set securely or dependably [4].

A real-time communication network can distribute appropriate settings to relays. The real-time system proposed in this paper can implement adaptive relaying to change relay settings.

4 SYSTEM REQUIREMENTS

The proposed system has features that give it real-time performance. The authors of [8] give requirements for power system protection communication channels. First, the protection system needs to have exclusive use of a channel or channel slot in a bundle of channels, such as an optical fiber. In current pilot protection schemes this requirement is already met; only the relays have access to the channel being used for protection. If protection were accomplished through a wide-area network, the network should be used exclusively for protection purposes. If the network has too much traffic, losses may occur and degrade the performance.

In [9] the authors test a network under loaded and noisy conditions to record GOOSE message transmission times at 100Mbps. Under no loading the transmission time was 9.85 milliseconds. The loading of the network was then increased, while at the same time a pulse train was injected to simulate noise. The maximum and typical transmission times that were recorded for different levels of load are given in Table 1.

Loading Percentage (%)	**Maximum Time (ms)**	**Typical Time (ms)**
10	20	13
20	25	13
30	32	13
40	32	13
50	37	15
60	44	15
70	29	16

Table 1: Network Test under Loaded Conditions

The maximum time delay experienced increases as the load increases; the range of transmission times also increases. The unexpected low maximum time experienced at 70% loading is most likely due to experimental error. Network based protection should exclusively occupy a LAN and WAN to guarantee real-time performance in main and backup schemes.

The second requirement in [8] is that intermediate devices in the system be limited to none. In current piloting schemes no devices lie between the teleprotection relays. Intermediate devices add delay to the network and add another possibility of failure. These requirements and others have led to the design of the real-time system proposed in this study.

5 PREVENTION OF HIDDEN FAILURE EFFECTS

Figure 3 represents the same real-time system in Figure 1, except four substations are depicted and the WAN is not shown. Only direct links and the substation LAN are shown because they serve the purpose of preventing the effects of hidden failures. The dark black lines indicate the paths in which signals are sent in this example.

The LAN in Substation A connects the IED and relay R_c. The rest of the connections are dedicated links. In this example, a fault occurs between Substations A and C. The main protection on the line will clear the fault, but the transmission line between Substations A and B will disconnect because of a hidden failure. This example will show that if the IED receives the outputs of the relays that are protecting the line between Substations A and C, it can generate a block signal and prevent the relay in Substation B from tripping.

Relay EM_m in Substation A has a hidden failure that makes the relay incapable of detecting a reverse fault. The hidden failure would normally cause the line between EM_m and EM_a to trip unnecessarily in the Directional Comparison Blocking (DCB) scheme, but the real-time system will prevent it from happening.

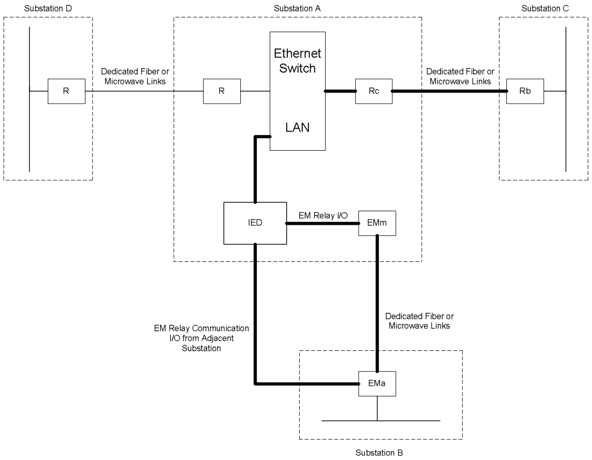
Substation D
Substation A
Substation C
Dedicated Fiber or Microwave Links
R
R
Ethernet Switch
LAN
Rc
Dedicated Fiber or Microwave Links
Rb
IED
EM Relay I/O
EMm
Dedicated Fiber or Microwave Links
EM Relay Communication I/O from Adjacent Substation
EMa
Substation B

Figure 3: Four substation depiction

When the fault occurs, relays EM_a, R_c and R_b will detect the fault and after a period of time the IED receives signals indicating their detection. Relay EM_m would normally send a block signal to relay EM_a to prevent it from tripping, but the hidden failure prevents it from sending the signal. The logic in the IED determines that the fault is present between relays R_c and R_b, since it receives trip signals from them. Since no signal is sent from relay EM_m, the IED generates and sends a blocking signal to relay EM_a.

A time log of these events is given in Table 2. The nominal transmission time is used from the experiment in [9]. Load of the network, noise, and additional coordination time could increase the total time required.

Action	Time	Total Time	Reason for Time Delay
EMa and Rb indicate a fault	0	0	Na
IED receives EMa's signal	1	1	Delay in the dedicated link
Rc receives Rb's signal	1	1	Delay in the dedicated link
Rc sends a GOOSE to indicate a fault	5.4	5.4	Preprocessing time of the message
Rc sends a second GOOSE message per Rb	5.4	6.4	Rc to process Rb's signal and send a GOOSE
IED receives Rc's first GOOSE message	3.174	8.574	Allows for GOOSE LAN propagation
IED receives Rc's second GOOSE message	3.174	9.574	Allows for the GOOSE message to go across the LAN
IED sends blocking signal to EMa	6.426	16	1ms for coordination between signals, 4.426ms for post processing time, and 1ms for algorithm processing time
EMa receives the blocking signal	1	17	Delay in the dedicated link

Table 2: Time-log of Hidden Failure Prevention

The time delay setting in the relays involved in the scheme should be set with good margin above the total time given in Table 2 to ensure that the blocking signal is received under loaded and noisy conditions. The time-log shows that the real-time system can prevent this hidden failure from having an effect since the block signal is received within the twenty millisecond standard for DCB schemes. The main protection scheme is more secure when relay outputs are received from adjacent substations. This is the most challenging application since the failures are in main protection schemes.

6 INHIBITION OF BACKUP PROTECTION

When the main protection has cleared a fault, backup protection has still operated in some instances. The real time system proposed in Figure 1 can aid in the prevention of this over-tripping. If a fault occurs and main protection clears it, open circuit breaker status can be sent by GOOSE messages over the WAN and received by the IED. The IED then issues block signals to zone two and three relays upon receipt.

Figure 4 extends the real-time system proposed above to three substations connected by main protection channels and the WAN. A fault occurs between relays R_b and R_c. Assuming the Permissive Underreaching Transfer Trip (PUTT) scheme, these relays send instantaneous trip signals to their respective circuit breakers. The trip signals will be received by each IED. Relay R_a will also indicate that it detects a fault in zone two and a message will be received by each IED indicating its change in state.

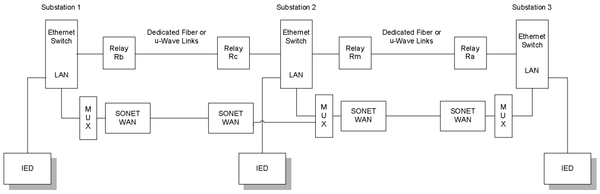

Figure 4: Three substation depiction

Once the breakers open, GOOSE messages will be generated because of their change in state. These messages will be received by the IED(s). The IED will in turn send a block signal to relay R_a to keep its zone two element from tripping its circuit breaker. A time-log of events is given in Table 3. It shows that the overall time required is much less than the typical zone two delay setting of 200 milliseconds. The transmission time of GOOSE messages is assumed to be the nominal transmission time in [9]. Added network load, noise, and additional coordination time between the receipts of events will increase the required total amount of time for this process to occur.

Action	Time	Total Time	Reason for Time Delay
Rb,Rc and Ra indicate a fault	0	0	Na
Rc receives Rb's signal	1	1	Dedicated link
Rm receives Ra's signal	1	1	Dedicated link
Rc sends a GOOSE	5.4	5.4	Preprocessing time of the message
Rc sends a GOOSE per Rb	5.4	6.4	Rc processes Rb's signal and send a GOOSE message
Rm sends a GOOSE per Ra	5.4	6.4	Rm processes Ra's signal and send a GOOSE message
IED receives Rc's first GOOSE	3.174	8.574	Allows for the GOOSE message to go across the LAN
IED receives Rc's second GOOSE	3.174	9.574	Allows for the GOOSE message to go across the LAN
IED receives Rm's GOOSE	3.174	9.574	Allows for the GOOSE message to go across the LAN
Open circuit breaker status sent	55.4	55.4	50ms circuit breaker operation and 5.4ms for pre-processing
IED receives breaker status	3.174	58.574	Allows for the GOOSE message to go across the LAN
IED receives breaker status	4	59.4	Allows for the GOOSE message to go across the WAN
IED sends a block signal to Ra	6.426	65.826	1ms for coordination between signals, 4.426ms for post processing time, and 1ms for algorithm processing time
Ra receives IED's block signal	4	69.826	Allows for the GOOSE message to go across the WAN

Table 3: Time-log of Zone 2 Over-tripping Prevention

Sometimes circuit breakers have internal faults. When this occurs, the contact might indicate that the circuit breaker is open, but in actuality it has stayed closed. A GOOSE message will still be sent by the circuit breaker indicating that it is open. Therefore, the IED will issue a block signal to the zone two relay. However, the block signals have duration. The duration of the block signal can be set at approximately 100 milliseconds. After the block signal expires, if the zone two relay is still detecting a fault, it can again start its zone two timer and can trip for the fault. Block signals having duration prevents failed circuit breakers from having effects as well.

7 HARDWARE SIMULATION OF RELAY INHIBITION

A small-scale realization of adapting relay operation in real-time has been tested at Bonneville Power Administration (BPA) laboratories. The goal of the simulation is to prove that a blocking signal can be sent to a relay before the relay can issue a trip signal to its associated circuit breaker. In this simulation, two relays were set up to mimic the zone protection on BPA's power system, as shown in Figure 5.

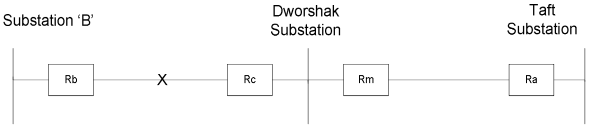

Figure 5: The power system simulation

A fault was simulated to occur between the Dworshak substation and one of its adjacent substations, labeled Substation B. A relay was chosen in the other adjacent substation, Taft, to receive a block signal as a means of preventing it from tripping in zone two. The relay in the Dworshak substation, R_c, and the relay in Substation B, R_b, should detect the fault and clear it in zone one. In normal operation, the relay at the Taft substation, R_a, would detect the fault in zone two and not issue a trip signal since the zone one relays have already cleared the fault. However, in this fictitious simulation scenario, the time delay setting on the zone two relay is set as the same time delay setting on the zone one relay so that they will both issue trip signals at the same time. Furthermore, the trip signal from R_a will be prevented by sending a block signal within its time delay setting. If the block signal prevents the relay from sending a trip signal, the simulation will meet its goal.

The hardware system used to run the simulation is given in Figure 6.

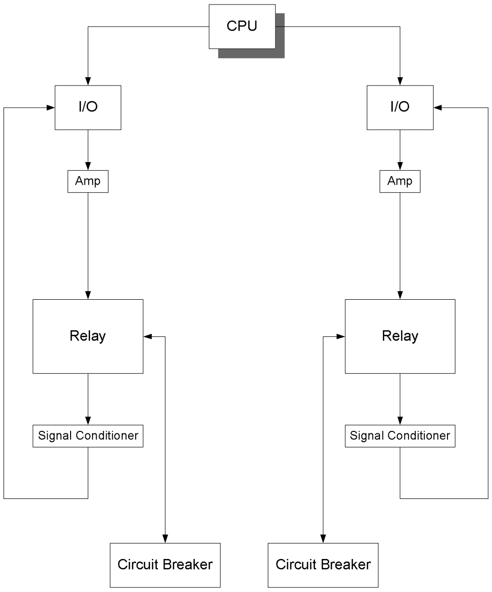

Figure 6: Hardware setup

The CPU is loaded with fault data from previous fault analysis. The data is played as input into the relay to simulate a fault. The outputs of the CPU are digital signals. These include the simulated fault conditions and the generated block signal, BT. A phase A one line to ground fault was simulated to occur at 100 milliseconds. Many relays can correctly identify a fault within eight milliseconds. This time delay is due to the process time of the running algorithm that detects the fault. Hence, the relays will detect the fault at 108 milliseconds. The blocking signal was expected to be sent at 124 milliseconds, which is 16 milliseconds after the relays detect the fault. Since the relays were set with a trip delay of 20 milliseconds after detection of a fault, they will try to issue trip signals at approximately 128 milliseconds. The blocking signal has to arrive before the trip occurs to achieve real time control.

One of the I/O's functions is to convert the CPU's digital signals into analog signals. These analog signals are then amplified by amplifiers. Its second function is to collect signals from the two relays. Relay signals refer to logic operations and trip signals. Once it collects the signals from the relays, it sends them to the CPU.

The signal conditioner takes the 130 volt output from the relay and converts it to 5 volts so that the I/O can receive the relay signals. The I/O can only receive signals at this voltage. It acts as a step-down transformer.

The relays are both set with a time delay of 20 milliseconds and are enabled for a single-pole trip. Once a fault has been detected, the relay will issue a trip signal to the circuit breaker after 20 milliseconds. One of the inputs, IN12, on the relays is set to receive a blocking signal. The output logic has also been changed on both relays to accommodate the blocking signal. The existing output logic was AND with '!BT', which is the logical NOT of the blocking signal. When the relay receives the BT signal, a logical one, the AND with the NOT of this signal is logical zero and no output trip signal to the circuit breaker will be sent. This logic was changed on all three outputs of the relays that are responsible for issuing trip signals to the circuit breakers.

First, the test was run without sending the blocking signal. Both relays correctly detected the fault, issued trip signals at the same time, and opened the circuit breakers. The test was then run again, except this time a blocking signal was sent to relay R_a. This time only the zone one relay issued a trip signal. The zone two relay did correctly detect the fault, but since it received a signal on IN12, it did not issue a trip signal to the circuit breaker. Therefore, the blocking signal prevented the zone two relay from operating in a real-time fashion.

Figure 7 depicts the outputs of relay R_a when no blocking signal is received. MAG2, XAG2, Z2G refer to logical operations that are used to detect the presence of faults. The presence of signal TPA indicates that the relay issued a trip signal to the circuit breaker.

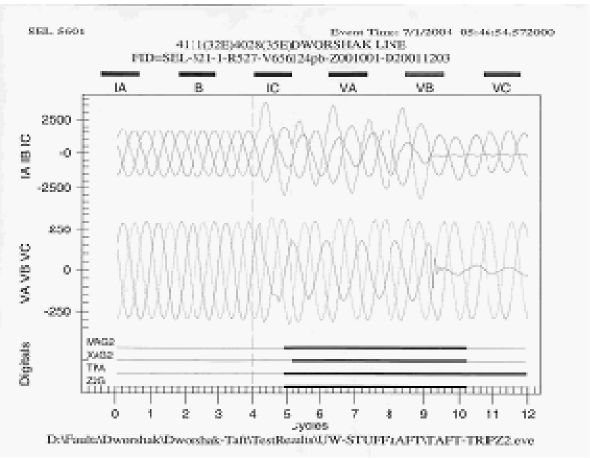

Figure 7: The zone two relay operates.

Figure 8 depicts the outputs of relay R_a when the blocking signal is received. The logical operations MAG2, XAG2 and Z2G are all the same. However, no TPA signal is generated, which means that no trip signal was sent to the circuit breaker and by manual observation, the circuit breaker did not open. The signal IN12 (blocking signal) was received by the relay and it effectively blocked generation of the trip signal TPA.

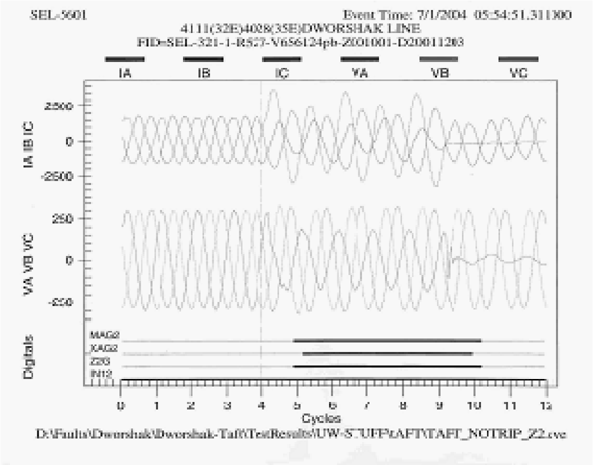

Figure 8: The zone two relay does not trip.

The event data reports from the relays were also analyzed. The event reports show that relay R_a did not trip when the blocking signal was received. The expected operation in both cases is to not trip since it is zone two detection. However, when the blocking signal is not received, the actual operation is trip.

The results prove that a relay can receive a blocking signal to inhibit it from issuing a trip signal in real-time. The simulation also forms the basis for other applications such as the hidden failure example of the Directional Comparison Blocking scheme. Instead of sending the blocking signal to the zone two relay, it could have been sent to a relay in the DCB scheme. Upon analysis of an external fault, an IED would determine that no blocking signal has been sent by the relay and issue one in its place.

To expand on the simulation further, the logic could be modified in the relays to change the blocking signal to a trip signal. Trip signals could be sent to main protection devices. The simulation has shown that a signal can be received by a relay in real-time to adapt its automatic operation.

8 CONCLUSION

Blackouts can be prevented by adapting automatic relay responses with increased communication. This study has shown how adaptation of relay operations can be achieved in real-time. Pre-programmed relay functions can degrade the power system performance when they are incorrect or fail. Real-time communication can prevent their effects and improve the power system security. The real-time system in this study incorporates the existing main and backup protection schemes while adding an additional layer of supervision. It has been based on specific real-time requirements and features.

This paper reports the results of a feasibility study. Further work in this area includes a larger test set-up on a network to simulate real-time performance. A larger test set-up would demonstrate how relays respond when they are connected to a network. Also, an IED needs to be designed with multiple functions and a higher level of logic. The device must be able to receive multiple inputs, analyze them, and send outputs. Further economic analysis also needs to be performed. For a power system to implement the real-time system proposed, a business case must be made. A business case would show the expenses saved by adapting relay operation in a year and explain how an initial investment in a real-time system would pay for itself.

9 ACKNOWLEDGEMENTS

The authors would like to thank the Advanced Power Technologies (APT) Center at the University of Washington for providing the tools necessary to complete this project. The APT Center is sponsored by AREVA T&D, Bonneville Power Administration, CESI, LG Industrial Systems, PJM Interconnection, and RTE. The project would not have been as successful without the help of the Grainger Foundation. We also appreciate the support from Bonneville Power Administration.

REFERENCES

[1] A.G. Phadke and J.S. Thorp, “Expose Hidden Failures to Prevent Cascading Outages,” Computer Applications in Power, IEEE, vol. 9, no. 3, pp. 20-23, July 1996

[2] J.C.Tan, P.A.Crossley, D.Kirschen, J.Goody, and J.A.Downes, "An Expert System for the Back-Up Protection of a Transmission Network," Power Delivery, IEEE Transactions on, vol. 15, no. 2, pp. 508-513, Apr. 2000.

[3] Anatomy of Power System Blackouts and Preventive Strategies by Rational Supervision and Control of Protection Systems, ORNL/SUB No.19X-SD630C, prepared for Energy Division, Oak Ridge National Laboratory, Martin Marietta Energy Systems, Inc., Oak Ridge, TN, 1993

[4] B.Stedall, P.Moore, A.Johns, J.Goody, and M.Burt, "An Investigation Into the Use of Adaptive Setting Techniques for Improved Distance Back-Up Protection," Power Delivery, IEEE Transactions on, vol. 11, no. 2, pp. 757-762, Apr. 1996.

[5] C.C. Liu, J. Jung, G.T. Heydt, V. Vittal, and A.G. Phadke; “Conceptual Design of the Strategic Power Infrastructure Defense (SPID) System,” IEEE Control System Magazine, vol. 20, no. 4, pp. 40-52, Aug. 2000.

[6] C.W. Taylor and D.C. Erickson, “Recording and Analyzing the July 2 Cascading Outage,” Computer Applications in Power, IEEE, vol. 10, no. 1, pp. 26-30, Jan. 1997

[7] "Fundamentals of Utilities Communication Architecture," Computer Applications in Power, IEEE, vol. 14, no. 3, pp. 15-21, July 2001.

[8] S.Ward, T.Dahlin, and B.Ince, "Pilot Protection Communication Channel Requirements," RFL Electronics. 2 Dec. 2004. <http://www.rflelect.com>.

[9] G. Scheer and D. Woodward, "Speed and Reliability of Ethernet Networks for Teleprotection and Control," Schweitzer Engineering Laboratories, Inc. 2001. 2 Dec. 2004. <http://www.selinc.com/techpprs/6116.pdf>.