3-22-2018

Evaluation of Resiliency in a Wide-area Backup Protection System via Model Checking

Kolby H. Elliot

EVALUATION OF RESILIENCY IN A WIDE-AREA BACKUP PROTECTION SYSTEM VIA MODEL CHECKING

THESIS

Kolby H. Elliott, Capt, USAF

AFIT-ENG-MS-18-M-023

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-18-M-023

EVALUATION OF RESILIENCY IN A WIDE-AREA BACKUP PROTECTION SYSTEM VIA MODEL CHECKING

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Engineering

Kolby H. Elliott, B.S.E.E.

Capt, USAF

March 22, 2018

AFIT-ENG-MS-18-M-023

EVALUATION OF RESILIENCY IN A WIDE-AREA BACKUP PROTECTION SYSTEM VIA MODEL CHECKING

THESIS

Kolby H. Elliott, B.S.E.E.
Capt, USAF

Committee Membership:

Dr. Kennith M. Hopkinson
Chair

Dr. Douglas D. Hodson
Member

Dr. Laurence D. Merkle
Member

Abstract

Modern civilization relies heavily on having access to reliable power sources. Recent history has shown that present day protection systems are not adequate. Numerous backup protection (BP) systems have been proposed to mitigate the impact of primary protection system failures. Many of these novel BP systems rely on autonomous agents communicating via wide-area networks. These systems are highly complex and their control logic is based on distributed computing. Model checking has been shown to be a powerful tool in analyzing the behavior of distributed systems. In this research the model checker SPIN is used to evaluate the resiliency of an agent based wide-area backup protection (WABP) system. All combinations of WABP system component malfunctions that lead to system failure are identified and classified. The results of this research indicate that the WABP system evaluated is more resilient to component malfunctions than previously reported. Possible WABP system improvements are introduced as well.

Acknowledgements

I would like to thank my wife for her unwaivering support, my sister for many refreshing study breaks, my schnauzer for his incessant motivation, and my otocinclus for his inspiration.

Kolby H. Elliott

Table of Contents

Page

List of Figures

List of Tables

EVALUATION OF RESILIENCY IN A WIDE-AREA
BACKUP PROTECTION SYSTEM VIA MODEL CHECKING

I. Introduction

This first chapter provides an overview of the thesis subject matter and an introduction to the problem. It details the research goals and contributions. It ends with a review of the entire document.

1.1 Motivation

Electricity plays a part in every aspect of American life from lighting to climate control, from transportation to communication. As the use of electricity becomes more pervasive in human life, so too does human dependence on having a reliable source of electricity. In 2003 that source was interrupted for 50 million people in the U.S. and Canada, for up to four days in some areas. This outage resulted in an estimated $10-billion in damages. The cause of that outage is complicated. One key element identified was the inability to maintain the situational awareness needed for remote monitoring and backup protection. This inability was attributed to a lack of adherence to standards [25]. Adhering to these standards can be costly and difficult as they are complicated and sometimes ambiguous.

The design of existing backup protection (BP) systems has focused largely on robustness rather than resiliency. Robustness is the measure of how difficult it is to break something. It is largely a function of using high quality products, precision manufacturing, and regular maintenance. On the other hand, resiliency is the measure of how many components in the system can malfunction and the system still

exhibit the desired behavior. Resiliency is generally achieved through overlapping functionality and redundant components or processes.

Existing backup protection systems do not make effective use of modern telecommunications advancements. Instead they rely on localized sensors and relays that have no ability to communicate critical information to neighboring BP systems elements in a timely manner. Overall situational awareness is maintained at regional control centers; however, long distance communication latency greatly reduces the ability of the control center to respond to faults in a timely manner [36]. The response delay is further impacted by employing human-in-the-loop decision making as opposed to fully autonomous systems.

Numerous alternate BP systems that employ autonomous agents have been proposed [43, 41, 12, 2, 18, 38, 21, 22]. These agents would develop a partial picture of the event based on sensor readings passed between neighboring substations and make more advanced control decisions based on predefined algorithms. The distribution of these agents would also enable them to provide backup for each other, thus greatly improving the BP systems resiliency. Additionally, the closer geographic proximity of these agents and their completely autonomous nature would greatly reduce their response times. That being said, the logical complexity of these systems causes problems. It is difficult to conduct large scale testing and the cost of implementation is prohibitive [39]. These factors make the risk of replacing existing backup protection systems too high.

The issue of rapidly increasing logical complexity is not new. Software development has been managing the impact of complexity for many years. One of the mitigation techniques they employ is model checking [3, 33]. Model checking utilizes formal methods to evaluate extremely complex systems and identify events and conditions that would cause the system to respond in an undesirable manner. This

research shows that employing model checking techniques can provide insight into the properties of a novel autonomous agent-based BP systems prior to implementation and in a cost-effective manner.

1.2 Problem Statement

Proposed autonomous agent-based BP systems have the potential to provide faster responses to more complicated fault scenarios and reduce the impact of component malfunctions. However, these systems are significantly more complicated and it is difficult to evaluate their response to all possible malfunction scenarios. Given that the response of each component has the potential to affect the response of each other component, it is no longer sufficient to evaluate each individual component of the BP systems. Due to this interdependency, evaluation of these systems' response is a combinatorically large problem. Small scale examples have been shown to behave in a desirable manner and this research explores a technique that can verify some of these systems' behavior on a larger scale.

1.3 Research Objectives

A large majority of today's research is focused on developing new BP algorithms and showing their response to a representative subset of the possible malfunction scenarios expected to be encountered in implementation. The objective of this research is to identify all possible scenarios that have the potential to result in undesirable system behavior and evaluate these scenarios. The specific research objectives are:

- Develop a model of a BP system implemented on a complete power transmission network.

- Identify all combinations of malfunctions in the model BP system that result in the BP system incorrectly responding to a given situation.
- Evaluate the malfunction combinations that result in incorrect BP system responses and identify common elements and patterns.
- Compare these results to previously identified responses in smaller scale BP system evaluations.

Completion of these objectives has resulted in a model that shows the response of the BP system to all possible combinations of a given number of component malfunctions. Successful completion of the model enabled the identification of all malfunction combinations that result in undesirable BP system behavior. The evaluation of these fatal fault combinations allowed for a quantitative analysis of the resiliency of the BP system as it is and insight to how it can be improved.

1.4 Approach

The approach used in this thesis was both qualitative and quantitative. The development of an analytical model capable of evaluating the desired properties while still being small enough to check exhaustively required a large number of details to be obfuscated [26]. Specifically, the behavior of the power transmission system and the sensors monitoring it are not modeled. Rather, the input from the monitoring sensors to the BP system is simulated. This enabled the behavior of the system to be evaluated against all possible combinations of inputs, not just those inputs whose cause could be simulated. The results obtained can then be analyzed by power systems experts to determine the possibility of those input combinations that lead to failures actually occurring in a real implementation of the system. The development of an analytical model also allowed for a larger sized system to be evaluated better

than a physical model would, given the amount of time and resources used. The development of the model relied heavily on the groundwork laid in a model used in a previous experiment.

1.5 Organization

This thesis is organized as follows:

Chapter 2 begins with a detailed introduction to the components used in protection systems in power transmission grids, their functionality, and their application. It then describes current primary and backup protection systems. Current research in agent-based wide-area backup protection (WABP) systems is then reviewed. The test WABP system that will be evaluated is introduced. Relevant research in model checking is reviewed and finally the model-checking tool SPIN is introduced.

Chapter 3 then describes the overall research objective in detail. It discusses critical constraints and limitations that impacted both the design of the model and the evaluation approach taken. Based on such limitations, it also discusses all critical assumptions made. The components of the model are discussed and the model-checking techniques are described. Finally, all hardware and software utilized to accomplish the overall objective are described.

Chapter 4 presents an analysis of the data collected. It introduces implications of applying model checking to the problem. A review of the test WABP system and its potential shortcomings is presented. Lastly, it provides a detailed recommendation for improving the selected BP system as well as some considerations for evaluating future BP systems.

Chapter 5 concludes the thesis with a summary of all research efforts and findings, proposes possible topics for future work, and enumerates the contributions of this research. It shows that this thesis provides further evidence of the usefulness of applying

model checking to complex problems and the need to evaluate interdependent systems on a sufficiently large scale to properly evaluate their behavior.

II. Background

This chapter presents information critical to a comprehensive understanding of BP systems and the use of model checking as an evaluation tool. It begins with the relays used in current protection systems where notable failures of existing BP systems are evaluated. The novel BP system that was selected for evaluation is discussed in detail. Then, the concepts of model checking are introduced. Once a foundation for model checking has been established, the history of its application to real world problems is discussed. Finally, the model checking software used for this experiment is introduced.

2.1 Protection Relays

Protection relays are devices that are designed to trip a circuit breaker when a fault is detected and they generally reside in the substation where the power line connects to the distribution bus [19]. Originally, relays relied on coils to operate on moving parts that would trip circuit breakers in the event of a power transmission system failure [5]. Each type of relay operates or activates in response to a single, specific abnormal operating condition such as over-current, over-voltage, reverse power flow, over-frequency, or under-frequency. Modern microprocessor-based digital protection relays, or Intelligent Electronic Devices (IEDs), are considerably more sophisticated. IEDs can provide additional types of protection by combining readings from numerous relays and applying logical algorithms before tripping breakers; however, they are limited to information provided by a single power line, or at most a subset of the power lines that intersect at a given substation. The two types of relays that are most pertinent to this research are directional overcurrent relays and zone distance relays.

2.2 Directional Overcurrent Relays

In a power grid, current can flow in any direction - both during normal operation as well as during a fault [45]. The presence of a fault is indicated by a spike in current, also known as fault current, that always flows towards the fault. The role of the IED during a fault is to isolate the faulted line by tripping the circuit breaker and disconnecting the faulted line from the rest of the power transmission grid. Therefore, it is necessary for the IED to know whether the fault is on the line that it monitors or on another line that is connected to the same bus. Since the IED is located at the connection between the power line and the bus, fault direction relative to that IED is ether in the direction of the line or in the direction of the bus. This information is provided by a directional overcurrent relay.

Protection areas are bounded between circuit breakers. When the circuit breaker is closed there is no appreciable impedance between the end of one protection area and the beginning of the next. A relay, therefore, cannot rely on fault current alone in order to determine the relative direction of the fault. That is to say, the relay sits on the boundary between two protection regions and the amount of current passing through the relay is not enough information to determine which of the two areas contains the fault. Since the impedance of the line is mostly reactive, a fault on the line side of the relay will result in a fault current that lags the bus voltage by a phase angle of almost 90 degrees. Conversely, a fault on the bus side of the relay will have a fault current that leads the phase angle of the bus voltage by almost 90 degrees. Therefore, the relative direction of the fault can be precisely determined by comparing the phase angle of the fault current to the phase angle of the fixed reference voltage on the bus [13].

2.3 Zone Distance Relays

A fault current in a power transmission grid has an effect on the entire grid. Therefore, it is not sufficient to detect the presence of a fault and its relative direction. The distance to the fault must also be known to determine if the fault has occurred within the protection area bounded by a given circuit breaker. This is accomplished through the use of an impedance relay.

During normal operation, load currents are usually much smaller than fault currents; therefore, the observed impedance of a faulted line is smaller than during normal operation. This property is leveraged in the design of distance relays by setting a threshold impedance, Z_r, which is the expected minimum impedance of the line during normal operation. If the observed impedance Z is less than the threshold impedance Z_r, then the fault is said to fall within the reach of the relay. This is fairly simple in principle and application, though, there are some complications that arise in implementation.

Unfortunately, the impedance of a transmission line is not fixed as many factors affect the impedance of a line. The more significant factors that affect the impedance are: the length of the line, the line temperature, and the line's proximity to other parallel lines. The transmission of electricity is not lossless; even at very high voltages, some energy is lost as heat. During normal operation, as the current in the line increases, the temperature of the medium increases. The temperature of the medium, generally aluminum or copper, directly affects its conductive properties as well as causing it to expand. This expansion causes the line to sag and increases the end-to-end length of the transmission line, thus further impacting its observed impedance. Additionally, high winds can cause lines to swing, changing the distance between parallel lines and thereby changing the impact of their respective magnetic fields on each other, once again affecting impedance.

To account for the variable nature of observed end-to-end line impedance, the threshold Z_r is set at between 70-90% of the expected end-to-end impedance of the line. This ensures that any fault that results in an impedance relay observing a Z that is less than Z_r can be assumed to be on that line. However, given that the reach of the impedance relay is at most 90% of the length of the line, it is possible for Z to be greater than Z_r and for the fault to still be on that line - just at the far end. This is remedied by the use of zone protection.

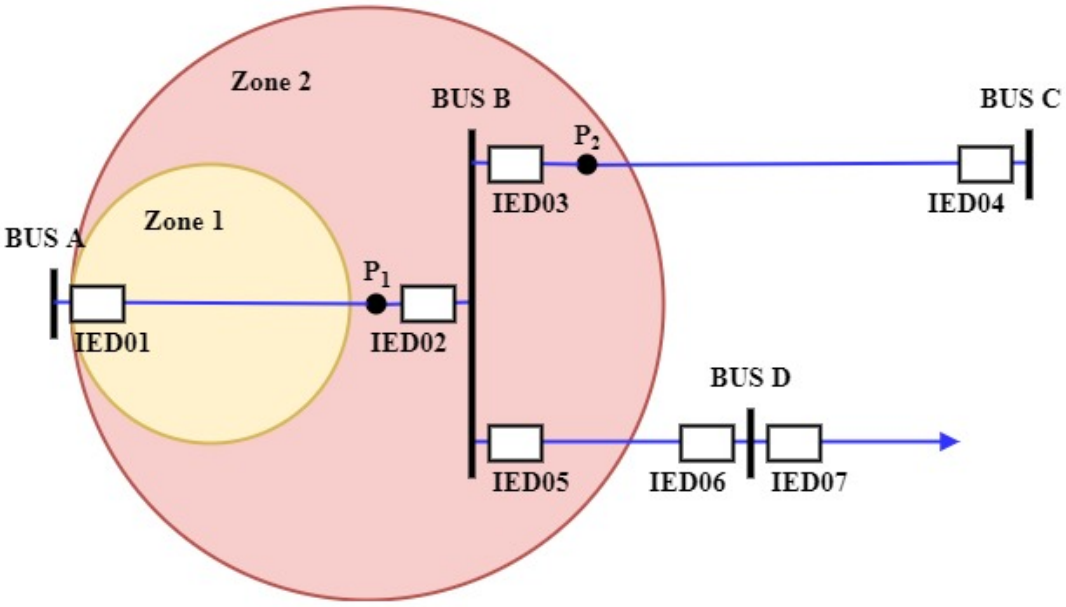

Figure 1. Range of Zone Distance Relays

Impedance relays are employed as distance zone relays as follows. Two impedance relays in each IED are given different threshold impedances: Z_{r1} and Z_{r2}. The first impedance relay, call it the zone 1 relay, has a threshold impedance (Z_{r1}) set to 80% reach. The second impedance relay, call it the zone 2 relay, has a threshold impedance (Z_{r2}) set to 120% reach. Therefore, if a fault occurs at point P_1 on line AB (Figure 1) the zone 1 relay in IED01 will observe an impedance, Z, that is greater than Z_{r1} and it will not activate. The zone 2 relay in IED01 will observe the same impedance, Z;

however, it is less than Z_{r2} and the relay will activate, indicating that IED01 should trip the breaker.

This ensures full coverage of line AB; however, it has the potential to cause problems if a fault occurs at point P_2 on line BC, which is also within the reach of the zone 2 relay. If the zone 2 relay in IED01 responds to the fault located at P_2 and trips the breaker, it will cut off line AB even though the fault is on line BC. To remedy this, zone 2 relays are designed with a 0.2-0.3 second delay timer. This allows the closer zone 1 relay in IED03 a chance to trip its breaker and clear the fault before neighboring lines are unnecessarily cut off.

These two types of relays are generally used in series with the directional overcurrent relay used as a blocking relay. This is due to the fact that the reach of a zone relay is not directional even though it is set as if looking down the line. Therefore, any fault on the bus side of the relay that results in a high enough fault current, such that the observed impedance, Z, is less than Z_r, will activate that relay. Placing the two types of relays in series results in the circuit breaker tripping only if both the directional overcurrent relay and the zone distance relay both activate. A common alternative to this configuration is the use of modified impedance relays (or mho relays); however, their description has been omitted as the system modeled in this experiment utilizes series relays as described here [13].

2.4 Backup Protection

Primary protection systems may fail for any number of reasons - equipment malfunctions and inadequate or improper maintenance are fairly common [5]. As such, backup protection systems are a necessity. Backup protection comes in two primary forms: local and remote.

Local backup protection is generally accomplished by redundant devices, usually

installed in parallel, such that if either or both devices operate correctly, the system will exhibit the correct response. This is the most effective form of backup as it generally involves no time delay in its response and isolates the smallest portion of the power grid necessary to clear the fault. That being said, there is a high locality element to events that result in real world faults. For example, if a substation that houses a power transmission bus is subject to a natural disaster, such as flooding or a tornado, it is likely that all systems at that location, primary and backup, will be destroyed or fail to operate. Hence the need for a backup located in a geographically separate location; i.e. remote backup protection.

Remote backup protection generally takes the form of remote monitoring or overlapping distance protection zones on neighboring lines. As damage to equipment caused by high fault currents can spread very rapidly through the power transmission system, remote monitoring is of little use outside of providing situational awareness and limited response to worst case scenarios which require entire regions of the grid to be isolated. That leaves overlapping zones as the more effective form of remote backup. The most common form of remote backup has already been described in the discussion of zone 2 distance relays. In the event of a fault at location P_2 (Figure 1), if the zone 1 relay located at IED03 fails to open its circuit breaker and clear the fault within the prescribed 0.2-0.3 second delay, then the zone 2 relay located at IED01 will open its circuit breaker and clear the fault. Likewise, an additional zone 3 relay can be installed in each IED with an even greater reach and longer delay timer, providing additional backup for faults even further away. This type of remote backup protection has a few notable disadvantages. The first of these is that the area affected when remote backup clears the fault is much larger; at a minimum, one more line than necessary is isolated from the grid. Additionally, the delayed response can result in extensive damage given that the high fault currents can rapidly overheat equipment.

Finally, using zone 3 impedance relays may be ineffective if the topography of the grid is not conducive to establishing a useful Z_r [13].

2.5 Wide-Area Backup Protection

Numerous alternatives to existing BP systems have been proposed [1, 23]. The increased reliability and availability of wide-area communications networks enable geographically separate components to share information quickly enough to respond to power transmission systems faults [9]. These hypothetical systems that rely on wide-area communications systems are referred to as Wide-Area Backup Protection (WABP) systems [10]. There are two basic communication models, peer-to-peer and centralized hub. The centralized hub is basically an extension of existing monitoring systems and suffers from marginally acceptable latency and multiple single point of failure risks. Combining peer-to-peer communication with autonomous local agents that employ artificial intelligence techniques results in a fast and redundant WABP system. Various artificial intelligence techniques have been tested including neural nets [7], Bayesian networks [46, 8], Petri nets [11, 37], and expert systems [38]. The WABP system selected for this experiment utilizes peer-to-peer communication between expert system agents. The agents' communication is limited to predefined regions to increase speed and reduce computational complexity. For the rest of this paper it will be referred to as the test WABP system.

Existing research has focused primarily on developing the expert systems and communications architecture required to achieve the desired results. Published case studies are generally limited to very small novel cases accounting for only a few possible scenarios that an implemented system would encounter. It is generally accepted that these agent-based WABP systems provide increased system resilience through redundancy; this has also been shown in numerous limited case studies. However,

rarely is there an attempt to quantify the resiliency of these systems in a larger scale implementation. This experiment provides a basic quantification of the resiliency of the test WABP system.

2.6 The Test WABP System

The test WABP system, designed by Tong et al., consists of three components; IEDs, Line Decision Agents (LDAs), and Regional Decision Agents (RDAs). Each IED has a corresponding LDA and each bus has a single RDA. The RDA manages communication between the local (on the same bus) LDAs and IEDs. Each RDA is connected to a wide area network (WAN) to facilitate communicating with other RDAs.

When a relay activates, the corresponding IED may or may not send a signal to trip a breaker according to the primary protection scheme. Either way, the IED will send a message to the local RDA indicating the current state of all its relays. The RDA will then activate the corresponding LDA and pass it a message containing the state of the relays in the IED. Additionally, the RDA will send a message to the RDA at the far side bus to ensure that the far side LDA is activated even in the event of failures in the far side IED.

The LDAs perform most of the logic in the BP system. Once activated, the LDAs that share a line will coordinate, through the RDAs, to determine the perceived state of the line. The possible perceived states are Normal, Special, Suspect, or Faulted. If the line is determined to be in the Normal state, a message is sent to a higher authority indicating the possible presence of faulty equipment. If the line is determined to be in the Special state, then directional protection information is collected from all neighboring lines; that is lines that share a bus with the line in question. Neighboring direction protection information is used to either downgrade

the state to Normal or upgrade the state to Suspect. If the line is determined to be in the Suspect state, then detailed line and relay state information is collected from all neighboring lines and the state of the line is downgraded to Normal or upgraded to Faulted, according to expert rules. If the line is determined to be in the Faulted state, protection actions are taken to clear the fault. Any time the perceived state of the line changes, the actions corresponding to that state are taken.

2.7 Model Checking

The application of model verification techniques to power systems is not new, Petri nets [42, 31, 24] and model-checking have been used in the past [20, 28, 27]. Petri nets are a mathematical modeling language used for the description of distributed systems [29]. Basic Petri nets that model simple systems are easy to construct and trivial to verify. Modeling more complex systems requires the use of extensions such as colored Petri nets [40], which are significantly more complicated to employ along with being more powerful. The complexity of these verification techniques makes their use difficult and time consuming. Model-checking has many advantages over other approaches to BP system verification. Although the end goal is the same, the process is considerably more automated. Rather than verifying the results using formal methods applied to symbolic statements, the model-checker iteratively verifies the results in a brute force manner [3, 16]. Additionally, many model checkers utilize a descriptive language that is similar to programming languages [17]. The ability to utilize familiar programming constructs, such as data structures, conditional branching statements, and loops, make these descriptive models easier to comprehend than intricate graph-based Petri net models.

Many different model-checking tools exist and each has its own set of appropriate verification tasks [35, 6]. For example, software engineers at Amazon apply the model

checker TLA+ to the complex distributed systems that underlie their Amazon Web Services [30]. The model-checker SPIN has been used successfully in a number of real world applications, such as, the Mars Exploration Rovers and Deep Impact, in a vehicle malfunction investigation involving the 2005 Toyota Camry, and in the verification of medical device transmission protocols [34, 14, 44]. SPIN has also been applied to verify the fault-tolerance of other types of distributed software systems [4, 26].

2.8 SPIN Background

SPIN belongs to a class of software tools called model checkers which are a subset of hardware and software verification techniques known as formal methods - the applied mathematics of design verification [32]. The Federal Aviation Authority (FAA), which has experience investigating the causes of catastrophic software failures in aircraft, recommends, "Formal methods should be part of the education of every computer scientist and software engineer, just as the appropriate branch of applied mathematics is a necessary part of the education of all other engineers". Model checking is a verification technique coined by Clarke and Emerson in the 1980's that uses optimized algorithms and tailored data structures to efficiently explore all possible system states in a brute-force manner. The theoretical and mathematical foundations of model checking are finite automata theory and linear temporal logic.

All model checkers have strengths and weaknesses. Within the scope of this experiment, SPIN has many strengths: it is free and open source, it is very well documented, it is a mature software product, it is under active development as of 2017, the syntax of its PROMELA programming language (a contraction of Process MetaLanguage) is C-based and familiar, and SPIN has several added-on features to ease model creation (e.g. a graphical user interface and support for auto-generating models from source

code).

SPIN was originally an acronym for Simple PROMELA Interpreter, but has now become a stand-alone term. Because SPIN is intended to model concurrent systems, PROMELA has built-in support for modeling nondeterministic behavior. PROMELA is technically not a programming language like C or Java, but a systems description language targeted to the descriptions of concurrent software systems. It was designed to help the programmer think in terms of the functions of a distributed system, and it makes it easy to capture common constructs like message passing, shared memory, nondeterministic behavior, and the atomic execution of instruction sequences.

Nondeterministic behavior is achieved in SPIN through the use of guard statements. These guard statements are conditions which must be met for their particular branch of the model to be taken. For example, an IF statement in PROMELA can contain any number of guard statements and execution of the model may proceed along any of the options whose guard condition evaluates to true.

SPIN has two modes of operation; verification and simulation. The primary mode is verification, which compiles a standalone program in C from the PROMELA model (conventionally called pan which is short for protocol analyzer). The compiled program will search the possible states that the model can reach and attempt identify a path that leads to an error that violates one of the predefined operating parameters. If a path to an error is identified, it is stored in an encoded trail file. When compiling the pan, there are a number of options available for setting the techniques used to search the state-space of the model. These options determine the run time, memory usage, and exhaustiveness of the search. By default, the program halts when the first error is found; however, there is an option that allows for the generation of all paths that lead to errors.

Simulation mode can be used one of two ways. The first requires a trail file to

be input along with the PROMELA model. SPIN will then decode the trail file and output the details of the path that leads to the error. If a trail file is not provided, simulation mode will choose a path at random and follow it until an error is reached or the end of the model. This mode is very useful for debugging new models.

2.9 Chapter Summary

The protective relays are the basic building blocks of both primary and backup protection systems and provide detailed information about the state of the line to the IED. The ability to share information between IEDs through high-speed wide-area communications networks has the potential to reduce the number of cascading failures in power distribution systems. Coupling this with distributed agents using artificial intelligence can enable WABP systems to respond to very complex failure scenarios. While the use of distributed agents clearly increases the redundancy of the BP system, the system complexity makes it difficult to determine the potential gains in resiliency. Model checking can provide the tools necessary to model the redundancy in a WABP system and determine its impact to resiliency.

III. Methodology

This chapter provides a detailed description of the evaluation tools and techniques used in the experiment. It presents the system to be modeled, including decisions made in the design process as well as limitations and assumptions. Finally, the model-checking tests employed are covered.

3.1 Objective

The intent of this research was to evaluate the resilience of the test WABP system as applied to the IEEE 14-bus system. This research builds on the previous research of [15] and expands the evaluation from the localized area of a single line (Line 15) to all lines in the 14-bus system. The first step in the evaluation was to determine if the previously identified level of resiliency held when the test WABP system was modeled on a larger system. Next, relationships between failure patterns and transmission grid topography were identified. Finally, recommendations for improved resiliency were developed.

3.2 Design Decisions and Constraints

Many of the design decisions were made in the research that this experiment expands upon [15]. The power transmission topography selected is one of the smaller examples of standardized grids used for modeling and simulation. The limitations and assumptions largely mirror those made in the previous study, whether or not they were explicitly stated therein. The model checker utilizes a descriptive language that is similar to C in many ways.

3.3 Transmission Grid Model

It is a bit of a misnomer to reference the model of the transmission grid, as the grid is not actually modeled, rather the responses of a hypothetical grid are simulated. However, the topography of the simulated grid dictates the arrangement and relationship of the components of the test WABP system. The IEEE 14-Bus system consists of 14 buses, 17 transmission lines, and 5 generators located in 10 substations (Figure 2). The model topography condenses the buses and lines contained within

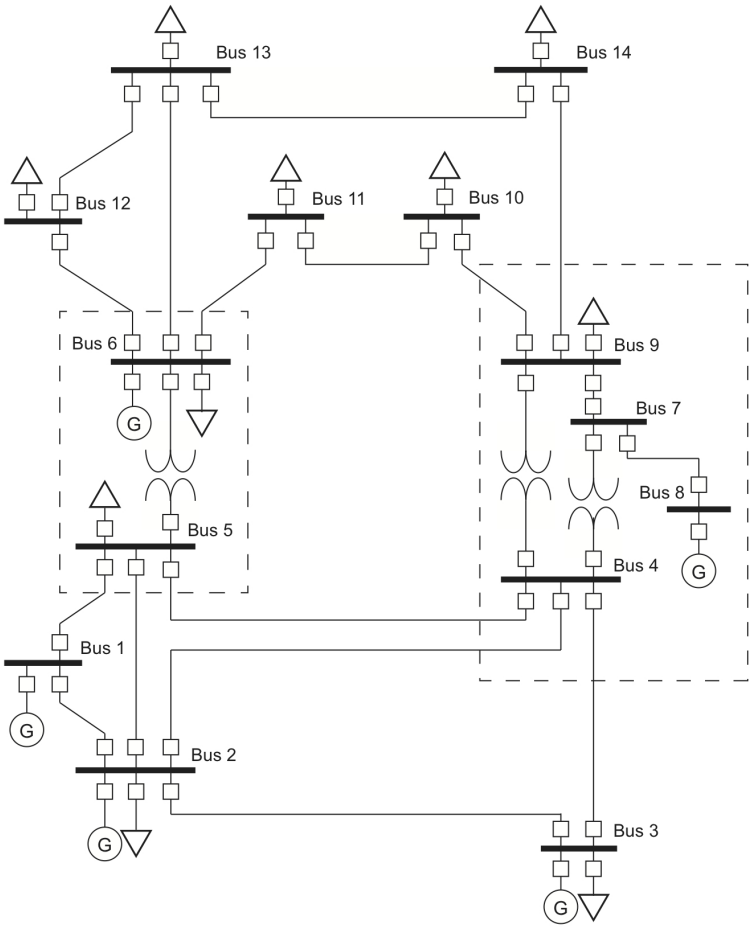

Figure 2. IEEE 14-Bus System

each substation and treats them logically as a single bus [12]. This representation of the system has 10 buses and 15 lines 3. Each line is monitored by a pair of Intelligent

Electronic Devices (IEDs), one on each end of the line where the line connects to the bus. Each of these IEDs contains three relays: a directional overcurrent relay, Zone 1

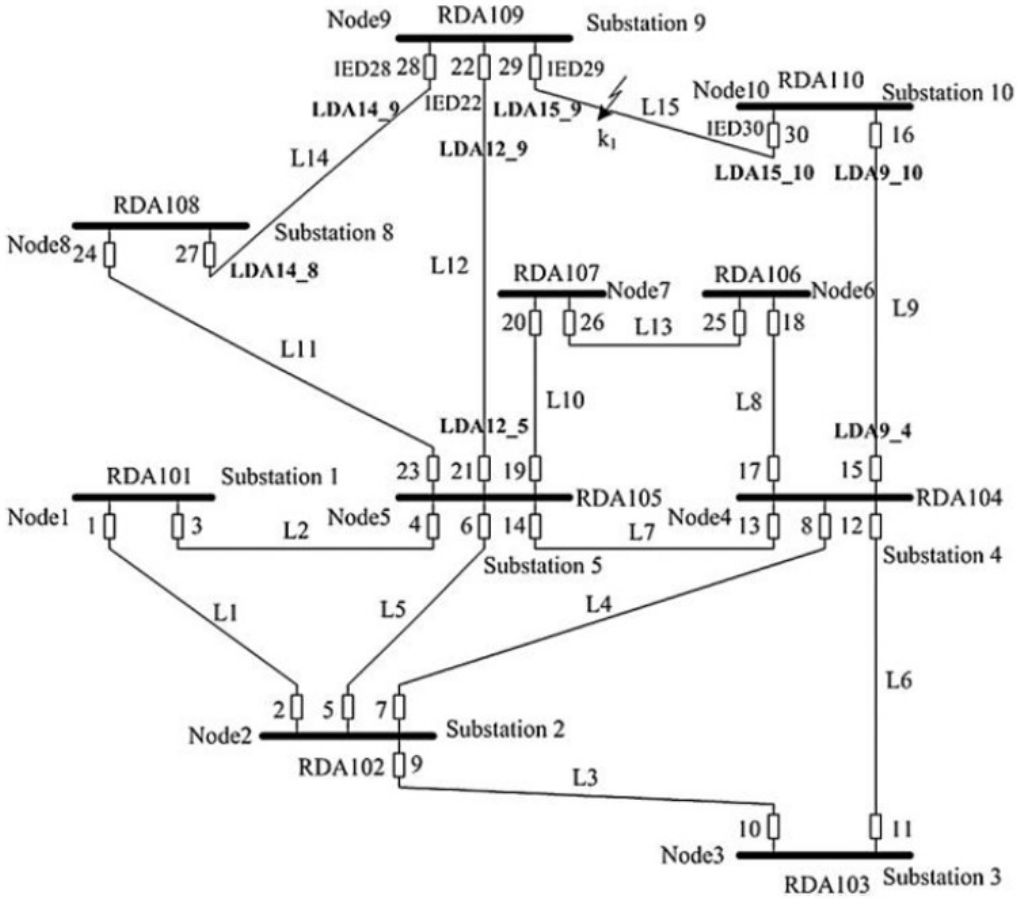

Figure 3. WABPS Modified IEEE 14-Bus System [41]

distance relay, and Zone 2 distance relay. The directional relay indicates the direction of the fault relative to the IED (bus side or line side). Both Zone relays are distance relays that observe line impedance. This paper will refer to their settings in length rather than impedance, given that line impedance is largely a function of line length [13]. The Zone 1 relay is set to respond to faults on the closest 80% of the line. The Zone 2 relay is set to detect faults on the entire length of the line plus 20% of the length of the shortest other line connected to the far side bus.

3.4 Test WABP System Model

The test WABP system is modeled as a system of codependent processes that pass messages via dedicated message buffers. In a physical implementation two separate LDAs are located on either end of each line.

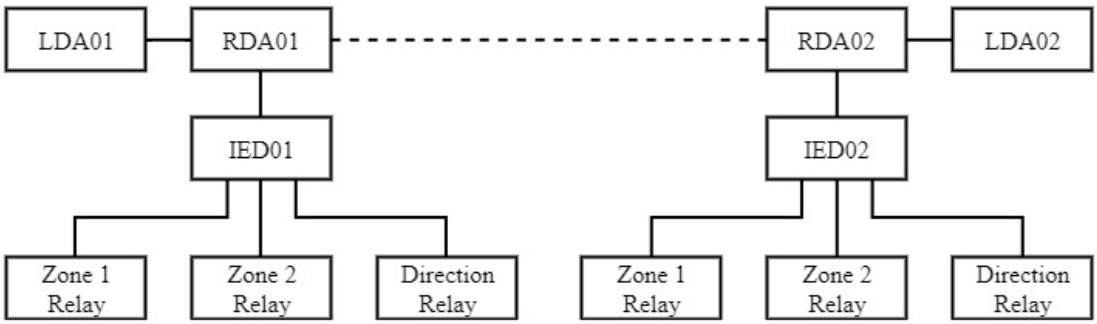

Figure 4. WABPS Physical Implementation

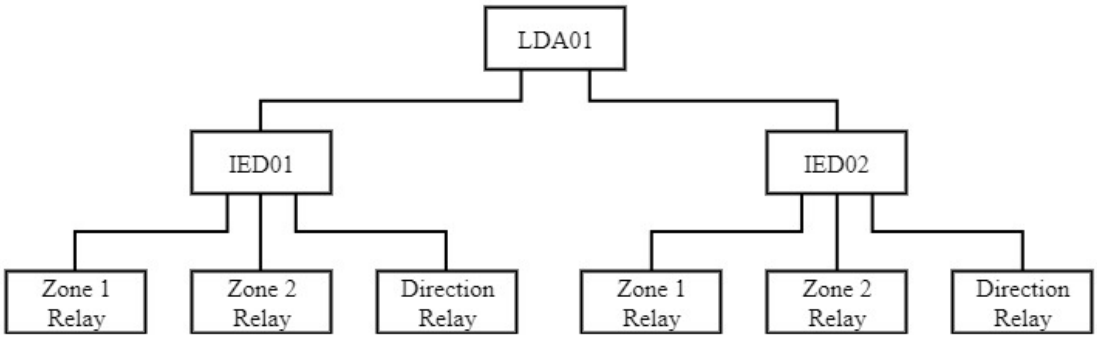

Figure 5. WABPS Model Implementation

In the model, the two LDAs on each line are treated as a single process - a combined LDA. This eliminates the need to explicitly model the message passing between the two LDAs. This does not have an impact on the results obtained. A message from one LDA not being able to reach the far side LDA is logically equivalent to a set of components in the combined LDA failing to provide a reading. Likewise, a

message being corrupted in transit is logically equivalent to a set of components in the combined LDA providing a faulty reading. As a result, the RDAs are completely obfuscated from the model. In the diagram of the physical implementation, if communication between the two RDAs is broken, the LDAs have the information shown in Table 1 available to make a control decision. This is logically the same as the combined LDA in the model responding to any of the three combinations shown in Table 3.

Table 1. Communication Failure in Physical Implementation

LDA01		**LDA02**	
IED01		IED01	
- Zone 1	FAULT	- Zone 1	NO_DATA
- Zone 2	FAULT	- Zone 2	NO_DATA
- Direction	LINE	- Direction	NO_DATA
IED02		IED02	
- Zone 1	NO_DATA	- Zone 1	FAULT
- Zone 2	NO_DATA	- Zone 2	FAULT
- Direction	NO_DATA	- Direction	LINE

Table 2. Communication Failure Modeled

LDA01		**LDA01**		**LDA01**	
IED01		IED01		IED01	
- Zone 1	FAULT	- Zone 1	NO_DATA	- Zone 1	NO_DATA
- Zone 2	FAULT	- Zone 2	NO_DATA	- Zone 2	NO_DATA
- Direction	LINE	- Direction	NO_DATA	- Direction	NO_DATA
IED02		IED02		IED02	
- Zone 1	NO_DATA	- Zone 1	FAULT	- Zone 1	NO_DATA
- Zone 2	NO_DATA	- Zone 2	FAULT	- Zone 2	NO_DATA
- Direction	NO_DATA	- Direction	LINE	- Direction	NO_DATA

The test WABP systems exact responses to the two inputs are not the same; however, all result in a failure of the test WABP system to correctly identify the faulted line. To exactly model the response of the test WABP system, the LDAs

would need to be modeled separately. This would increase the complexity of the model but would enable more accurate evaluation of the type of failure, strong or weak, and the scope of the impact to the system, which would be the number of other lines isolated.

3.5 Limitations

The model does not account for back reach from zone distance relays. Given that distance relays are not directional, faults may fall within the reach of zone distance relays of IEDs on neighboring lines that share the same bus, even though they are bus side faults relative to these neighboring line IEDs. This is a function of obfuscating the length of the lines and the impedance of the buses in the model. The closer the fault is to a bus, the more likely it is that the fault will be within reach of the zone distance relays in other IEDs on that bus. However, without including line length and bus impedance in the model, there is no way to determine how far the backward reach extends along neighboring lines. Due to the large reference impedances for zone distance relays on long lines, faults even at the far end of shorter lines that share a bus would fall within the reach of the Zone 1 distance relay of the longer line. In the example below, any fault occurring in the purple shaded region would cause the Zone 1 distance relay in IED03 to activate.

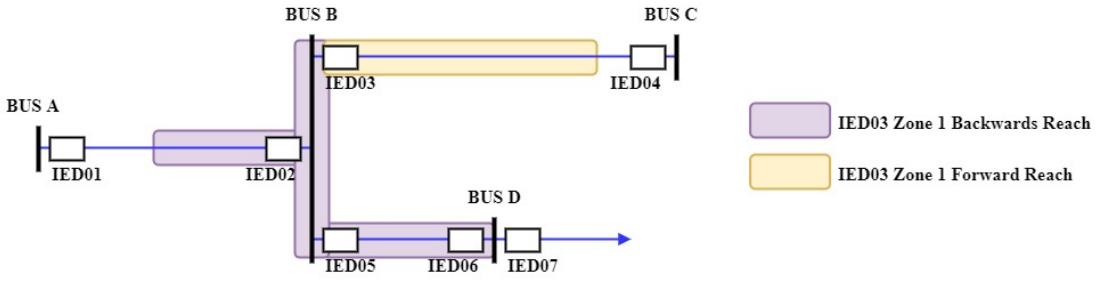

Figure 6. Back Reach of Zone Distance Relays

3.6 Assumptions

All faults are assumed to occur within the reach of the Zone 1 distance relays at both ends of the line. It would be possible to evaluate the system by adding fault profiles for faults at either end of the line; however, that would triple the number of fault profiles to be evaluated.

All faults are assumed to occur outside the reach of all neighboring Zone 2 distance relays. It is not possible to evaluate the response of the BP system to faults falling within the reach of neighboring Zone 2 distance relays without defining how far each neighboring Zone 2 region extends along a given line. Then a separate fault profile would need to be created for each combination of overlapping Zone 2 regions on each line. This would result in additional fault profiles equal to the average number of neighboring lines times the number of lines. In this case, that would be 30 more fault profiles. This number would increase exponentially if neighboring Zone 2 distance and Zone 1 and Zone 2 backward reach are included in the model.

Theoretically, the fault is detectable from every direction overcurrent relay in the entire system. However, the farther from the fault, the smaller the fault signal; therefore, at some distance the magnitude of the fault signal will be so small as to fall within normal operating range and will not cause the relay to respond. These relays are designed and intended to detect faults at most two buses away so there is not any data on exactly how far the effective range of the direction relay extends. It is assumed that every direction relay in the system will respond to all faults in the system.

3.7 Verification Design

The model is initialized to the expected state of the system immediately following a fault on one of the lines. Then, a predefined number of relay inputs are nondeter-

ministically selected and modified to an incorrect value. The processes representing the LDAs are started and execute the BP system control logic and return a verdict about the state of each of the lines. Finally, the verdicts are compared to the truth values to determine whether or not the system arrived at the correct verdict for each line.

There are four possible inputs for the overcurrent direction relays and three for the zone distance relays, Table 3. An incorrect reading other than no data simulates the impact of faulty equipment, or corrupted messages, either from transmission error or a malicious entity operating in the system. The no data reading simulates faulty equipment or a loss of communication between components in the BP system.

Table 3. Possible Relay States

Directional Relay States	
BUS	Bus Side Fault Detected
LINE	Line Side Fault Detected
NO_FAULT	No Fault Detected
NO_DATA	No Data Received/State Unknown

Zone Relay States	
FAULT	Fault Detected Within Zone
NO_FAULT	No Fault Detected
NO_DATA	No Data Received/State Unknown

SPIN was run in verification mode to ensure that all conditions that result in system failure were identified. Faults on each line are tested separately. It is possible to create a single large model that produces all of the results for faults on all of the lines in a single verification run. However, this model is very large and the verification time and memory usage are prohibitive. Therefore, a separate model for each line was created, the only difference between these models are the initialization states and the line verdict that is checked for strong correctness. Verification is accomplished for up to four component malfunctions and up to four complete IED malfunctions, with

a total of at most four malfunctions. All combinations that result in system failure are recorded in separate trace files.

Two types of failure are tested for: strong correctness and weak correctness. The system fails the strong correctness test if the BP system verdict is not correct for every line. The system fails the weak correctness test if the BP system verdict is not correct for the faulted line. Therefore, all weak correctness failures are strong correctness failures. In the event that the BP system verdict is that multiple lines are faulted, as long as the correct faulted line is included, the system is considered to be weakly correct. In real world application, weakly correct responses are acceptable in some cases as they do clear the fault, even if not in the least impactful manner.

Previous experiments did not verify that the results were unique. The model is designed such that each component is selected individually for malfunction testing. Duplicate results occur because SPIN differentiates between traces based on the line of the model (PROMELA assert statement) that resulted in the system failure. All verifications terminate when the first assert statement is violated. For example, say during a verification of two component malfunctions combinations that the selection of IED01 and IED02 results in a violation of assert statement A. Verification will then continue to see if any other violations can be reached from this selection of malfunctions. If there is some other assert statement B that is violated by this combination of malfunctions, then a separate trail file is produced for the section combination. This results in some combinations appearing in multiple trail files causing the failure count appear larger than it actually is.

3.8 Chapter Summary

The purpose of this research was to evaluate the ability of the test WABP system to operate in the presence of component malfunctions. Given the complexity of power

transmission systems and need to utilize existing components to reduce cost, model checking was used to evaluate the combinatorically large number of possible malfunctions. This approach required the development of a model capable of exhibiting the desired behaviors while remaining small enough to run in polynomial time. Once completed, the model enabled evaluation of the test WABP systems design as well as identifying questions that will need to be answered prior to implementation.

IV. Results and Analysis

Table 4. Example of Results

Line15

Total IED	Single Relay 0	1	2	3	4
0	0	28	7610	564408	552590
1	4	1778	377441	94593	140691
2	101	41035	96163	116327	169401
3	1206	101051	112526	144753	-
4	12352	95736	109910	-	-

*search not completed for results > 10000

The full set of tabulated results can be found in the appendix. These results represent the number of distinct system failures that result from each of the tested combinations of single component and total IED malfunctions. All results have been verified to ensure that there are no redundant combinations of malfunctions (see section 3.7). There is overlap in the results - if a set of malfunctions, A, results in a misdiagnosis, then any set, B, such that $A \subset B$, will also result in a misdiagnosis. Additionally, weak correctness errors are a subset of strong correctness errors. Weak correctness errors fail to correctly diagnose the state of the faulted line, and strong correctness errors fail to correctly diagnose the state of all lines. Therefore, if at least one line diagnosis is incorrect then the test for strong correctness fails.

4.1 Analysis

It is useful to differentiate between incorrect reading malfunctions and no-data malfunctions. Incorrect reading malfunctions are those that result in the component returning a value that is valid, but incorrect. No data malfunctions are all malfunctions that result in the component either not responding or responding with an invalid

reading, as could be caused by a communication failure.

The sets of component malfunctions that lead to a WABP failure can be divided into three categories. Category 1 failures result in an unfaulted line being misdiagnosed, Category 2 failures result in the faulted line being misdiagnosed, and Category 3 failures result in the faulted line and one unfaulted line that share a bus both being misdiagnosed. These sets of component malfunctions are predominantly independent; however, that does not prevent failures from multiple categories affecting the system at the same time. Many lines may be misdiagnosed in the same incident, but this analysis shows that each misdiagnosed line can be traced back to a specific set of component malfunctions that fall into one of the three categories.

Category 1 Failures.

There are two conditions that lead to a Category 1 failure. The first is simply for the integrated fault value (F_{out}) for the line to be greater than the threshold (F_{set}) for that line. The second requires that the line enter a Suspect state as well as not sharing a bus with a line that the WABP system has diagnosed as Faulted. There are separate sets of malfunctions that can lead to each of these two conditions, some sets require more malfunctions than others, but all follow specific patterns. With x as the faulted line and y as any shared bus line:

Condition 1: $F_{out}(x) > 1$

Condition 2: $(0 \leq F_{out}(x) \leq 1) \quad \& \quad (F_{out}(x) > F_{out}(y)) \quad \text{for all} \quad y$

The F_{out} for a line is calculated by summing the action factors (AF) for each LDA on the line. The possible AF values are 1, 0.5, -1, and 0 (Table 5) and the F_{out} threshold is 1 for all lines in this experiment.

To simulate a line fault scenario, the LDAs of all unfaulted lines in the system are

Table 5. AF **Calculation**

AF	Directional Relay	Zone 1 Relay	Zone 2 Relay
1	LINE	FAULT	ANY
0.5	LINE	NO_FAULT	FAULT
-1	BUS	NO_FAULT	NO_FAULT
0	All Other Combinations		

initialized to the starting configuration for an unfaulted line (Table 6).

Table 6. Starting Configuration for IEDs on an Unfaulted Line

IED A		**IED B**	
- Zone 1	NO_FAULT	- Zone 1	NO_FAULT
- Zone 2	NO_FAULT	- Zone 2	NO_FAULT
- Direction	LINE	- Direction	BUS

In the starting configuration for an unfaulted line, the AF value for IED A is 0 and the AF value for IED B is -1. This results in a F_{out} value of -1. It takes a minimum of three component malfunctions to reach an F_{out} value greater than 1 when starting from this configuration. However, any three component malfunctions will not produce this condition. Two specific malfunctions must occur in addition to one of two other malfunctions. The two malfunctions that must occur are: the IED A Zone 1 distance relay must read a fault condition and the IED B directional overcurrent relay must indicate a line side fault. In addition, either the IED B Zone 1 or Zone 2 distance relay must read a fault condition. The presence of these malfunctions would cause the AF for IED A to be 1 and the AF for IED B to be 1 or 0.5, depending on whether or not the Zone 1 or Zone 2 distance relay malfunctioned, respectively. These conditions are not only sufficient for this condition, they are also necessary. Any set of four or more component malfunctions must have three component malfunctions in this configuration to result in this condition. Furthermore, no number of complete IED failures can lead to this condition. This is a result of the fact that all complete

IED failures are treated as a set of three no-data malfunctions. No-data malfunctions specific incorrect reading malfunctions are required for this condition.

For a line to enter the Suspect state in the WABP system, the F_{out} value of the line in question must be greater than or equal to 0 and less than F_{set}, which is 1 for all lines in this experiment. To resolve a Suspect state, the LDAs will query all neighboring lines, that is all lines that they share a bus with. If one of these neighboring lines has been diagnosed by the system as Faulted, then the line in question will be downgraded to the Normal state. If all of the neighboring lines have been diagnosed as Normal, then the line in question will be upgraded to the Faulted state. In the event that multiple lines that share a bus are in the Suspect state, the line with the highest F_{out} will be upgraded to the Faulted state and the rest downgraded to Normal. If there are two Suspect lines with the same F_{out}, the line with more zone distance relays reading fault will be the one upgraded to the Faulted state and the other downgraded to Normal.

Again, we begin the analysis with the starting configuration for an unfaulted line, with $AF(A) = 0$, $AF(B) = -1$, and a $F_{out} = -1$. There are 10 separate single-component malfunctions and one complete IED failure (IED B) that will result in a F_{out} of 0 and place the line in a Suspect state. After one of these malfunctions, the LDAs will query their neighbors to resolve the Suspect state. This is where the second criteria for this condition comes into play. If the line in question does not share a bus with the faulted line, the WABP system will incorrectly diagnose it as Faulted. These criteria are sufficient for this condition but are not necessary. There are a large number of sets of multiple malfunctions that result in a line entering the Suspect state. That is why the state was included in the WABP system - to resolve a large number of possible malfunctions. The only criteria that is necessary for this condition is that the line in question not share a bus with a line that has been diagnosed as

Faulted.

The second condition that can lead to a Category 1 failure has not been addressed in previous studies as their example simulations do not evaluate malfunctions on lines that do not neighbor the faulted line. The real-world implications of this behavior may be negligible because the model does not account for generator locations. Directional overcurrent relays indicate the direction the current is flowing and fault current always flows from source to ground. Therefore, to meet the criteria for this condition, the line in question would have to reside between the generator and the fault along the path of least impedance. Determining the possibility of transmission system having a line that could meet all of these criteria would require further research.

Category 2 Failure.

There is only one condition that results in a Category 2 failure and it requires that the F_{out} of the faulted line to be less than 0.

$$\text{Condition: } F_{out}(x) < 0$$

To simulate the fault scenario, the faulted line in the system is initialized to the starting configuration for a faulted line (Table 7). There are only a few sets of malfunctions that can lead to this failure condition and they all follow a very specific pattern. All four zone distance relays must malfunction and read no fault and both directional overcurrent relays must malfunction and indicate a bus side fault or indicate no fault. That means that the minimum number of malfunctions for this condition is six, any fewer and the line would enter the Suspect state and the fault would be correctly diagnosed when the Suspect state is resolved. As there are only six components between the two LDAs, all of them must malfunction for a Category 2 failure to occur.

Table 7. Starting Configuration for IEDs on a Faulted Line

IED A		IED B	
- Zone 1	FAULT	- Zone 1	FAULT
- Zone 2	FAULT	- Zone 2	FAULT
- Direction	LINE	- Direction	LINE

Category 3 Failures.

There are two conditions that result in a Category 3 failure. These conditions are a combination of conditions that we have already seen. Both conditions require that the F_{out} of the faulted line be greater than or equal to 0 and less than or equal to 1. For the first condition, the F_{out} of the faulted line must be less than the F_{out} of at least one other shared bus line. The second condition requires that the F_{out} of the faulted line be equal to a shared bus line, and said shared bus line must have more zone distance relays indicating a fault condition that the faulted line.

Condition 1: $(0 \leq F_{out}(x) \leq 1) \quad \& \quad (F_{out}(x) < F_{out}(y))$

Condition 2: $(0 \leq F_{out}(x) \leq 1) \quad \& \quad (F_{out}(x) = F_{out}(y)) \quad \& \quad (P_a(x) < P_a(y))$

Where x is the faulted line and y is a neighboring line that shares a bus with x, and $P_a(i)$ is the number of zone distance relays on line i that read a fault.

Table 8. Starting Configuration for the IEDs on Line x

IED A		IED B	
- Zone 1	FAULT	- Zone 1	FAULT
- Zone 2	FAULT	- Zone 2	FAULT
- Direction	LINE	- Direction	LINE

For analysis, line x, the faulted line, is initialized to the starting configuration of a faulted line (Table 8) and line y, the neighboring unfaulted line, is initialized to the starting configuration of an unfaulted line (Table 9). The first requirement for both

Table 9. Starting Configuration for the IEDs on Line y

IED A		**IED B**	
- Zone 1	NO_FAULT	- Zone 1	NO_FAULT
- Zone 2	NO_FAULT	- Zone 2	NO_FAULT
- Direction	LINE	- Direction	BUS

criteria is that the faulted lines F_{out} be reduced. There are many sets of malfunctions that can meet this requirement. At a minimum, one relay in each IED on line x must malfunction, with the malfunctions being either the in the directional overcurrent or zone distance relays.

The set of malfunctions that will achieve the second requirement for the first condition is dependent on the F_{out} for line x, but all of these malfunctions affect components on line y. If $F_{out}(x) = 0$ then $F_{out}(y) = 0.5$ will meet the requirement and this can be accomplished by two incorrect data malfunctions in IED02 (direction and zone 2), or by one incorrect data malfunction on either of the IED01 zone distance relays in combination with any malfunction on the IED02 distance overcurrent relay. The malfunctions required to meet the requirement when $F_{out}(x) = 1$ follow a similar pattern, but a third incorrect data malfunction is required. This brings the total number of malfunctions required to meet the first condition up to four malfunctions.

The set of malfunctions that meet the second and third requirements for the second condition is very specific and rather large in comparison to the other malfunction sets discussed in this paper. Meeting the second requirement is very similar to meeting the second requirement for the first condition and still requires at least two malfunctions, only with fewer possible combinations of malfunctions. The third requirement is very simple; at least two zone distance relays on line y must have an incorrect data malfunction and at least two zone distance relays on line x must have any malfunction. This brings the total number of malfunctions required to meet the second condition up to eight malfunctions.

4.2 Implications

Up to this point, the analysis has been focused on the patterns and number of malfunctions that lead to system failure. In this section the impact of these failures and the likelihood of their respective malfunction patterns is addressed. First, the concepts of strong and weak correctness, discussed in section 3.7, will be combined with the failure categories.

BP systems that are expected to pass the weak correctness test, that is they isolate at least the faulted line, are the current industry standard. In the event that primary protection and local backups fail, the outage will encompass more than just the faulted line. When only accounting for weak correctness test failures, the WABP system is quite resilient. For the test WABP system to fail the weak correctness test, it must experience a Category 2 or Category 3 failure. Every condition in these two categories requires four or more malfunctions, with two or more of them being incorrect data malfunctions. These malfunctions would all also result in an otherwise properly functioning primary protection system failing to isolate the fault. Therefore, an implementation of this system would not introduce any new responses that could result in failing the weak correctness test.

The number of WABP system strong correctness failures is more disparaging at first glance. To put them in context requires reintroducing some of the factors that were obfuscated from the mode. All strong correctness failures with fewer than four combined malfunctions (single component and complete IED) fall in the second condition for a Category 1 failure. In the current model, the directional overcurrent relays will always wake all the LDAs in the system. Additionally, all lines in the system that are not faulted will have the direction relay on one side indicating a line side fault and the other will indicate a bus side fault. In the event that the relay that should be reading a bus side fault provides an incorrect reading (reads a line side fault) or fails

to respond (no-data), then that line will be placed in a Suspect state. Likewise, if the IED that is reading a line side fault has a Zone 1 distance relay incorrect reading malfunction, the line will be placed in the Suspect state. In a real-world implementation, the directional overcurrent relay indicates the direction of current - which is always from source to drain. In this case, the drain would be the faulted line and the source would be a generator. Furthermore, the directional overcurrent relay would not sense the fault current unless it was on the path of the fault current - which is the path of least impedance from source to drain. That means that the only way for failures of this type to occur would be for the malfunctions to occur on a line that is both on the path of the faulted current and have an unfaulted line separating it from the faulted line. To determine the path of the fault current would require adding the generators to the model as well as including the impedance for all the components in the transmission grid. This is possible as all of the necessary data is provided in the documentation for the IEEE-14 bus system but would greatly increase the complexity of model generation. Further research is required to determine if useful data could be obtained from a more complex model.

This experiment did not evaluate the scope of the faults. Some weak correctness failures have a greater negative impact than others. For example, diagnosing every line in the transmission grid would meet the criteria for weak correctness, however, this is a very undesirable behavior. A better understanding of the performance of the test WABP system could be obtained by evaluating the number of misdiagnosed unfaulted lines in the weakly correct cases. Unfortunately, there is no way to measure outage scope directly with SPIN. The verification terminates as soon as a single line is found to be incorrectly diagnosed. It would be possible to include additional print statements in the PROMELA model that could then be evaluated. Then the plaintext output from the verification runs that fail the strong correctness test but pass weak

correctness could be evaluated to determine the scope of the outage.

The data collected includes the test case when there is not a fault on any of the lines. It is interesting to note that the number and type of failures for each test configuration match those that include a faulted line. Thus, the results collected indicate that the WABP system is no more or less likely to fail regardless of the presence of a line fault or not.

There is one final item of note that was observed in the analysis of the collected data. The use of the certification factor (CF) has not been directly addressed in order to try and reduce the complexity of the analysis presented above. In the absence of generator locations and known impedances, the distance from the IED to the fault was used to determine the starting configuration of the directional overcurrent relays. This resulted in a CF greater than or equal to 0.5 for more than 65% of the LDAs in the system, regardless of the location of the fault. It is interesting to note that this resulted in lines 02, 05, 07, 09, 10, 11, and 12 having no failures with only one component malfunction. This resulted in most of the lines with a F_{out} equal to one being elevated to the Suspect state. There were few sets of malfunctions that resulted in a F_{out} equal to 1, and all of them required more malfunctions than those sets that resulted in a F_{out} less than one. As such, the existence of the CF had very little impact on the observed system response. Not to say that the CF is not a valuable component of the WABP system logic; however, determining its impact more accurately would require the incorporation of the generators and transmission grid impedances.

4.3 Comparison to Previous Results

The results previously reported by Hamman et. al [cite] for WABP system failures in responding to a line 15 fault vary noticeably from those reported here. These

differences deserve explanation (Table **??**). The addition of a no-data option added a large number of results. In the previous model all malfunctions were assumed to be incorrect readings. Also, the inclusion of every IED in the entire 14-bus system

Table 10. Comparison of Results

		Single Relay							
		0		1		2		3	
		Old	New	Old	New	Old	New	Old	New
Total IED	0	0	0	0	28	0	7610	268	564408
	1	0	4	0	1778	247	37744	-	-
	2	0	101	45	41035	-	-	-	-
	3	6	1206	-	-	-	-	-	-

increased the number of failures that were of the same pattern as those previously reported. That being said when these results are normalized by removing those results that have been shown to be constructs of the model and not representative of the test WABP system all of the new results listed in this table go to zero. The reason for this is that the Zone 2 relays were not included in the previous model, even though they are present in the original WABP system specification [cite]. All of the previously reported failures were Category 3 failures. The inclusion of the Zone 2 relays increased the number of malfunctions necessary for a Category 3 failure from three to four.

4.4 Recommendations

In light of these findings, a number of recommendations can be made. That being said, many of the recommended actions are already employed in in real-world protection systems. The model used in this experiment is based on models used in previous research in order to facilitate the comparison of results. These previous models did not include the components in question and therefore were not included in the model used for this experiment. Incorporating a number of these omitted components is likely to increase the test WABP system's resilience.

First, many protection systems employ local backup relays. Combining these relays in parallel, either logically or physically, helps reduce the likelihood that a single relay malfunction results in a primary protection system failure. If the readings from these local backups could be incorporated in the WABP system logic, it would likely result in greater resilience. For example, if the Zone 1 distance relay local backup were to be incorporated and the AF calculation modified (Table 11), then the minimum number of component malfunctions necessary to cause a failure would increase from four to five. And this is probably not the best possible employment of the Zone 1 backup, though it still increases system resilience.

Table 11. Hypothetical *AF* Calculation

AF	**Directional Relay**	**Zone 1 Relay**	**Zone 1 Backup**	**Zone 2 Relay**
1	LINE	FAULT	FAULT	ANY
0.5	LINE	FAULT	NO_FAULT	ANY
0.5	LINE	NO_FAULT	FAULT	ANY
0.5	LINE	NO_FAULT	NO_FAULT	FAULT
-1	BUS	NO_FAULT	NO_FAULT	NO_FAULT
-1	BUS	NO_FAULT	NO_FAULT	NO_FAULT
0	All Other Combinations			

Furthermore, Zone 3 distance relays with an even greater range than Zone 2 relays are not uncommon. As with the Zone 2 backup relay, incorporating Zone 3 relays in the WABP system logic would increase resilience.

Because of the overlap in coverage from Zone 2 and Zone 3 distance relays, it is very likely that a fault on a line would be detected by some number of zone distance relays on neighboring lines. It is possible that incorporating readings from Zone 2 and 3 relays on the distant end of neighboring lines would improve resiliency. Likewise, the back readings from neighboring lines could be added. This can be accomplished by assuming that an IED with a directional overcurrent reading of a bus side fault and Zone 2 reading a fault is an indicator of a fault on a neighboring line.

Based on the results obtained, directional overcurrent relays have a disproportionate impact on the WABP system decision logic. Almost all conditions that lead to failures require at least one directional relay malfunction. This may be a construct of the assumptions made in modeling, namely the absence of generators and impedance values rather than a true characteristic of the test WABP system.

All of these recommendations would increase the complexity of the WABP system logic and likewise increase the resources required to model its response. It may be the case that the added complexity would reduce the response time of the WABP system, which could render it an unviable option. On the other hand, if some of these changes can be incorporated without significant negative impact, it is likely that the systems resilience could be greatly increased. Whether or not the system is resilient enough without modification is outside the scope of this experiment.

V. Conclusion

This chapter provides conclusions from the results of this research. It details how each research objective was accomplished. Additionally, recommendations for future work are presented.

5.1 Conclusions of Research

A high level PROMELA model detailing the application of the logical processes of a novel WABP system to the entire IEEE 14-bus system was created. The model facilitates the evaluation of the WABP system's responses to faults on any of the lines in the system. The number of WABP system component malfunctions can be varied to observe the resiliency of the system. Using the SPIN model checker to verify the model produces detailed output files that were analyzed to determine which sets of malfunctions lead to system failure. These sets of malfunctions were sorted and compared to identify patterns. Three basic patterns of malfunctions were identified as leading to WABP system failure. The malfunction patterns were further analyzed to determine whether they originated from the design of the WABP system or were a result of the modeling assumptions. It was identified that many of the malfunction sets were in fact the result of modeling assumptions. The malfunction patterns that originated from the WABP system's design were studied to determine possible mitigation actions. A number of suggestions were made that may lead to WABP system improvements. When the obtained results were compared to previous findings it was determined that the test WABP system is in fact more resilient to component failures than previously reported.

5.2 Future Work

The future work proposed here falls into two basic categories: improving the model and improving the WABP system. Of the two the improvements to the model have the highest potential for producing valuable results.

Model Improvements.

- Incorporate generators and line impedances. The addition of these components will provide answers to many of the questions raised in the analysis of this research. The most significant of which is the impact of malfunctions on components that are significantly separated from the faulted line. The question of the significance of the CF value in the WABP system algorithm would be answered by this modification as well.

- Determine the scope of strong correctness failures that pass the test for weak correctness. Most BP systems will eventually clear faults in the system but the size of the area affected can vary greatly. It would be useful to evaluate how well a novel WABP system performs when comparing the size of the isolated area in the process of clearing faults.

- Analyze WABP system responses to faults near the ends of lines. All of the faults in this research were assumed to fall within the reach of both of the Zone 1 distance relays on either end of the line. Real world faults are not likely to adhere to this convention. Modifying the initialization of relay readings could help determine if the results reported here compare to different types of faults.

WABP System Improvements.

- Modify Action Factor (AF) calculation to include local backup relays. A simple suggestion for an improved AF calculation is presented in the analysis of the results. This is not a recommendation to use that table, rather an observation that it seems likely that an improved AF calculation could be devised utilizing components that are already commonly incorporated in IEDs.

- Take advantage of the bidirectionality of zone distance relays. In the current WABP system distance relays of shared bus neighbors only indirectly impact the line state verdict. Redesigning the logic to take advantage of them would likely notably increase the system logic but it is another piece of information that is already available.

Appendix: Tabulated Results

*All values over 10,000 were not evaluated for duplicates, values over 50,000 are the count when the verification terminated due to lack of memory.

Line00

Total IED \ Single Relay	0	1	2	3	4
0	0	0	0	36	2047
1	0	0	30	485	0
2	0	0	28	9754	0
3	0	0	378	0	-
4	0	0	3276	-	-

Line01

Total IED \ Single Relay	0	1	2	3	4
0	0	35	8813	50733	56252
1	5	1985	58003	60819	59297
2	105	36364	67901	72013	74263
3	1120	58654	60941	60296	-
4	7960	57514	61354	-	-

Line02

Total IED \ Single Relay	0	1	2	3	4
0	0	0	84	3864	4744
1	0	12	5882	1397	21598
2	0	362	5669	3587	21864
3	5	6266	3082	18427	-
4	112	1447	4314	-	-

Line03

Total IED \ Single Relay	0	1	2	3	4
0	0	21	5912	34667	33447
1	3	1382	41706	40150	37224
2	78	27846	54687	46044	48934
3	967	49131	50649	47718	-
4	7611	56080	54116	-	-

Line04

Total IED \ Single Relay	0	1	2	3	4
0	0	7	1957	11208	10986
1	1	434	12117	12034	11595
2	23	7894	15267	12982	18084
3	258	11970	12153	14758	-
4	1875	13697	13426	-	-

Line05

Total IED \ Single Relay	0	1	2	3	4
0	0	0	28	1392	1420
1	0	4	2078	2412	1476
2	0	140	2040	486	4058
3	6	3518	529	2739	-
4	130	1401	1393	-	-

Line06

Total IED \ Single Relay	0	1	2	3	4
0	0	7	2102	16909	15665
1	1	491	16644	17046	68388
2	28	9796	29695	29122	76103
3	382	20652	21389	59360	-
4	3327	26942	27212	-	-

Line07

Total IED \ Single Relay	0	1	2	3	4
0	0	0	0	18	2021
1	0	0	88	592	53569
2	0	28	460	9916	53846
3	7	2115	1100	40953	-
4	139	1392	4837	-	-

Line08

Total IED \ Single Relay	0	1	2	3	4
0	0	7	2112	16882	16150
1	1	499	17777	19776	70008
2	29	9892	29292	30678	54816
3	390	22235	23055	63518	-
4	3278	28000	27963	-	-

Line09

Total IED \ Single Relay	0	1	2	3	4
0	0	0	160	5261	2940
1	0	36	3673	3914	56363
2	2	1501	11824	13725	81355
3	55	6258	6749	47956	-
4	719	12172	10949	-	-

Line10

Total IED \ Single Relay	0	1	2	3	4
0	0	0	94	4726	4527
1	0	20	8037	3095	66138
2	1	800	2330	12974	87489
3	30	2980	4983	50963	-
4	404	3712	7442	-	-

Line11

Total IED \ Single Relay	0	1	2	3	4
0	0	0	122	6088	4348
1	0	24	1594	2974	66248
2	1	924	2492	13174	77672
3	30	3348	4570	50671	-
4	413	3598	8137	-	-

Line12

Total IED	Single Relay 0	1	2	3	4
0	0	0	94	4766	4604
1	0	20	8010	2933	66182
2	1	798	2247	13034	65990
3	30	3736	4857	48710	-
4	401	3592	7824	-	-

Line13

Total IED	Single Relay 0	1	2	3	4
0	0	35	10026	71250	82336
1	5	2146	100885	106080	151055
2	120	47514	112753	131987	179852
3	1389	119162	128257	161216	-
4	15802	118870	130307	-	-

Line14

Total IED	Single Relay 0	1	2	3	4
0	0	28	7702	58526	49047
1	4	1817	88273	69202	118267
2	104	39516	84654	81076	126731
3	1276	100780	84963	116449	-
4	12607	95847	80262	-	-

Line15

Total IED	Single Relay 0	1	2	3	4
0	0	28	7610	564408	552590
1	4	1778	377441	94593	140691
2	101	41035	96163	116327	169401
3	1206	101051	112526	144753	-
4	12352	95736	109910	-	-

Bibliography

1. A. Bani-Ahmed and A. Nasiri. Development of real-time hardware-in-the-loop platform for complex microgrids. In *Renewable Energy Research and Applications (ICRERA), 2015 International Conference on*, volume 5, pages 994–998, 2015.

2. M. Begovic. Trends in Power System Wide Are Protection. *IEEE PES Power Systems Conference and Exposition*, 3:1612–1613, 2004.

3. M. Ben-Ari. A primer on model checking. *ACM Inroads*, 1(1):40, 2010.

4. C. Bergenhem. A status protocol for system-operation in a fault-tolerant system - Verification and testing with SPIN. *IEEE International Conference on Emerging Technologies and Factory Automation, ETFA*, 2012.

5. J. Blackburn and T. Domin. *Protective relaying: principles and applications*. CRC Press, third edition, 2007.

6. T. A. Bopp, R. Ganjavi, R. Krebs, B. Ntsin, M. Dauer, and J. Jaeger. Improving Grid Reliability through Application of Protection Security Assessment. *12th IET International Conference on Developments in Power System Protection (DPSP 2014)*, pages 2.4–2.4, 2014.

7. G. Cardoso, J. G. Rolim, and H. H. Zurn. Application of neural-network modules to electric power system fault section estimation. *IEEE Transactions on Power Delivery*, 19(3):1034–1041, 2004.

8. C.-F. Chien, S.-L. Chen, and Y.-S. Lin. Using bayesian network for fault location on distribution feeder. *IEEE Transactions on Power Delivery*, 17(3):785–793, 2002.

9. W. Cong, Z. Pan, and L. Ding. Study of a high-speed communication network based wide-area protection system. *IEE Conference Publication*, 2:689–692, 2004.

10. Z. F. Fan, G. B. Song, C. Q. Wang, and S. Y. Bai. Study on distance protection based on wide area information. In *China International Conference on Electricity Distribution (CICED)*, pages 10–13, 2016.

11. P. S. Georgilakis, J. Katsigiannis, and K. P. Valavanis. Petri Net based transformer fault diagnosis. In *Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on*, volume 5, pages 980–983, 2004.

12. R. Giovanini, K. M. Hopkinson, D. V. Coury, and J. S. Thorp. A primary and backup cooperative protection system based on wide area agents. *IEEE Transactions on Power Delivery*, 21(3):1222–1230, 2006.

13. J. D. Glover and M. S. Sarma. *Power system analysis and design: with personal computer applications*. International Thomson Publishing Company, fifth edition, 2012.

14. A. Gmeiner, I. Konnov, U. Schmid, H. Veith, and J. Widder. Tutorial on parameterized model checking of fault-tolerant distributed algorithms. In *International School on Formal Methods for the Design of Computer, Communication and Software Systems*, pages 122–171, 2014.

15. S. T. Hamman, K. M. Hopkinson, and J. E. Fadul. A Model Checking Approach to Testing the Reliability of Smart Grid Protection Systems. *IEEE Transactions on Power Delivery*, PP(99):1, 2016.

16. G. J. Holzmann. The model checker spin. *IEEE Transactions on software engineering*, 23(5):279–295, 1997.

17. G. J. Holzmann. *Spin model checker, the: primer and reference manual*. Addison-Wesley Professional, 2003.

18. S. H. Horowitz and A. G. Phadke. Third zone revisited. *IEEE Transactions on Power Delivery*, 21(1):23–29, 2006.

19. S. H. Horowitz and A. G. Phadke. *Power system relaying*. John Wiley & Sons, fourth edition, 2014.

20. A. Khurram, H. Ali, A. Tariq, and O. Hasan. Formal reliability analysis of protective relays in power distribution systems. In *International Workshop on Formal Methods for Industrial Critical Systems*, pages 169–183, 2013.

21. S. J. Lee, B. W. Min, K. H. Chung, M. S. Choi, S. H. Hyun, and S. H. Kang. An adaptive optimal protection of a distribution system using a multi-agent system. *Developments in Power System Protection, 2004. Eighth IEE International Conference on*, 2:611–614 Vol.2, 2004.

22. S.-I. Lim, M.-S. Choi, and S.-J. Lee. Adaptive protection setting and coordination for power distribution systems. *Proceedings of the 11th International Middle East Power Systems Conference, MEPCON'2006*, 1:129–134, 2006.

23. X. Lin, Z. Li, K. Wu, and H. Weng. Principles and implementations of hierarchical region defensive systems of power grid. *IEEE Transactions on Power Delivery*, 24(1):30–37, 2009.

24. Z. Lin, F. Wen, C.Y. Chung, and K.P. Wong. A survey on the applications of petri net theory in power systems. *2006 IEEE Power Engineering Society General Meeting, PES*, pages 1–7, 2006.

25. B. Liscouski and W. Elliot. Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations. *A report to US Department of Energy*, 40(4):86, 2004.

26. B. Long, J. Dingel, and T. C. N. Graham. Experience applying the SPIN model checker to an industrial telecommunications system. *Proceedings of the 13th international conference on Software engineering - ICSE '08*, page 693, 2008.

27. A. Mahmood, O. Hasan, H. R. Gillani, Y. Saleem, and S. R. Hasan. Formal reliability analysis of protective systems in smart grids. In *Region 10 Symposium (TENSYMP), 2016 IEEE*, pages 198–202, 2016.

28. M. Moulin, L. Gluhovsky, and D. Geist. Formal verification analysis of load-voltage power control. *Intelligent Automation and Soft Computing*, 12(1):23–30, 2006.

29. T. Murata. Petri Nets : Properties , Analysis and Applications. *Proceedings of the IEEE*, 77(4):541–580, 1989.

30. C. Newcombe, T. Rath, F. Zhang, B. Munteanu, M. Brooker, and M. Deardeuff. How Amazon web services uses formal methods. *Communications of the ACM*, 58(4):66–73, 2015.

31. G. Ramos, J.L. Sanchez, a. Torres, and M.a. Rios. Power Systems Security Evaluation Using Petri Nets. *IEEE Transactions on Power Delivery*, 25(1):316–322, 2010.

32. J. Rushby. Formal methods and their role in the certification of critical systems. In *Safety and reliability of software based systems*, pages 1–42. Springer, 1997.

33. H. Saissi, P. Bokor, C. A. Muftuoglu, N. Suri, and M. Serafini. Efficient verification of distributed protocols using stateful model checking. In *Reliable Distributed Systems (SRDS), 2013 IEEE 32nd International Symposium on*, pages 133–142, 2013.

34. F. Schneider, S. Easterbrook, J. R. Callahan, and G. J. Holzmann. Validating Requirements for Fault Tolerant Systems using Model Checking. *Third International Conference on Requirements Engineering*, pages 1–13, 1998.

35. A. Sengupta, S. Mukhopadhyay, and A. K. Sinha. Automated verification of power system protection schemes - Part I: Modelling and specifications. *2015 IEEE Power & Energy Society General Meeting*, 30(5):1–1, 2015.

36. Y. Serizawa, H. Imamura, and M. Kiuchi. Performance Evaluation of IP-based Relay Communications for Wide-area Protection Employing External Time Synchronization. In *Power Engineering Society Summer Meeting, 2001*, volume 2, pages 909–914, 2001.

37. J. Sun, S.-Y. Qin, and Y.-H. Song. Fault Diagnosis of Electric Power Systems Based on Fuzzy Petri Nets. *IEEE Transactions on Power Systems*, 19(4):2053–2059, 2004.

38. 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. *IEEE Transactions on Power Delivery*, 15(2):508–514, 2000.

39. C.-W. Ten, K. Yamashita, Z. Yang, A. Vasilakos, and A. Ginter. Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems. *IEEE Transactions on Smart Grid*, pages 1–1, 2017.

40. X. Tong, X. Wang, and K. M. Hopkinson. The modeling and verification of peer-to-peer negotiating multiagent colored petri nets for wide-area backup protection. *IEEE Transactions on Power Delivery*, 24(1):61–72, 2009.

41. X. Tong, X. Wang, R. Wang, F. Huang, X. Dong, K. M. Hopkinson, and G. Song. The study of a regional decentralized peer-to-peer negotiation-based wide-area backup protection multi-agent system. *IEEE Transactions on Smart Grid*, 4(2):1197–1206, 2013.

42. F. Wang and J. Tang. Modeling of a transmission line protection relaying scheme using petri nets. *IEEE transactions on Power Delivery*, 12(3):1055–1063, 1997.

43. X. R. Wang, K. M. Hopkinson, J. S. Thorp, R. Giovanini, K. Birman, and D. Coury. Developing an Agent-based Backup Protection System for Transmission Networks. *Power Systems and Communications Infrastructures for the Future*, 2002.

44. Official SPIN Website. Inspiring applications of spin. Available: http://spinroot.com/spin/success.html. [Accessed 10-Feb-2018].

45. A. J Wood and B. F. Wollenberg. *Power generation, operation, and control*. John Wiley & Sons, second edition, 2012.

46. Z. Yongli, H. Limin, and L. Jinling. Bayesian networks-Based approach for power systems fault diagnosis. *IEEE Transactions on Power Delivery*, 21(2):634–639, 2006.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
22–03–2018	Master's Thesis	Sept 2016 — Mar 2018

4. TITLE AND SUBTITLE

Evaluation of Resiliency in a Wide-Area Backup Protection System via Model Checking

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Elliott, Kolby H., Capt, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-18-M-023

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

intentionally left blank

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Modern civilization relies heavily on having access to reliable power sources. Recent history has shown that present day protection systems are not adequate. Numerous backup protection (BP) systems have been proposed to mitigate the impact of primary protection system failures. Many of these novel BP systems rely on autonomous agents communicating via wide-area networks. These systems are highly complex and their control logic is based on distributed computing. Model checking has been shown to be a powerful tool in analyzing the behavior of distributed systems. In this research the model checker SPIN is used to evaluate the resiliency of an agent based wide-area backup protection (WABP) system. All combinations of WABP system component malfunctions that lead to system failure are identified and classified. The results of this research indicate that the WABP system evaluated is more resilient to component malfunctions than previously reported. Possible WABP system improvements are introduced as well.

15. SUBJECT TERMS

Model Checking, Thesis, Backup Protection, WABP

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Kennith M. Hopkinson, AFIT/ENG
U	U	U	U	62	19b. TELEPHONE NUMBER *(include area code)* 937-255-3636 x4579; kennith.hopkinson@afit.edu