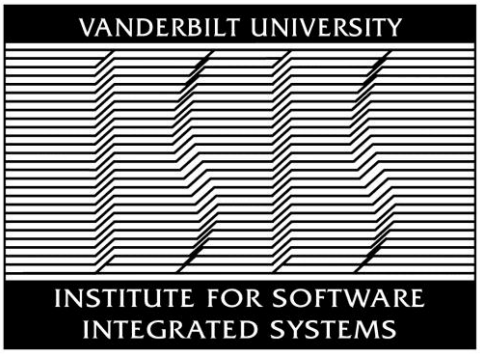

Institute for Software-Integrated Systems

Technical Report

TR#: **ISIS-17-101**

Title: **Cyber-Physical Vulnerability Analysis**

Authors: **Saqib Hasan, Ajay Chhokra, Nagabhushan Mahadevan, Abhishek Dubey and Gabor Karsai**

Cyber-Physical Vulnerability Analysis

Saqib Hasan, Ajay Chhokra, Nagabhushan Mahadevan, Abhishek Dubey and Gabor Karsai
Institute for Software-Integrated Systems.
Vanderbilt University, Nashville, TN 37212, USA
Email:{saqibhasan,chhokraad,nag,dabhishe,gabor}@isis.vanderbilt.edu

Abstract

Electrical power systems consists of various components including physical components such as generator, transmission lines, buses, loads, transformers etc. and discrete components such as protection relays and other supervisory and control devices. Cyber failures in discrete components such as protection devices contribute towards cascading failures resulting in blackouts in electrical power transmission systems. These cyber failures can result from a number of ways such as data errors, communication errors, cyber attacks causing software malfunction etc. The technical report aims to model the behavior of these components in nominal and faulty conditions and apply it towards cascade simulation thereby performing contingency analysis and identifying highly vulnerable components in the system for specific combinations of faults. The results are demonstrated using a standard IEEE-14 Bus System.

I. Introduction

Electrical power systems consists of various components including physical components such as generator, transmission lines, buses, loads, transformers etc. and discrete components such as protection relays and other supervisory and control devices. The responsibility of protection devices is to isolate faulty components from the power system network as per deterministic protection schemes. However, the control actions employed by these devices are based upon the local information i.e. branch power flows and bus voltages. While this approach of using local information helps to quickly identify and isolate faulty components, locally optimal solutions may not always improve the overall system stability as a whole. Presence of component failures or relay mis-operations can further produce cascading effects leading to blackouts as seen in the Aug 2003 Northeast blackout of the USA [1], 2003 Italian [2] blackouts. For instance, consider the IEEE 14 bus system shown in Figure 1. Outage of line L1_5 due to physical fault (three phase to ground fault) may not cause any further failures in the system but if there is a protection assembly failure (stuck breaker fault in circuit breaker) in PA12 along with the physical fault in line L1_5 due to which the protection assembly PA12 is unable to isolate the fault then this will lead to a cascading failure until all the current carrying paths to this fault are isolated. This can cause further disturbance to the system in the form of overloads and can contribute towards cascade progression. Similarly, other protection assembly failures cause different interactions within the system which needs to be included in cascading failure studies.

Failures in these protection elements can affect the nominal behavior of the relay and can contribute to cascade progression. These failures in protection assembly can be categorized as 1) Missed Detection Faults 2) Spurious Detection Faults and 3) Stuck Breaker Faults due to cyber attacks, which are referred to as *cyber faults* later in the paper. *Missed detection faults* force a component to avoid detection of a failure condition whereas *Spurious detection fault* incorrectly conclude the presence of a fault condition. *Stuck breaker fault* has two types namely *Stuck Open Fault* and *Stuck Close Fault*. These failure modes do not let the circuit breakers to operate as desired due to cyber-attacks. So in order to diagnose and predict cascade evolution, its important to consider the behavior of discrete devices with reasonable timing accuracy.

Existing approaches for cascading failure analysis is to perform off-line simulations to assess the current state of power system and study its evolution using different cascade simulation models [5], [6], [7], [8], [9], [10], [11]. Models referenced in [5], [7], [8], [9], are based on initiating failures that cause line overloads leading to cascading failures in the system but they do not consider the interaction of cyber failures in protection devices that can also contribute to such failures. However models in [6], [10], [11] considers faults in protection assembly in the form of hidden failures or sympathetic tripping. But this greatly limits the cascade evolution paths as this tripping is permissible only in the lines which are connected to the same bus of the previous line outage. Moreover in all these models time causality of the events is not considered. This can be very useful in initiating a failure at any desired instant, that can change the cascade evolution path as well as in analyzing the effect of a particular fault in cascade progression. Time is also helpful for the operators in detailed cascading analysis and designing better mitigation strategies. Taking these cyber failures and time causality of events into account will evolve the cascade in a different way, which cannot be studied based on above models but is possible via this approach.

This report aims at providing detailed behavioral models of distance relays, over current relays and breakers in nominal and faulty modes of operation, where it takes into account timing of the events and cyber failures that can lead to cascading failures/blackouts. We also propose a simple cascade simulation model and show the applicability of behavioral models considering *cyber faults* in performing contingency analysis and finding highly vulnerable components in the system for specific fault combinations. The study is done on a standard IEEE-14 Bus System.

The report is organized as follows: Section II discusses the detailed explanation of distance relay, over current relay and circuit breaker behavioral models. Section III describes cascade simulation model and provides an approach towards identifying

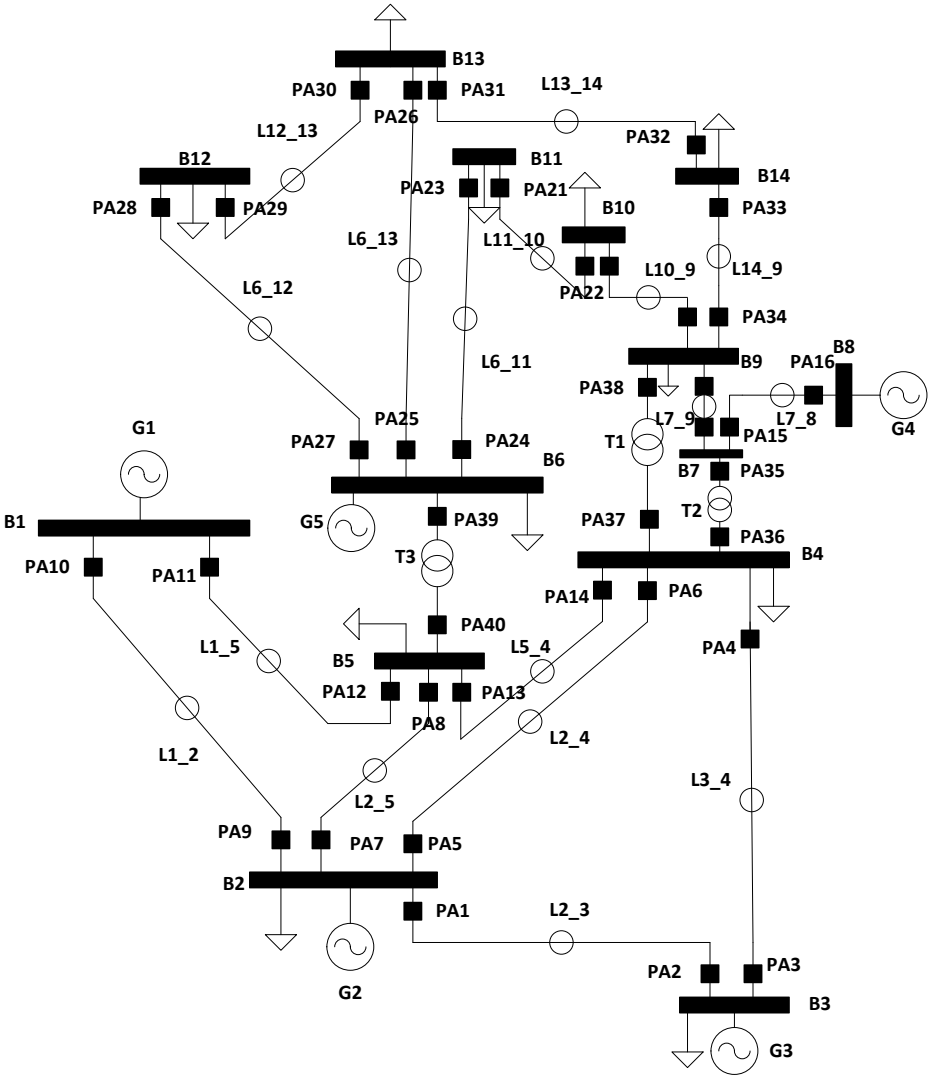

Fig. 1: IEEE 14 Bus System [3]

vulnerable components in the system. Experimental setup and system under test is discussed in Section IV. The results are listed in Section V followed by the conclusion in Section VI.

II. Protection Assembly Behavioral Model

The protection assembly consists of a distance relay, an over-current relay and circuit breaker. The distance relay act as the primary protection whereas the over-current relay acts as the backup protection. This backup protection kicks in only if the primary protection fails to operate and there is a persisting overload condition in the system. In case of faults, relays and circuit breakers operate and protect the network from severe damage but due to failures within them they can cause cascading failures which result in blackouts. These failures are modeled as cyber faults in the protection assembly and are listed in Table I along with other parameters used in the modeling of the protection assembly. Three types of *cyber faults* are modeled namely *Missed Detection Fault*, *Spurious Detection Fault* and *Stuck Breaker Fault*. Each fault can be triggered externally at any desired time. *Missed Detection Fault* is a cyber fault when the relay is unable to detect an active fault. This causes an inability in the relay to provide the necessary control action for fault clearance. *Spurious Detection Fault* is a cyber fault when the relay detects a random fault without evaluating the detection algorithm. However, *Stuck Breaker Fault* is a cyber fault in the circuit breaker when it is unable to operate as needed i.e. if the breaker contacts are unable to open/close as desired due to cyber-attacks. A combination of these faults along with physical faults (for instance 3 phase to ground fault) can help us simulate and analyze cascading failure leading to blackout which are otherwise not obvious and can also help in performing

TABLE I: Protection Assembly- Parameters Description

Port Name	Type	Description
Distance Relay		*Common variables for over-current relay
F_de1*	Variable	boolean variable that determines the presence of a Missed Detection Fault
F_de2_zX(X =1,2,3)	Variables	boolean variables that determines the presence of a zone1, zone2, zone3 Spurious Detection Fault
V, I*	Data	data variables representing 3 phase bus voltage and line currents
R, L, Len	Data	These variables represents the resistance, inductance and length of the transmission line
RelayTrip	Variable	Change in its state causes the relay to trip based on POTT scheme [4]
c_reset	Variable	boolean variable that determines the presence of a reset signal. This signal brings the relay in normal mode of operation.
Trip*	Variable	If this signal is high the circuit breaker disconnects the branch in the network
Z1, Z2, Z3	Events	Represents the presence of zone1, zone2, zone3 fault
RelayTrip_	Event	Occurrence of this event forces the relay in POTT scheme [4] to trip
cmd_open*, cmd_close*	Events	Occurence of these events cause the circuit breaker to open/close
relayFs*	Variable	Determines the frequency at which relay operates
ZxWT (X=2,3)	Variables	Holds the zone2 and zone3 wait time for which the relay is supposed to wait before taking an action
Circuit Breaker		
F_stuck_open, F_stuck_close	Variables	boolean variables that determines the presence of Stuck open and Stuck close Faults respectively.
cmd_open, cmd_close	Variables	Change in the value of these variables cause the activation of the physical circuit breaker
PhysicalStatus	Variable	This variable keeps track of the state of the physical circuit breaker, 0 is open and 1 is close
Trip	Variable	This variable tells the state of the circuit breaker, 0 is open and 1 is close
st_open, st_close	Events	Occurrence of these events provide the state of the circuit breaker, st_open means circuit breaker is open and st_close means circuit breaker is close
Over-Current Relay		
F_de2_Px(x=1,2,3)	Variables	boolean variables that determine the presence of high, medium and low overloads-Spurious Detection Fault
Px_OL(x=1,2,3)	Events	Represents the presence of High, Medium and Low overloads
CThres	Data	It holds the maximum loading value of the branch
ZoneWaitTime	Variable	It holds the time for which the relay is supposed to wait before taking an action

contingency analysis on these simulation models.

1. Distance Relay: A distance relay is used as the primary protection in electrical power transmission systems. Its behavioral model (Figure 2) is designed using Matlab/Stateflow [12]. Table I shows the details about the parameters used in the modeling of distance relay. The sampling rate of the relay is 1 ms. Three zone reaches (zone1, zone2, zone3) are modeled in the distance relay behavioral model (Figure 2), which are represented by states 'chkZx' (where x=1, 2, 3 for zone1, zone2 and zone3 respectively). These zones mark the protection zones of the transmission line as per reference [13].

Normal mode operation: During normal operation, the distance relay remains in 'idle' state because the load impedance seen by the relay does not fall in any of the zone reaches. However, when a three phase to ground fault (physical fault) occurs in a transmission line and there is no cyber fault, the distance relay transitions from its 'idle' state to one of the 'chkZx'(x= 1, 2, 3) state depending on the load impedance seen by it. These transitions depend on a simple detection algorithm (dl(V,I,R,L,Len), based on references [13], [14]), which computes the load impedance and direction of the fault. This computation is based on the line voltages and currents.

In case of a zone1 fault detection, the relay transitions immediately from its 'idle' state to the 'Tripped' state and sends a 'cmd_open' to its associated circuit breaker behavioral model. However, if there is a zone2 or zone3 fault detection, the relay transitions from its 'chkZx'(x=2, 3) state to the 'waitingX' (X= 1, 2) state after the wait time for its respective zone is elapsed. These wait times are external parameters, which can be set by the user. If fault gets cleared while the distance relay is in the 'waitingX' (X= 1, 2) state, it transitions back to the 'idle' state. However, if fault persists, the relay transitions to the 'Tripped' state and sends the 'cmd_open' to the circuit breaker.

Operation under cyber faults: In case there is a *Missed detection Fault* while the relay is in 'idle' state (Figure 2), it transitions to the 'DetErr' state resulting in no detection even though there might be an active zone fault. The relay will transition back to its 'idle' state once the fault is cleared. In the presence of *Spurious Detection Fault*, the relay incorrectly detects a fault and transitions from 'idle' state to the 'DetErrX'(where X=2,3) state and then transitions to the 'Tripped' state based on the zone2 and zone 3 wait times. In case of a zone 1 *Spurious Detection Fault*, the relay immediately transitions from 'idle' state to the 'Tripped' state.

2. Over-Current Relay: An over-current relay is used as a backup protection for transmission lines in electrical power systems. Its behavioral model is shown in Figure 3 and Table I lists the details about the parameters used in its modeling. An inverse-time over-current relay is modeled for handling different amounts of overloads. These overloads are classified as high, medium and low overloads represented by states 'Px' (Figure 3, where x=1,2,3). There is a wait time associated with each overload, high overload having the least wait time and low overload having the longest wait time. These wait times are multiplied by constants (2, 3 and 7) in order to depict inverse time over-current characteristics in the relay. It means that higher the detected overload quicker the over-current relay will send the trip command to the circuit breaker. For instance, consider a wait time of 1 seconds, if the overload is high the relay trips the circuit breaker at 2 seconds. However, if the

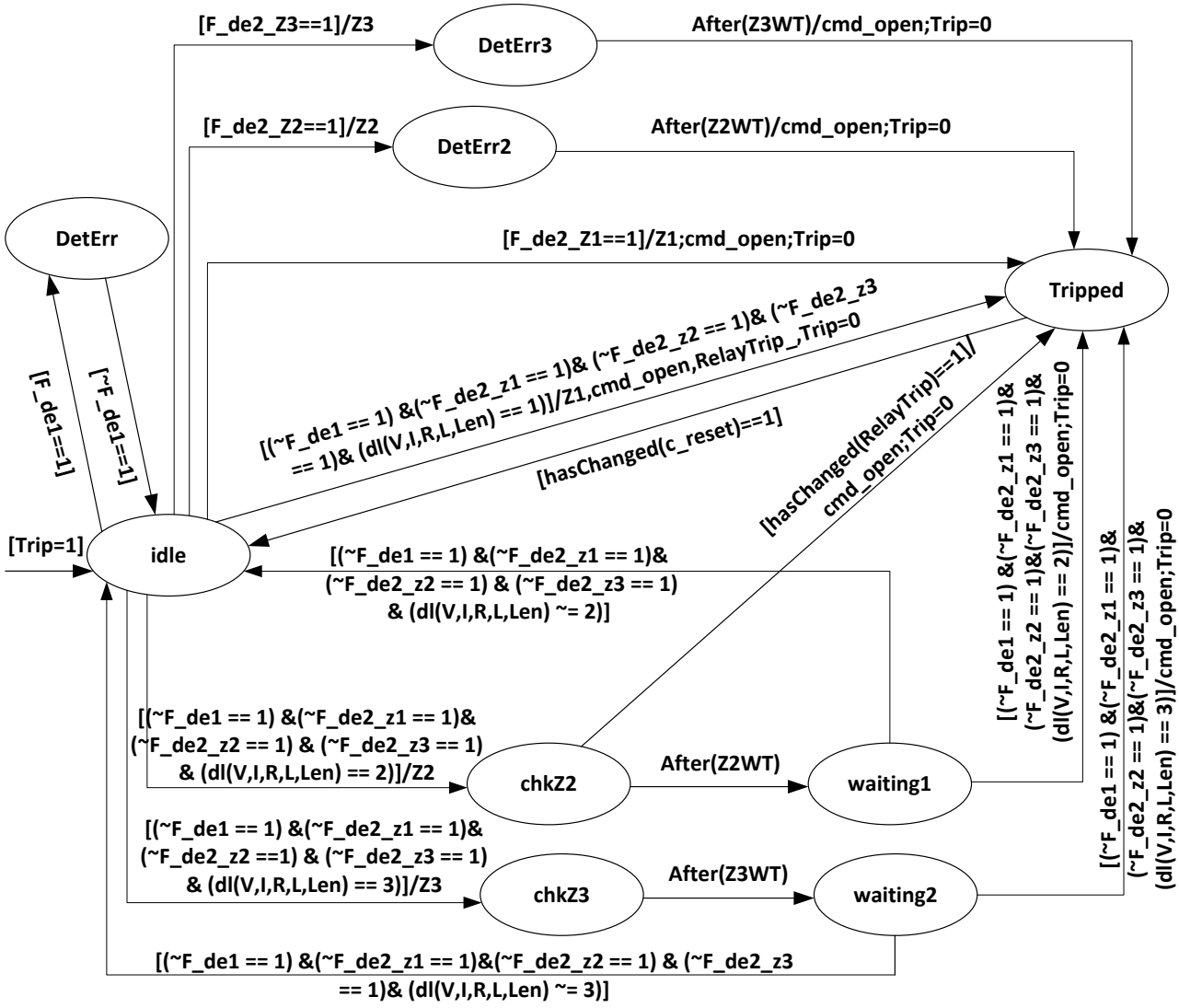

Fig. 2: Distance Relay Stateflow Behavioral Model.

overloads are medium or low the relay trips the circuit breakers at 3 seconds, 7 seconds respectively. This depicts the inverse time over-current relay characteristics.

Normal mode operation: During normal operation, the relay remains in the 'idle' state (Figure 3). However, if there is an overload condition, the relay transitions from 'idle' state to its 'Px' state (where x=1 to 3), depending on the amount of overload. These transitions are based on a simple detection algorithm (OC(I,CThres)) used for sensing overloads [15]. Being in one of the 'Px' states, the relay transitions to its 'waitingX' (X =1, 2) state after the wait time associated with the overload elapses. In this state, the relay again checks for the overload condition and if it persists, the relay transitions to the 'Tripped' state sending a 'cmd_open' to the circuit breaker. Otherwise, the relay transitions to the 'idle' state.

Operation under cyber faults: In case there is a *Missed detection Fault* while the relay is in 'idle' state (Figure 3), it transitions to the 'DetErr' state resulting in no detection even though there might be an overload condition. In the presence of a *Spurious Detection Fault*, the relay transitions from the 'idle' state to the 'DetErrX'(where X=1,2,3) state (Figure 3) and then transitions to the 'Tripped' state after the wait time associated with it has elapsed.

3. Circuit Breaker: The circuit breaker behavioral model is designed using Matlab/Stateflow (Figure 4) and Table I shows the details about the parameters in its modeling.

Normal mode operation: Under normal operation, the circuit breaker remains in 'close' state because of the absence of 'cmd_open' from the distance relay or over-current relay. However, if it receives a 'cmd_open', the circuit breaker transitions from 'close' state to the 'opening' state. Circuit breaker being a mechanical device takes time to open/close. Hence, we

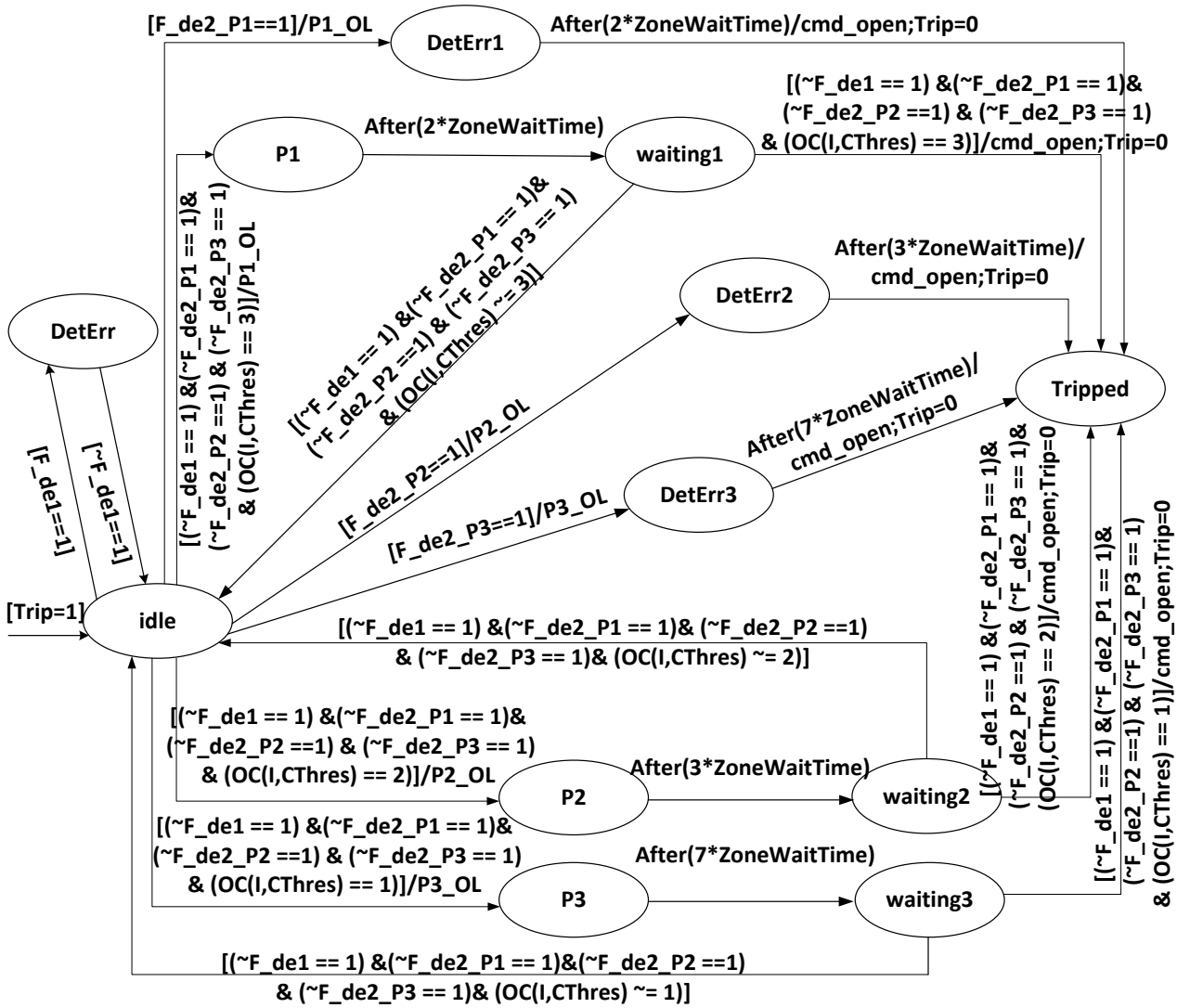

Fig. 3: Over-Current Relay Stateflow Behavioral Model.

introduced a delay in the opening/closing operations of the circuit breaker for more realistic behavior. This delay is provided by the variables tto and ttc in the model. After the delay has elapsed it transitions from the 'opening' state to the 'wait_open' state and then transitions to the 'open' state indicating the status of the circuit breaker (as 'open') using the event 'st_open'. If the circuit breaker receives a 'cmd_close', while being in 'open' state, it transitions to 'closing' state. Again, it waits for the delay to elapse and transitions to the 'wait_close' state. From 'wait_close' state it transitions to the 'close' state signaling the state of the circuit breaker (as 'close') using 'st_close'.

Operation under cyber faults: If the circuit breaker is in 'close' state and there is a *Stuck Close Fault* then it remains in the 'close' state. However, if the same fault occurs while the circuit breaker is in the 'opening' state then it transitions back to the 'close' state. If the circuit breaker is in 'open' state and there is a *Stuck Open Fault* then it remains in the 'open' state. However, if the same fault occurs while the circuit breaker is in the 'closing' state then it transitions back to the 'open' state.

In the simulation, a logger function is used to log the details such as occurrence of the cyber faults, zone fault detection, overload detection and activation commands such as 'cmd_open', 'cmd_close', 'st_open', 'st_close' etc. which helps in performing detailed analysis.

III. Towards Contingency Analysis and Vulnerability Analysis

Contingency analysis in electrical power transmission systems is necessary to identify those critical sets, which can cause cascading failures and eventually lead to blackout. By critical set, we mean outage of those components that initiate the cascading

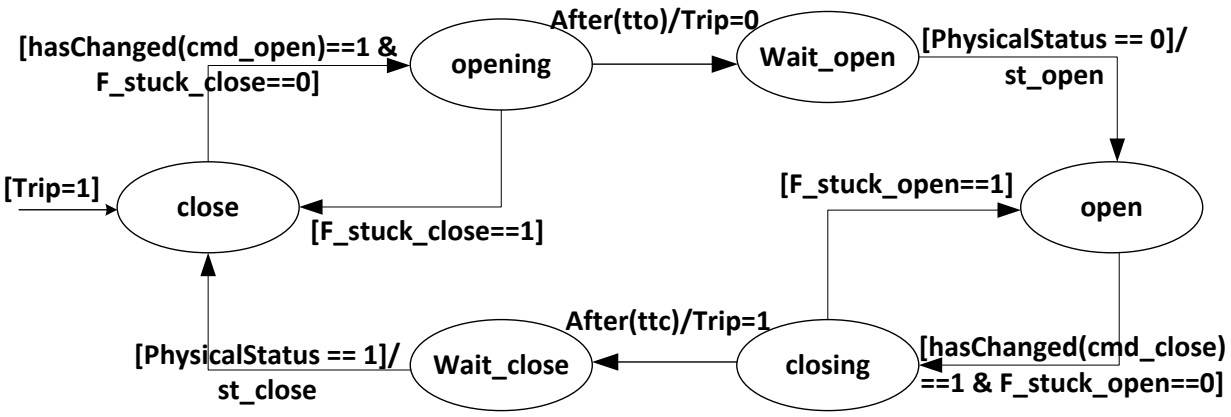

Fig. 4: Circuit Breaker Stateflow Behavioral Model.

failure. Tools such as MATCASC [8], CASCADE model [5] do cascade analysis but they do not consider details about the time between contingencies and cyber failures in the protection equipments, which can lead to severe cascading outages resulting in blackout. This is achieved by integrating the detailed behavioral models of protection assembly in Matlab/Simscape simulation models. The proposed contingency analysis model is shown in Figure 5(a).

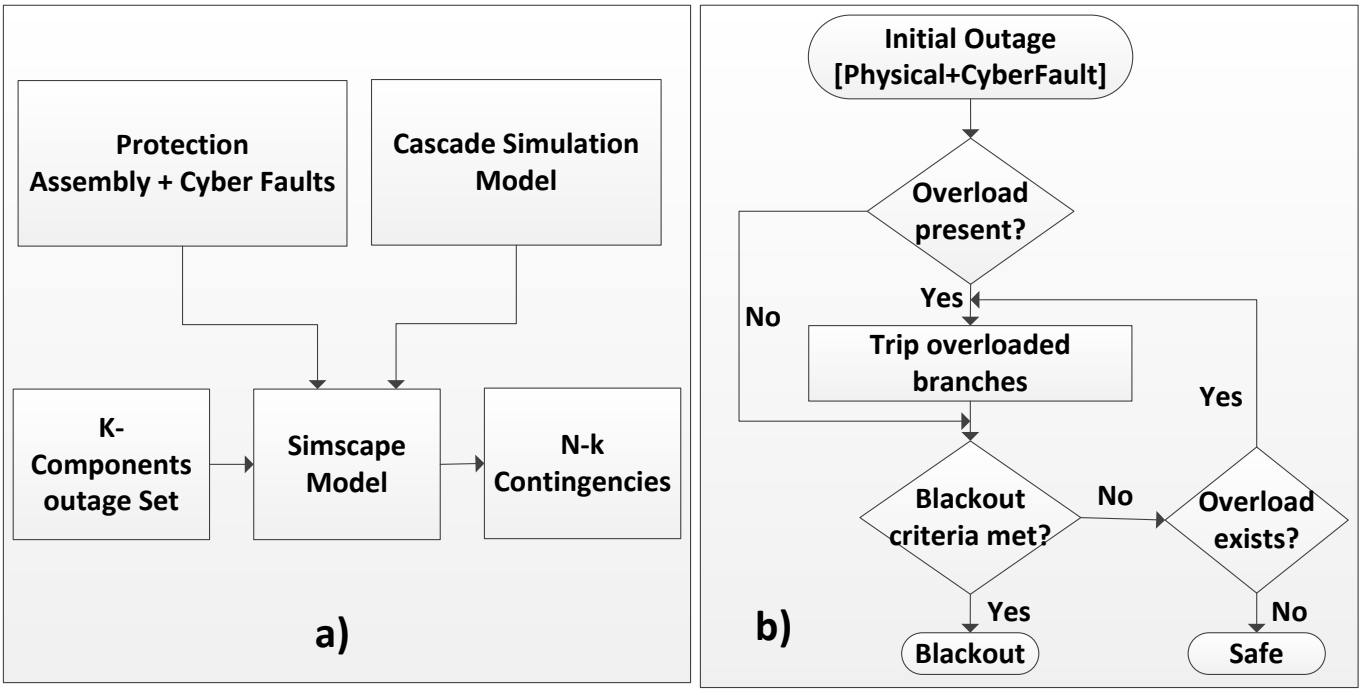

Fig. 5: Cascade Progression Flowchart

Initial components outage (k-components outage) set and the protection assembly blocks can be provided to the Simscape model (modeling of Simscape models are described in Section IV). The set here means, a list of components that are supposed to fail or have faults initially. The protection assembly blocks will contain information about the cyber faults based on the initial component outage set. Simscape model uses this information to simulate the entire system for the desired simulation time and list the contingency in N-k contingency set if it causes a blackout. The N-k contingency set contains the individual combinations of those initial component outages which led to the blackout. Entire simulation progresses based on the cascade simulation model. This model initializes the simulation with initial contingency and checks for further disturbances in the system while evaluating the blackout criteria. Currently, amount of load loss is considered as the blackout criteria in this model as referenced in [16] but it can be extended by taking into account other blackout criterion as well.

The cascade simulation model used to simulate the progression of the initial contingency is based on a simple cascade progression algorithm as shown in Figure 5(b). An initial contingency can be caused due to a combination of physical and cyber fault. However, some cyber faults such as *Missed Detection Fault and Stuck Breaker Faults* manifest only in the presence of a physical fault. For instance, if there is a *Stuck Close Fault in circuit breaker* in PA4 of the system as shown in Figure 1, it will not have any effect on the system unless there is a physical fault present in the transmission line L3_4 which will then be cleared through other protection assemblies as the circuit breaker of PA4 is unable to open. *Spurious Detection Faults* on the other hand can manifest on itself at any time. For instance consider the system of Figure 1, outage of transmission lines L5_4 and L2_4 due to the presence of *Spurious Detection Faults* in the protection assemblies PA13 and PA6 can lead to a cascading event which may result in loss of load but this progression do not require the presence of any other fault such as physical fault in the system.

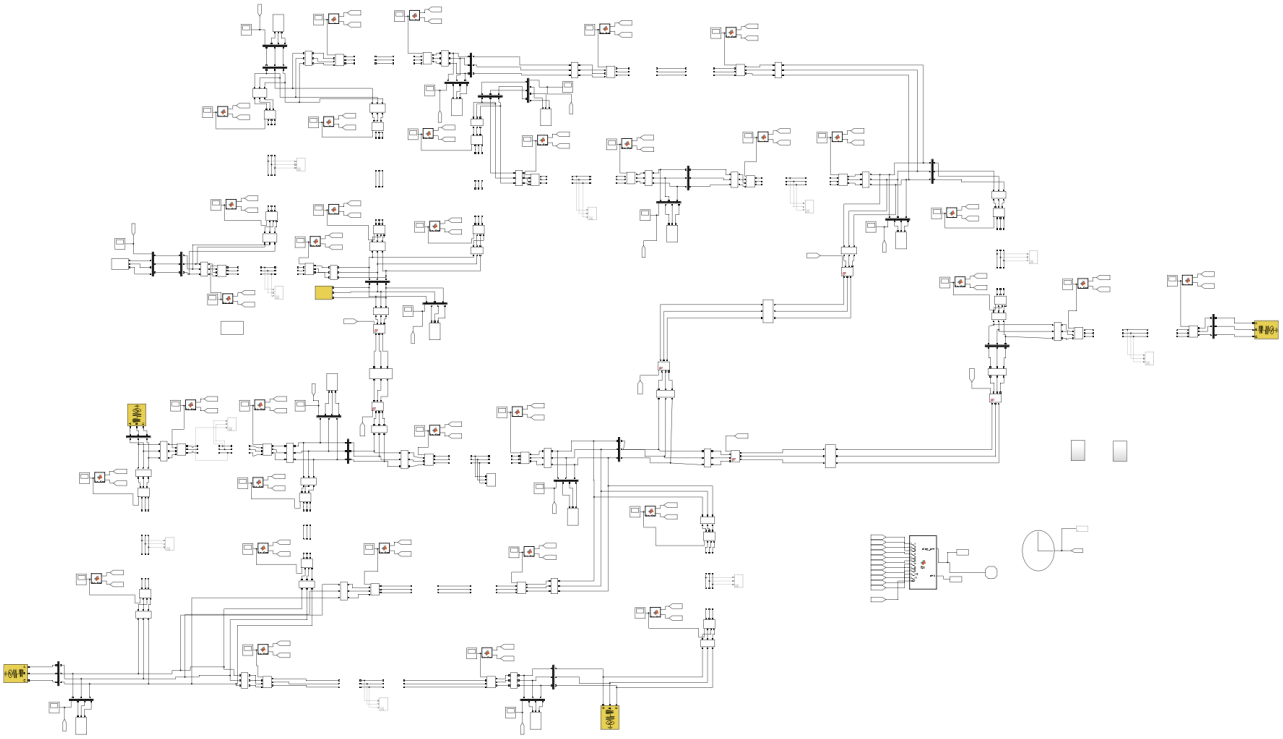

Fig. 6: IEEE-14 Bus System- Simscape Model

In order to simulate the cascade progression using the cascade algorithm as shown in Figure 5(b), the initial contingency is given to the system and it is analyzed for further overloads. If there are overloaded branches (transmission lines and transformers), they are tripped and blackout criteria is verified. If this criteria is not met but the system is still overloaded then the process is repeated again. However, if the blackout criteria is satisfied then the contingency is marked as the one causing 'Blackout'. Otherwise, if the blackout criteria is not satisfied and there is no further overload then the contingency is considered as 'Safe'. Once all the blackout causing initial contingencies are identified, it can be used to find the highly vulnerable components within the system. The model also has a feature of introducing random outages at specific times during the simulation, which could be of interest to the user for analyzing the behavior of the system. For instance, if a random outage is given while the cascade is progressing it can result in obtaining a different trajectory due to change in system topology and this is one of the key feature of the model. Also, the same outage when triggered at different times during the progression can aid in finding those specific points where it is highly disruptive. This may result in a severe outage and can help us identify vulnerable components at during different states of the system. This type of analysis is not possible in tools where an initial outage is given and the system is simulated to check for possible cascading failures causing blackout. In this model it can be done by setting the model parameters accordingly. When these random outage(s) are triggered in the system, the cascade model simulates these failures in the same fashion as described above. At present, this task is done manually but automating it using a Matlab script can be looked into for future work.

IV. System Under test and Experimental Setup

The proposed contingency and vulnerability analysis has been performed on the standard IEEE-14 Bus System [3] shown in Figure 1, which consists of 14 buses, 5 generators and 11 loads. The base voltage and base MVA for the system are 138 kV and 100 MVA respectively. Length of each line is 16 km. The system is modeled in Matlab/Simscape using Simscape library blocks and supporting functions and is shown in Figure 6. Figure 7 shows the Simulink/ Simscape model corresponding to the transmission line 'L2_3 in IEEE 14 bus system (Figure 1), its associated bus and protection assemblies.

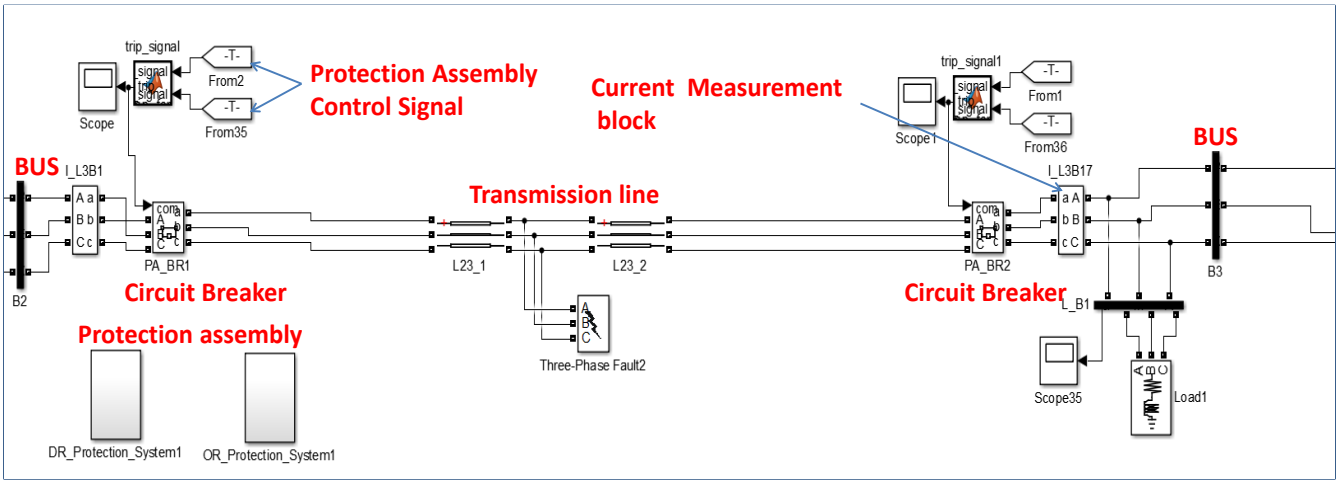

Fig. 7: Portion of IEEE-14 Bus System- Simscape Model

As shown in Figure 7, the transmission line is broken down into segments in-order to introduce faults at different line lengths. It is protected by a pair of protection assembly on each side, which is denoted by PAn ($n \in \mathbb{N}$). Each protection assembly includes a Distance relay (PA_DRn), over-current relay (PA_ORn), and circuit breaker ((PA_BRn). The protection assembly is modeled as a separate subsystem therefore only the circuit breakers are shown at each end of the line (Figure 7). They receive control signals from the protection assembly subsystem. Current measurement takes place at the current measurement blocks and the voltage measurement happens at the bus. Generators are modeled as voltage sources with required base kV and MVA ratings and the loads are modeled as the constant PQ type loads. A Power GUI block is required to run the system in different modes namely phasor, discrete and continuous mode. We run the system in phasor mode for our analysis. The solver type is a variable-step solver and the solver used is ode45 (Dormand-Prince).

V. Results

The study is done on IEEE-14 Bus System assuming that the lines are loaded at 70% of their loading capacity. It consists of two parts namely part 1 and part 2. Part 1 presents a scenario with two cases namely case1 and case2 showing, how presence of cyber fault along with physical fault can lead to severe cascading failures causing blackouts thereby identifying vulnerable components. Part 2 demonstrates the analysis results considering a physical fault and a cyber fault (Stuck Close Fault) in each transmission line and its associated protection assembly (circuit breakers). The assumption is that the *Stuck Close Fault* in the circuit breakers are due to cyber-attacks which does not allow the normal operation of the circuit breakers by preventing the signal to reach them from the protection assembly. The results help in identifying highly vulnerable components which can help in improving system resiliency. The results also show how certain components can be very critical for system resiliency, others less critical and some others not critical at all. This greatly depends on the topology of the system and the type of cyber faults associated with the system components.

Part 1: A scenario is presented which shows how physical and cyber faults together can lead to severe cascading failures.
Case 1: At time t=.5 sec, an initial contingency (a three phase to ground fault) occurs in the transmission line 'L3_4' as shown in Figure 1. A zone 1 fault is detected by the protection assembly 'PA_DR3', 'PA_DR4' and the fault is cleared by sending a command open ('cmd_open') to trip the required circuit breakers ('PA_BR3' and 'PA_BR4'). In the absence of a cyber fault, outage of transmission line 'L3_4' did not cause any further contingency and the system remained stable.

Case 2: Same scenario of case 1 is taken and a cyber fault (*Stuck Close Fault*) is introduced in circuit breaker ('PA_BR4') of protection assembly PA4 as shown in Figure 1 in addition to the physical fault in line 'L3_4' at time t= .5 sec. As a result of this initial contingency, it is observed that a number of transmission lines gets overloaded and are eventually removed from the network. At time t= 2 sec, another cyber fault (*Spurious Detection Fault*) occurred in the distance relay ('PA_DR27') of

TABLE II: Progression of Cascading Failure Leading to Blackout due to Physical and Cyber Faults

Time(sec)	Event Description
0.500	a) 3 phase to ground fault (Physical fault) in Line L3_4, b) Stuck close fault (Cyber fault) in PA_BR4.
0.501	a) Zone 1 fault detection by distance relays PA_DR3, PA_DR4, b) Zone 3 fault detection by PA_DR1, c) 'P1_OL'- High overload detected by PA_OR3, d) 'P2_OL'- Medium level overload detected by PA_OR5, PA_OR1, PA_OR13, e) 'P3_OL' - Low overload detected by PA_OR9, PA_OR15, PA_OR21, f) 'cmd_open' received by circuit breaker PA_BR3.
0.532	a) 'st_open'- circuit breaker PA_BR3 is opened, b) One end of Line L3_4 is disconnected.
2.000	a) Cyber fault (Spurious detection fault) in PA_DR27, b) 'cmd_open' sent by PA_DR27 and received by PA_BR27.
2.031	a) 'st_open'- circuit breaker PA_BR27 is opened, b) Line L6_12 is disconnected.
3.503	a) 'P2_OL'- Medium overload detected by PA_OR13, b) 'cmd_open' sent by PA_OR5, PA_OR21 and received by PA_BR5, PA_BR21.
3.534	a) 'P2_OL'-Medium overload detected by PA_OR31, b) 'st_open'-breaker PA_BR5, PA_BR21 opened, c) Lines L2_4, L11_10 removed.
5.505	a) 'cmd_open' sent by PA_OR13 and received by PA_BR13
5.536	a) 'P1_OL'- High overload detected by PA_OR25, PA_OR33, b) 'P2_OL'- Medium overload detected by PA_OR35, PA_OR40, c)'P3_OL' -Low overload detected by PA_OR29, PA_OR37, d) 'st_open'- circuit breaker PA_BR13 is opened, e) Line L5_4 is disconnected.
6.536	a) 'P1_OL'- High overload detected by PA_OR31.
7.503	a) 'cmd_open' sent by PA_OR15 and received by PA_BR15.
7.534	a) 'st_open'- circuit breaker PA_BR15 is opened, b) Line L7_8 is disconnected.
7.538	a) 'cmd_open' sent by PA_OR25, PA_OR33 and received by PA_BR25, PA_BR33 respectively.
7.569	a) 'P3_OL'- Low overload detected by PA_OR1, b) 'st_open'- breaker PA_BR25, PA_BR33 opened, c) Lines L6_13, L14_9 disconnected.
14.571	a) 'cmd_open' sent by PA_OR1 and received by PA_BR1.
14.602	a) 'st_open'- circuit breaker PA_BR1 is opened, b) Line L2_3 is disconnected.

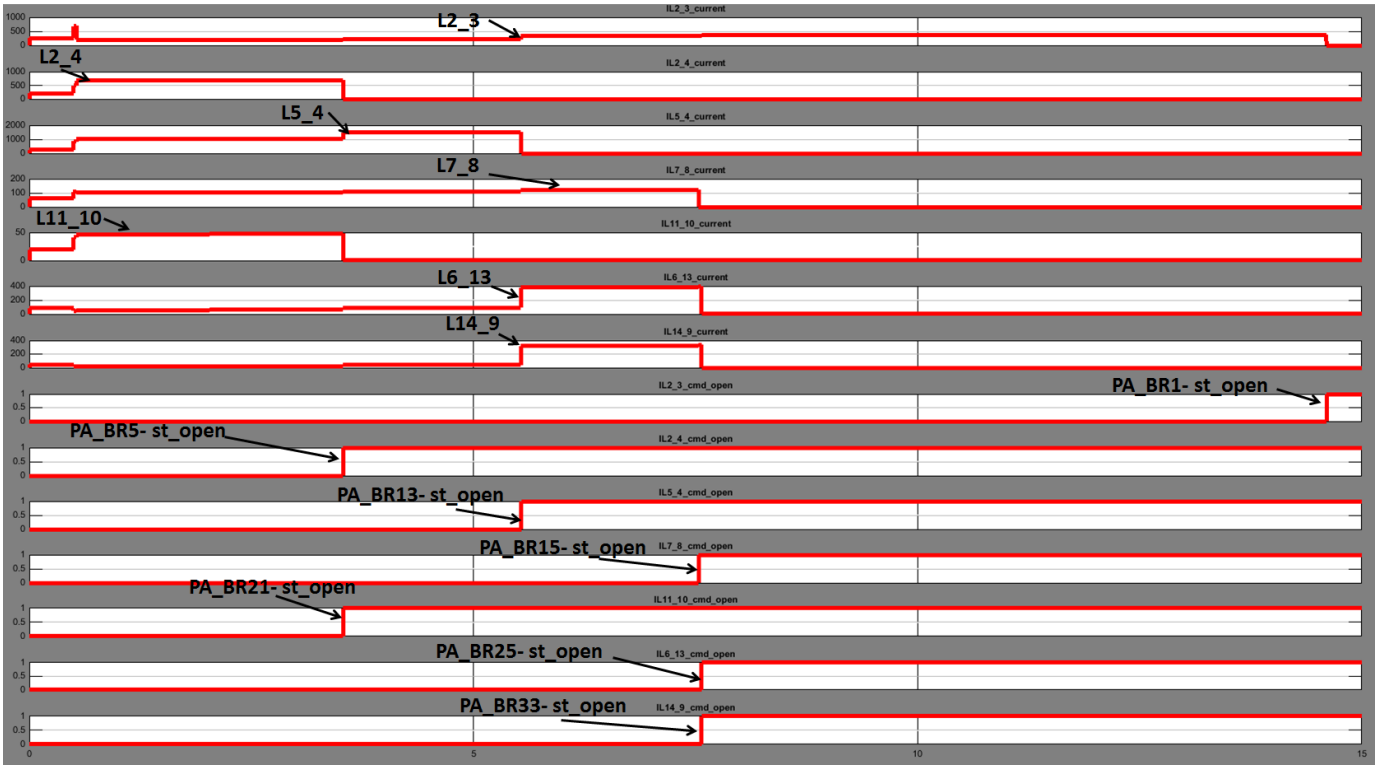

Fig. 8: Line Currents and Circuit Breaker status.

protection assembly PA27 in transmission line 'L6_12' as shown in Figure 1. This contingency is shown to overload some other transmission lines, which gets removed in the process. Figure 8 shows the change in line currents and the status of the circuit breakers connected to these lines during the cascade process. It has 14 waveforms. First 7 waveforms reflect the line currents and the next 7 waveforms show the status of the circuit breakers associated with these lines. Labels L2_3, L2_4, L5_4, L7_8, L11_10, L6_13 and L14_9 show, the current increase in these lines. However, labels PA_BR1-st_open, PA_BR5-st_open, PA_BR13-st_open, PA_BR15-st_open, PA_BR21-st_open, PA_BR25-st_open and PA_BR33-st_open show, the disconnection of these lines from the network through the status open (st_open) of the circuit breaker.

Occurrence of each contingency event and its impact on the system is described in detail in Table II. It shows how the cascade has progressed with time causing multiple failures in the system. Post analysis, it is observed that transmission lines 'L12_13', 'L13_14', 'L10_9', 'L7_9' and transformers 'T1', 'T2' are also considered disconnected because they do not have a current carrying path through them as a consequence of the line removals listed in Table II. These events eventually resulted in a load loss of 46.9% out of the total load and hence caused a blackout based on the criteria referenced in [16]. Due to

this, the initial contingency was marked as a blackout causing contingency and the components causing it are identified as vulnerable components. Similar contingencies and vulnerable components are found based on this approach and are discussed in Part 2. Prior knowledge of such contingencies can help in designing effective mitigation strategies, which could prevent the progression of cascades.

Part 2: A physical fault and a cyber fault is given in each transmission line and its associated protection assembly and the analysis results are discussed in this section. Only the *Stuck Close Breaker Faults* along with physical faults are considered in this study.

As shown in Table III each transmission line is given a physical fault (Three-Phase to Ground Fault) and the associated circuited breakers are given a *Stuck Close Breaker Fault* (Cyber Fault) individually. The simulation is run using the cascade simulation model discussed in section IV and post simulation status of the system (Blackout or not) along with the percentage load loss is recorded. This is performed by considering physical faults for each transmission line and cyber faults (*Stuck Close Breaker Faults*) in each protection assembly associated with the transmission lines. Based on the blackout criterion, Table III shows that there are three highly vulnerable protection assembly components (L3_4, PA_BR4, L5_4, PA_BR13, L5_4, PA_BR14) in the system with this combination of physical and cyber faults. Analysis results from Table III also shows similar combination of this type of faults in other components, which resulted in less load loss. However, there are eight protection assembly components which do not cause any load loss in the system considering the same type of fault combination. Thus highly vulnerable components are identified and the system resiliency can be improved in case of this type of cyber and physical fault. Other combinations can be studied similarly and identifying vulnerable components for those combinations can further improve the resiliency of the system.

TABLE III: Analysis results of transmission lines and protection assemblies with physical and cyber faults.

Line Name and Physical Fault	**PA Name and Fault Type**	**Blackout**	**Load Loss(%)**
L2_3, 3-phase to ground fault	PA_BR1- stuck close fault	No	0
L2_3, 3-phase to ground fault	PA_BR2- stuck close fault	No	0
L3_4, 3-phase to ground fault	PA_BR3- stuck close fault	No	0
L3_4, 3-phase to ground fault	PA_BR4- stuck close fault	Yes	46.9
L2_4, 3-phase to ground fault	PA_BR5- stuck close fault	No	0
L2_4, 3-phase to ground fault	PA_BR6- stuck close fault	No	39.22
L2_5, 3-phase to ground fault	PA_BR7- stuck close fault	No	39.22
L2_5, 3-phase to ground fault	PA_BR8- stuck close fault	No	2.81
L1_2, 3-phase to ground fault	PA_BR9- stuck close fault	No	0
L1_2, 3-phase to ground fault	PA_BR10- stuck close fault	No	0
L1_5, 3-phase to ground fault	PA_BR11- stuck close fault	No	0
L1_5, 3-phase to ground fault	PA_BR12- stuck close fault	No	0
L5_4, 3-phase to ground fault	PA_BR13- stuck close fault	Yes	43.46
L5_4, 3-phase to ground fault	PA_BR14- stuck close fault	Yes	40.65
L7_8, 3-phase to ground fault	PA_BR15- stuck close fault	No	23.27
L7_8, 3-phase to ground fault	PA_BR16- stuck close fault	No	21.84
L7_9, 3-phase to ground fault	PA_BR17- stuck close fault	No	21.84
L7_9, 3-phase to ground fault	PA_BR18- stuck close fault	No	30.98
L9_10, 3-phase to ground fault	PA_BR19- stuck close fault	No	3.88
L9_10, 3-phase to ground fault	PA_BR20- stuck close fault	No	21.84
L10_11, 3-phase to ground fault	PA_BR21- stuck close fault	No	11
L10_11, 3-phase to ground fault	PA_BR22- stuck close fault	No	27.27
L6_11, 3-phase to ground fault	PA_BR23- stuck close fault	No	11
L6_11, 3-phase to ground fault	PA_BR24- stuck close fault	No	13.29
L6_13, 3-phase to ground fault	PA_BR25- stuck close fault	No	18.71
L6_13, 3-phase to ground fault	PA_BR26- stuck close fault	No	15
L6_12, 3-phase to ground fault	PA_BR27- stuck close fault	No	11
L6_12, 3-phase to ground fault	PA_BR28- stuck close fault	No	11.86
L12_13, 3-phase to ground fault	PA_BR29- stuck close fault	No	11.86
L12_13, 3-phase to ground fault	PA_BR30- stuck close fault	No	15
L13_14, 3-phase to ground fault	PA_BR31- stuck close fault	No	18.71
L13_14, 3-phase to ground fault	PA_BR32- stuck close fault	No	5.7
L14_9, 3-phase to ground fault	PA_BR33- stuck close fault	No	5.7
L14_9, 3-phase to ground fault	PA_BR34- stuck close fault	No	28.69

Figure 9 shows the amount of load loss and the number of cases for a particular load loss while considering physical faults and cyber faults (*Stuck Close Faults*). It clearly shows that there are some highly vulnerable components that cause blackout (40% and above load loss) and significant others (5%-40% load loss) which cause load loss but not enough to be classified under the blackout category but are still unhealthy for system resiliency. However, there is a fair number of components which do not cause any load loss while such faults are present.

Fig 9: Load Loss and corresponding occurence

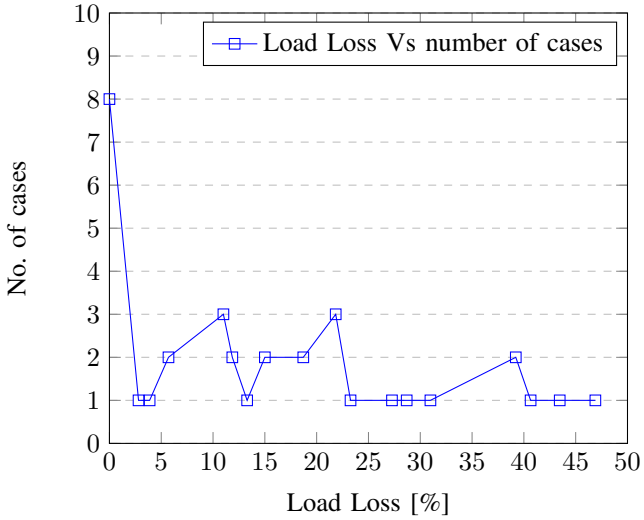

TABLE IV: Critical Components Categorization

Category Name	Component Name	Load Loss
Category I	PA_BR4 PA_BR13 PA_BR14	above 40%
Category II	PA_BR6 PA_BR7	very close to 40% (39.22%)
Category III	PA_BR18 PA_BR22 PA_BR34	above 25% and less than 35%

Based on the study, critical components are identified and categorized in Table IV. Here the components listed in 'Category I' are the components which will lead to a blackout in the presence of a physical fault and a cyber fault. However, the components listed in 'Category II' of Table IV can cause a blackout if there is any other outage in addition to the studied physical fault and cyber fault as the load loss is very close to the blackout criterion. Hence they are less critical compared to 'Category I' but still should be considered while improving system resiliency. Components listed in 'Category III' are comparatively not very critical but can lead to blackout if further system disturbance takes place which would lead to a significant load loss due to other faults or outages. Thus the study clearly shows that not all components in the system are equally vulnerable and it is important to identify the highly vulnerable components to help improve system resiliency.

VI. Conclusion

In this technical report detailed behavioral models of the protection assembly is presented along with the capability of introducing cyber faults at specific instants. Integration of these behavioral models with the simulation models in Matlab/Simscape helped us simulate and analyze severe cascading failures that eventually lead to blackout thereby identifying the highly vulnerable components in the system. The study on IEEE-14 Bus System showed how introduction of cyber faults in addition to physical faults can lead to severe cascading failures causing blackout and how these faults can affect the system. Discussion on the study demonstrates how the vulnerable components in the system are identified in the presence of these faults. Moreover, this approach can be applied in finding N-k contingencies as discussed in Section IV. In addition to that, the design provides the flexibility to easily understand and extend itself to incorporate more aspects, which could help improve the analysis of cascading failures and improve system resiliency. As part of the future work, more complex models need to be analyzed and the entire approach can be automated so as to find highly vulnerable components during specific fault combinations in the system.

Acknowledgment

This work is funded in part by the National Science Foundation under the award number CNS-1329803 and the FORCES project under the award number CNS-1238959. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of NSF or FORCES.

REFERENCES

[1] U.-C. Force, "Final report on the august 14th blackout in the united states and canada," *Department of Energy and National Resources Canada*, 2004.

[2] A. Berizzi, "The italian 2003 blackout," in *Power Engineering Society General Meeting, 2004. IEEE*. IEEE, 2004, pp. 1673–1679.

[3] ICSEG, "Illinois Center for a Smarter Electric Grid(ICSEG)," http://icseg.iti.illinois.edu/ieee-14-bus-system/, [Online; accessed 24-July-2015].

[4] S. SIPROTEC, "Distance protection 7sa522 v4. 70," *instruction manual*, 2011.

[5] I. Dobson, B. A. Carreras, and D. E. Newman, "A loading-dependent model of probabilistic cascading failure," *Probability in the Engineering and Informational Sciences*, vol. 19, no. 01, pp. 15–32, 2005.

[6] J. Chen and J. Thorp, "A reliability study of transmission system protection via a hidden failure dc load flow model," in *Power System Management and Control, 2002. Fifth International Conference on (Conf. Publ. No. 488)*. IET, 2002, pp. 384–389.

[7] P. D. H. Hines, I. Dobson, E. Cotilla-Sanchez, and M. Eppstein, ""dual graph" and "random chemistry" methods for cascading failure analysis," in *Proceedings of the 2013 46th Hawaii International Conference on System Sciences*, ser. HICSS '13. Washington, DC, USA: IEEE Computer Society, 2013, pp. 2141–2150.

[8] Y. Koç, T. Verma, N. A. Araujo, and M. Warnier, "Matcasc: A tool to analyse cascading line outages in power grids," in *Intelligent Energy Systems (IWIES), 2013 IEEE International Workshop on*. IEEE, 2013, pp. 143–148.

[9] B. A. Carreras, D. E. Newman, I. Dobson, and N. S. Degala, "Validating opa with wecc data." in *HICSS*, 2013, pp. 2197–2204.

[10] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, "Criticality in a cascading failure blackout model," *International Journal of Electrical Power & Energy Systems*, vol. 28, no. 9, pp. 627–633, 2006.

[11] Y. Jun, Z. Xiaoxin, and X. Yunan, "Model of cascading failures in power systems," in *2006 International Conference on Power System Technology*. IEEE, 2006, pp. 1–7.

[12] http://www.mathworks.com/, The mathworks, Natick, MA, USA.

[13] J. L. Blackburn and T. J. Domin, *Protective relaying: principles and applications*. CRC press, 2015.

[14] J. Roberts and A. Guzman, "Directional element design and evaluation," in *proceedings of the 21st Annual Western Protective Relay Conference, Spokane, WA*, 1994.

[15] [Online]. Available: http://www.nptel.ac.in/courses/108101039/download/lecture-15.pdf

[16] "Ieee cascading failure working group." [Online]. Available: http://sites.ieee.org/pes-cascading/presentations/