A Simulation Testbed for Cascade Analysis

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

Rishabh Jain, Srdjan Lukic
North Carolina State University,
Raleigh, NC 27606, USA
Email:{rjain5,smlukic}@ncsu.edu

***Abstract*—Electrical power systems are heavily instrumented with protection assemblies (relays and breakers) that detect anomalies and arrest failure propagation. However, failures in these discrete protection devices could have inadvertent consequences, including cascading failures resulting in blackouts. This paper aims to model the behavior of these discrete protection devices in nominal and faulty conditions and apply it towards simulation and contingency analysis of cascading failures in power transmission systems. The behavior under fault conditions are used to identify and explain conditions for blackout evolution which are not otherwise obvious. The results are demonstrated using a standard IEEE-14 Bus System.**

***Index Terms*—Behavioral Models, Blackouts, Cascading Failures, Contingency Analysis, Cyber Faults.**

I. Introduction

Electrical power systems are heavily instrumented with protection devices whose primary responsibility is to identify and isolate faulty physical components from the power system network as per deterministic protection schemes. While these devices act on local information i.e. branch power flows and bus voltages to quickly arrest the fault propagation, the lack of a system-wide perspective could lead to cascading failures. Additionally, failures or mis-operations in the protection devices (referred to *cyber faults* in this paper) can affect the nominal behavior of the relay and/or breakers and can contribute towards cascade progression leading to blackouts as seen in Aug 2003 USA [1], 2003 Italian [2] blackouts. For instance, in 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. However, presence of an additional fault in an associated protection device (stuck breaker fault in circuit breaker PA12) will lead to a cascading failure tripping all current carrying paths to the affected line. This can cause further disturbance to the system in the form of overloads and can contribute towards cascade progression. Hence it is important to understand the unintendend consequence of protection assembly failures and include these in cascading failure studies.

In order to diagnose and predict cascade evolution in a better way and to perform contingency analysis, its important for the simulation models to consider the behavior models of these discrete devices with reasonable timing accuracy. These models should be able to emulate the behavior of actual hardware in both nominal and faulty modes and allow the ability to alter the model parameters, injection of missed or spurious detection faults, modification of response delays and threshold values.

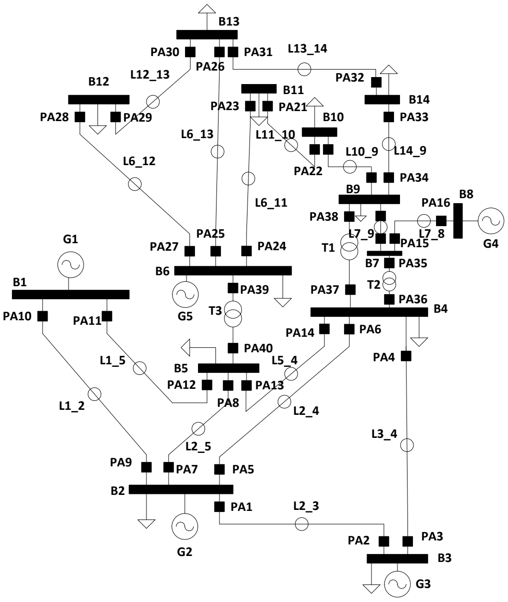


Fig. 1: IEEE 14 Bus System [3]

Existing approaches for cascading failure analysis are to perform off-line simulations to assess the current state of power system and study its evolution using different cascade simulation models [4], [5], [6], [7], [8], [9]. Models referenced in [4], [6], [7], [8], are based on initiating faults that cause line overloads leading to cascading failures in the system but they do not consider the interaction of cyber failures in protection devices. Models in [5], [9] 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 possible only in the lines which are connected to the same bus as the line outage fault. 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 cascade analysis and designing better mitigation strategies. Taking these cyber failures and time causality of events into account cascade progression will evolve in a different way, which cannot be studied based on above models but is possible via this approach.

TABLE I: Protection Assembly- Parameters Description

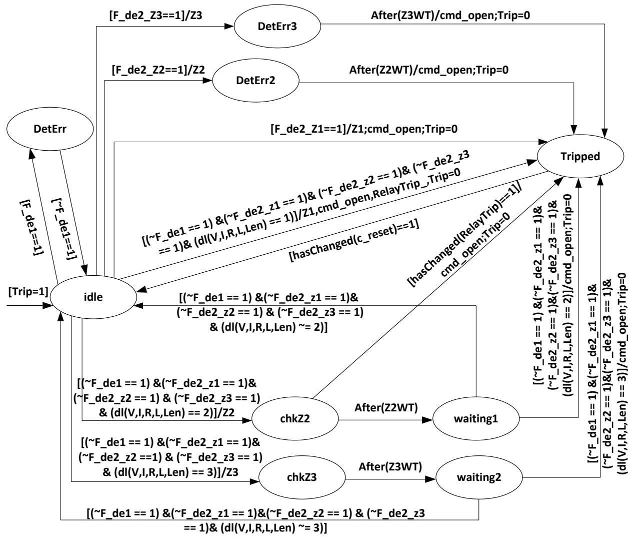
Parameter Name	Description
Distance Relay	*Common parameters for over-current relay
F_de1*/∼F_de1*	Presence/Absence of Missed Detection Fault
F_de2_zX/∼F_de2_zX (X =1,2,3)	Presence/Absence of a zone1, zone2, zone3-Spurious Detection Fault
V, I*	3 phase bus voltages and line currents
R, L, Len	Resistance, inductance and length of the transmission line
RelayTrip	POTT scheme relay trip command reception
c_reset	Resets the relay to 'idle' state
Trip*	Relay status to disconnect the branch
Z1, Z2, Z3	Presence of zone1, zone2, zone3 faults
RelayTrip_	POTT scheme relay trip command issue
cmd_open*/cmd_close*	Open/Close command to circuit breaker
ZxWT(x=2,3)	zone2, zone3 wait times
Circuit Breaker	
F_stuck_open, F_stuck_close	Presence/Absence of Stuck open and Stuck close Faults (Stuck Faults).
cmd_open/cmd_close	Open/Close command to physical breaker
PhysicalStatus	Open/Close status of physical circuit breaker
Trip	Circuit breaker Open/Close command
st_open/st_close	Open/Close status of the circuit breaker
Over-Current Relay	
F_de2_Px/∼F_de2_Px (x=1,2,3)	Presence/Absence of high, medium and low overloads-Spurious Detection Fault
P1_OL, P2_OL, P3_OL	Presence of High, Medium, Low overloads
CThres	Max. loading value of the branch
ZoneWaitTime	Wait time for the relay

The approach presented in this paper uses detailed behavioral model of the protection devices (distance relays, over current relays and breakers) in nominal and faulty modes of operation, taking into account *cyber faults* and time causality of the events. The behavioral models are used as part of a simple cascade simulation and contingency analysis framework to study the evolution of cascades in the presence of *cyber faults*. The results of such an analysis presents new new cascade evolution trajectory leading to blackout, which are otherwise not obvious. An example is shown with a case-study of IEEE 14 bus system.

The paper 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 proposes a new approach of contingency analysis that involves behavioral models. 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 devices considered as part of the protection assembly in this work include distance relays, over-current relays and circuit breakers. The relays detect the fault conditons (reduction in impedance, increase in current) and command the breaker to open. The breakers respond to the command and open the ciruit, thereby arresting the failure propagation. This nominal operation of the protection devices is affected in the presence of *cyber faults*. The behavioral models consider three types of *cyber faults* namely *Missed Detection Faults*, *Spurious Detection Faults* and *Stuck Breaker Faults*. As the names suggest, in the presence of a *Missed Detection Fault*, a relay fails to detect the anomaly. As a result, the breaker is not commaded to open and arrest the failure propagation. In case of a *Spurious Detection Fault*, a relay incorrectly reports the presence of an anomaly (under nominal conditions) and subsequently commands the breaker to open. With a *Stuck Breaker Fault*, a breaker does not operate as commanded i.e. to open or close and continue to remain in their current state.



[F_de2_Z3==1]/Z3
DetErr3
After(Z3WT)/cmd_open;Trip=0
[F_de2_Z2==1]/Z2
DetErr2
After(Z2WT)/cmd_open;Trip=0
DetErr
[F_de2_Z1==1]/Z1;cmd_open;Trip=0
Tripped
[(~F_de1 == 1) &(~F_de2_z1 == 1)& (~F_de2_z2 == 1)& (~F_de2_z3 == 1)& (dl(V,I,R,L,Len) == 1)]/Z1,cmd_open,RelayTrip_,Trip=0
[F_de1==1]
[~F_de1==1]
[hasChanged(c_reset)==1]
[hasChanged(RelayTrip)==1]/ cmd_open;Trip=0
[Trip=1]
idle
[(~F_de1 == 1) &(~F_de2_z1 == 1)& (~F_de2_z2 == 1) & (~F_de2_z3 == 1) & (dl(V,I,R,L,Len) ~= 2)]
[(~F_de1 == 1) &(~F_de2_z1 == 1)& (~F_de2_z2 == 1)&(~F_de2_z3 == 1)& (dl(V,I,R,L,Len) == 2)]/cmd_open;Trip=0
[(~F_de1 == 1) &(~F_de2_z1 == 1)& (~F_de2_z2 == 1)&(~F_de2_z3 == 1)& (dl(V,I,R,L,Len) == 3)]/cmd_open;Trip=0
[(~F_de1 == 1) &(~F_de2_z1 == 1)& (~F_de2_z2 == 1) & (~F_de2_z3 == 1) & (dl(V,I,R,L,Len) == 2)]/Z2
chkZ2
After(Z2WT)
waiting1
[(~F_de1 == 1) &(~F_de2_z1 == 1)& (~F_de2_z2 ==1) & (~F_de2_z3 == 1) & (dl(V,I,R,L,Len) == 3)]/Z3
chkZ3
After(Z3WT)
waiting2
[(~F_de1 == 1) &(~F_de2_z1 == 1)&(~F_de2_z2 == 1) & (~F_de2_z3 == 1)& (dl(V,I,R,L,Len) ~= 3)]

Fig. 2: Distance Relay Stateflow Behavioral Model.

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 [10]. Table I shows the details about the parameters used in its modeling. 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 [11].

Normal mode operation: During normal operation, the distance relay remains in 'idle' state when the load impedance seen by the relay is nominal. The load impedance seen by the relay is computed based on a simple detection algorithm (dl(V,I,R,L,Len)) referenced in [11], [12]. When the relay sees a drop in impedance (probably due to a physical fault such as three phase to ground fault in a transmission line), it transitions out of 'idle' state.

When the impedance falls in the zone1 reach, the relay transitions immediately from 'idle' to 'Tripped' state and sends a 'cmd_open' to its associated circuit breaker. However, if the impedance falls in zone2 or zone3 regions, 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.

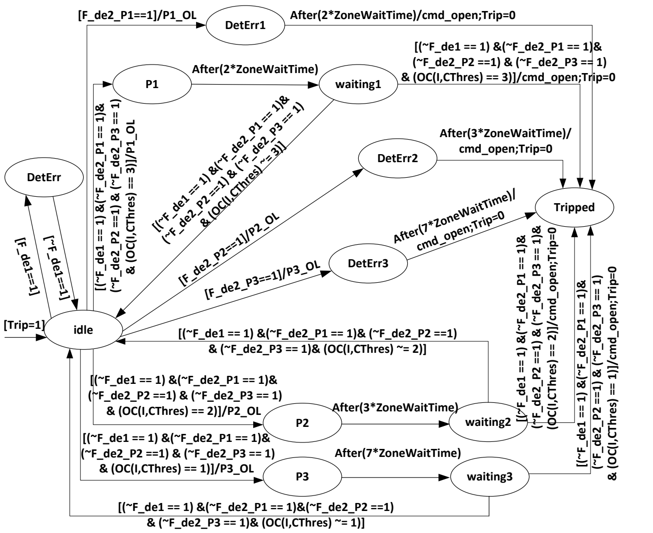

[F_de2_P1==1]/P1_OL
DetErr1
After(2*ZoneWaitTime)/cmd_open;Trip=0
P1
After(2*ZoneWaitTime)
waiting1
[(~F_de1 == 1) &(~F_de2_P1 == 1)&
(~F_de2_P2 ==1) & (~F_de2_P3 == 1)
& (OC(I,CThres) == 3)]/cmd_open;Trip=0
[(~F_de1 == 1) &(~F_de2_P1 == 1)&
(~F_de2_P2 ==1) & (~F_de2_P3 == 1)
& (OC(I,CThres) == 3)]/P1_OL
[(~F_de1 == 1) &(~F_de2_P1 == 1)&
(~F_de2_P2 ==1) & (~F_de2_P3 == 1)
& (OC(I,CThres) ~= 3)]
After(3*ZoneWaitTime)/
cmd_open;Trip=0
DetErr2
DetErr
Tripped
[F_de1==1]
[~F_de1=1]
[F_de2_P2==1]/P2_OL
After(7*ZoneWaitTime)/
cmd_open;Trip=0
[F_de2_P3==1]/P3_OL
DetErr3
[Trip=1]
idle
[(~F_de1 == 1) &(~F_de2_P1 == 1)& (~F_de2_P2 ==1)
& (~F_de2_P3 == 1)& (OC(I,CThres) ~= 2)]
[(~F_de1 == 1) &(~F_de2_P1 == 1)&
(~F_de2_P2 ==1) & (~F_de2_P3 == 1)
& (OC(I,CThres) == 2)]/P2_OL
P2
After(3*ZoneWaitTime)
waiting2
[(~F_de1 == 1) &(~F_de2_P1 == 1)&
(~F_de2_P2 ==1) & (~F_de2_P3 == 1)&
(OC(I,CThres) == 2)]/cmd_open;Trip=0
[(~F_de1 == 1) &(~F_de2_P1 == 1)&
(~F_de2_P2 ==1) & (~F_de2_P3 == 1)
& (OC(I,CThres) == 1)]/P3_OL
P3
After(7*ZoneWaitTime)
waiting3
[(~F_de1 == 1) &(~F_de2_P1 == 1)&
(~F_de2_P2 ==1) & (~F_de2_P3 == 1)
& (OC(I,CThres) == 1)]/cmd_open;Trip=0
[(~F_de1 == 1) &(~F_de2_P1 == 1)&(~F_de2_P2 ==1)
& (~F_de2_P3 == 1)& (OC(I,CThres) ~= 1)]

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

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 in electrical power systems. Its behavioral model is shown in Figure 3 and parameters used for modeling are listed in Table I. 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' (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.

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 [13]. Being in one of the 'Px' states, the relay transitions to its 'waitingX' (X =1 to 3) state after the wait time associated with the overload elapses. If overload 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 of *Spurious Detection Fault* and *Missed Detection Fault*, the over-current relay behavior is similar to the distance relay.

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 'closed' state. However, if it receives a 'cmd_open', the circuit breaker transitions from 'closed' state to the 'opening' state. Circuit breaker being a mechanical device takes time to open/close. Hence, we introduced a delay in the opening/closing operations of the circuit breaker for more realistic behavior. This delay is provided by the variables tto/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'. Similar transitions takes place if the circuit breaker receives a 'cmd_close' while being in the 'open' state.

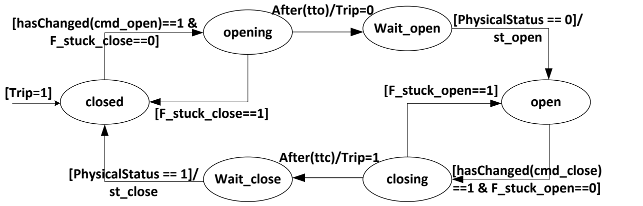


Fig. 4: Circuit Breaker Stateflow Behavioral Model.

Operation under cyber faults: If the circuit breaker is in 'closed' state and there is a *Stuck Close Fault* then it remains in the 'closed' state. However, if the same fault occurs while the circuit breaker is in the 'opening' state then it transitions back to the 'closed' state. Similar behavior is observed for the *Stuck Open Fault* as shown in Figure 4.

III. Towards Contingency 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 failure. Tools such as MATCASC [7], CASCADE model [4] perform cascade analysis but they do not consider details about the time between contingencies and cyber faults in the protection equipments.

In our simulation and contingency analysis framework, we integrate the power transmission system simulation models in Matlab/ Simulink with detailed behavioral models of protection assembly. In the phasor mode of simulation, we are able to capture the time between occurrences of different events in a contingency and also trigger cyber fault(s) in specific protection devices at specified time(s). The analysis allows us to identify contingencies which can possibly result in severe cascading outages or blackouts.

The proposed contingency analysis model is shown in Figure 5(a). The inputs to the analysis framework include the initial components outage (k-components outage) set, cascade simulation model and the protection assembly blocks. The initial component outage set is a initial list of components that are supposed to fail or have faults. An initial contingency can be a combination of physical and cyber faults. The protection assembly blocks will contain information about the cyber faults based on the initial component outage set. A simscape model (described later) of the power transmission system is executed taking into account the faults associated with the initial contingency set and the simulation is executed to evaluate the cascade progression through cascade simulation model. This simulation model is based on a simple cascade progression algorithm as shown in Figure 5(b). After the initial contingency, the system is checked for overloads and if it exists, the overloaded branches (transmission lines and transformers) are identified and tripped. The simulation is repeated to identify and trip new sets of overloaded branches. The process is repeated until there are no more overloads to trip or a blackout criteria is reached. 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'. Currently, amount of load loss is considered as the blackout criteria in this model as referenced in [14] but it can be extended by taking into account other blackout criterion as well. At the end of the contingency analysis, a N-k ($k \in \mathbb{N}$) contingency set that can cause blackouts is identified and reported. The N-k contingency set contains the individual combinations of those initial component outages which can lead to a blackout.

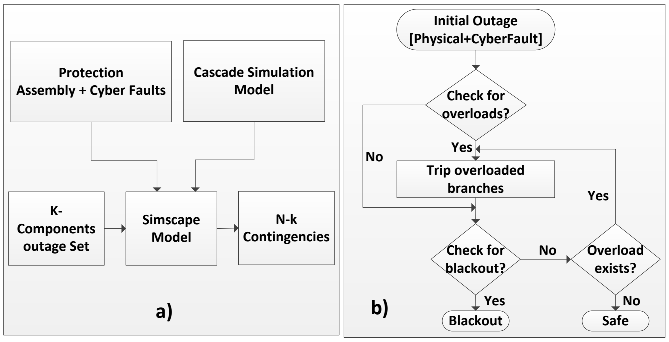


Fig. 5: a) Contingency Analysis Model b) Cascade Flowchart

The cascade analysis framework also has a feature of introducing random outages at specific times during the simulation. This could be of interest as it could reveal different cascade evolution trajectory and possible blackouts due to changes in system topology. Also, the same outage when triggered at different times during the progression can contribute in finding those specific points where it is highly disruptive. This type of analysis is not possible with tools where outage can be specified only as part of the initial outage set. In our tool set, currently the random injection of faults is triggered manually. Automating it is left for future work.

IV. System Under test and Experimental Setup

The proposed contingency analysis has been performed on an exemplar IEEE-14 Bus System [3] shown in Figure 1. The base voltage is 138 kV and length of each line is 16 km. The system is modeled in Matlab/Simscape using Simscape library blocks. Figure 6 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.

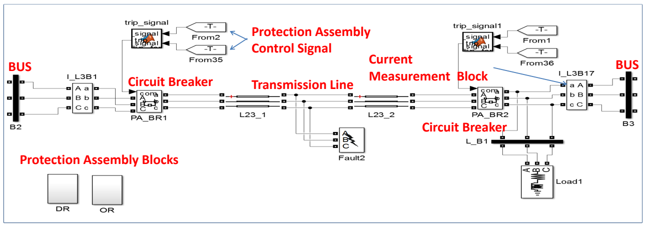


Fig. 6: Portion of IEEE-14 Bus System- Simscape Model

As shown in Figure 6, 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 6). 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.

V. Results

The study is done on IEEE-14 bus system assuming that the lines are loaded at 70% of their loading capacity. It shows, how presence of cyber fault along with physical fault can lead to severe cascading failures causing blackouts and how it can be used in finding N-k contingencies which are otherwise not obvious.

Case 1: At time t=0.5 sec, an initial contingency (a three phase to ground fault) occurs in the transmission line 'L3_4'(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 circuit breakers ('PA_BR3', 'PA_BR4'). In the absence of any cyber fault, outage of transmission line 'L3_4' did not cause any further contingency and the system remained stable.

Case 2: The fault scenario in case 1 is repeated. A cyber fault (*Stuck close Fault*) is introduced in circuit breaker ('PA_BR4') of protection assembly PA4 (in Figure 1) in addition to the physical fault in line 'L3_4' at time t=0.5 sec. As a result of these initial faults, it is observed that a number of transmission lines gets overloaded and are eventually tripped and removed from the network. At time t=2 sec, another cyber fault (*Spurious Detection Fault*) occurred in the distance relay ('PA_DR27') of protection assembly PA27 in transmission line 'L6_12' (in Figure 1). This leads to overloading in other transmission lines, which gets tripped in the process.

TABLE II: Sequence of cascading events

Time(sec)	Event Description
0.500	**F:** 3ϕ-G fault- Line L3_4, Stuck close fault- PA_BR4.
0.501	**D:** Z1, Z3 in PA_DR{3,4}, PA_DR1, 'P1_OL' in PA_OR3, 'P2_OL' in PA_OR{5,1,13}, 'P3_OL' in PA_OR{9,15,21}. **CR:** 'cmd_open' in PA_BR3.
0.532	**S:** st_open-PA_BR3 is opened. **L:** Line L3_4 tripped partially.
2.000	**F:** Spurious detection fault in PA_DR27. **CS/CR:** 'cmd_open' in PA_DR27/PA_BR27.
2.031	**S:** 'st_open'-PA_BR27 is opened. **L:** Line L6_12 is removed.
3.503	**D:** 'P2_OL' in PA_OR13. **CS/CR:** 'cmd_open' in PA_OR{5,21}/PA_BR{5,21}.
3.534	**D:** 'P2_OL' in PA_OR31. **S:** 'st_open'- PA_BR{5,21} are opened. **L:** Lines L2_4, L11_10 removed.
5.505	**CS/CR:** 'cmd_open' in PA_OR13/PA_BR13.
5.536	**D:** 'P1_OL' in PA_OR{25,33}, 'P2_OL' in PA_OR {35,40}, 'P3_OL' in PA_OR{29,37}. **S:** 'st_open'-PA_BR13 is opened. **L:** Line L5_4 is disconnected.
6.536	**D:** 'P1_OL' in PA_OR31.
7.503	**CS/CR:** 'cmd_open' in PA_OR15/PA_BR15.
7.534	**S:** 'st_open'-PA_BR15 is opened. **L:** Line L7_8 is removed.
7.538	**CS/CR:** 'cmd_open' in PA_OR{25,33}/PA_BR{25,33}.
7.569	**D:** 'P3_OL' in PA_OR1. **S:** 'st_open'- PA_BR{25,33} are opened. **L:** Lines L6_13, L14_9 are removed.
14.571	**CS/CR:** 'cmd_open' in PA_OR1/PA_BR1.
14.602	**S:** 'st_open'- PA_BR1 is opened. **L:** Line L2_3 is tripped.

F: Occurrence of fault events, **D:** Detection of zone faults and overloads, **CS/CR:** Send/Receive commands from relays to circuit breakers, **S:** Status of the circuit breakers, **L:** Outage of lines.

Occurrence of each contingency event and its impact on the system is described in detail in Table II. It shows the progression of cascade 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. This is because they do not have a current carrying path through them due to line outages listed in Table II. These events eventually resulted in a load loss of 46.9% and hence caused a blackout based on the criteria referenced in [14]. Due to this, the initial contingency can be marked as a blackout causing contingency. Similar contingencies can be found based on this approach which could lead to severe cascading outages in electrical power transmission systems. Prior knowledge of such contingencies can help in designing effective mitigation strategies, which could prevent the progression of cascades.

In order to validate the generated cascade progression paths, an independent study is performed using a different simulation platform, OpenDSS [15]. WSCC 9 bus system [16] is used as the example system. The results of contingency analysis matched for all but three cases. The 3 cases where the contingency analysis results did not match can be attributed to the different solvers resulting in about $\sim$ 3% difference in the voltages and currents magnitudes computed in the two platforms.

VI. Conclusion

In this paper 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. The study on IEEE 14 bus system showed how introduction of cyber faults in addition to physical fault can lead to severe cascading failures causing blackout. 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. As part of the future work, more complex models need to be analyzed and the entire approach can be automated so as to find severe N-k contingencies that can result from a combination of physical and cyber faults.

Acknowledgment

This work is funded in part by the National Science Foundation under the award number CNS-1329803.

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)." [Online]. Available: http://icseg.iti.illinois.edu/ieee-14-bus-system/

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

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

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

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

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

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

[15] O. P. Model and O. S. Element, "Opendss manual," *EPRI,[Online] Available at: http://sourceforge. net/apps/mediawiki/electricdss/index. php.*

[16] ICSEG, "Illinois center for a smarter electric grid(icseg)." [Online]. Available: http://http://icseg.iti.illinois.edu/wscc-9-bus-system/