

Temporal Causal Diagrams for Diagnosing Failures in Cyber-Physical Systems

Nagabhushan Mahadevan¹, Abhishek Dubey¹, Gabor Karsai¹, Anurag Srivastava², and Chen-Ching Liu²

¹ *Institute for Software-Integrated Systems, Vanderbilt University, Nashville, TN 37212, USA*
nag,dabhishe,gabor@isis.vanderbilt.edu

² *The School Of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99163, USA*
asrivast,liu@eecs.wsu.edu

ABSTRACT

Resilient and reliable operation of cyber physical systems of societal importance such as Smart Electric Grids is one of the top national priorities. Due to their critical nature, these systems are equipped with fast-acting, local protection mechanisms. However, commonly misguided protection actions together with system dynamics can lead to un-intentional cascading effects. This paper describes the ongoing work using Temporal Causal Diagrams (TCD), a refinement of the Timed Failure Propagation Graphs (TFPG), to diagnose problems associated with the power transmission lines protected by a combination of relays and breakers.

The TCD models represent the faults and their propagation as TFPG, the nominal and faulty behavior of components (including local, discrete controllers and protection devices) as Timed Discrete Event Systems (TDES), and capture the cumulative and cascading effects of these interactions. The TCD diagnosis engine includes an extended TFPG-like reasoner which in addition to observing the alarms and mode changes (as the TFPG), monitors the event traces (that correspond to the behavioral aspects of the model) to generate hypotheses that consistently explain all the observations. In this paper, we show the results of applying the TCD to a segment of a power transmission system that is protected by distance relays and breakers.

1. INTRODUCTION

Cyber-Physical Systems (CPS) such as the Smart Electric Grids are going through transformational reform powered by federal funding and in line with the stated national energy security mission goals (Garrity, 2008). These systems work in dynamic environments resulting from varying load, changing

operational requirements and conditions, physical component degradation, and software failures. To reach the required level of resiliency and reliability, efficient online management of CPS is necessary to operate safely within specified parameters, even in the presence of faults (Ilic et al., 2005). One aspect of online management is fault identification, diagnostics, prognostication, and mitigation. Inability to automatically and timely diagnose and pinpoint the source(s) of failures combined with the potential side-effects of automated protection actions lead to impending fault cascades, which can be avoided (Zhang, Ilic, & Tonguz, 2011; Tholomier, Richards, & Apostolov, 2007). Recent blackouts and hurricane Sandy in 2012 demonstrated the grid vulnerability and reasons to look at existing defense mechanism more closely.

Fast acting localized protection mechanisms are used arrest the propagation of failure effects. Electrical protection systems include detection devices such as fast-acting relays that are designed to detect abnormal changes in physical properties (current, voltage, impedance) and actuation devices such as breakers that can be triggered to open the circuit in electrical networks. To observe, track, and possibly diagnose these systems, it is important to consider the discrete and continuous dynamics of the physical system, the protection systems and their interactions both in the nominal and faulty modes of operations. During nominal (fault-free) operation, both physical and protection systems should operate nominally to provide the desired functionality. If a fault appears in the physical system, the nominal protection system is expected to detect the failure effect and isolate the faulty part of the system. In some cases, the nominal protection system is assisted by a set of algorithms to restore the system functionality to its original configuration once the physical fault disappears (due to a temporary fault or after repair).

Operators have to consider the possibilities of misoperations of protection systems. Distance relays have been known to incorrectly initiate tripping due to an apparent impedance that

Nagabhushan Mahadevan et al. This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 United States License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

fall into the Zone settings of line relays caused by heavy load and depressed voltage conditions (Pourbeik, Kundur, & Taylor, 2006). In fact, an investigation by North Electric Reliability Corporation (NERC) demonstrated that nearly all major system events, excluding those caused by severe weather, have had relay or automatic control misoperations (almost 2,000 in one year) contributing to worsening the impact of failure propagation (North American Electric Reliability Corporation, 2012). Protection malfunction and its correlation with major blackouts require a careful rethinking of its system-wide effects (Zhang et al., 2011; Pourbeik et al., 2006).

This paper describes Temporal Causal Diagrams (TCD), a refinement of the Timed Failure Propagation Graphs (TFPG) (Abdelwahed, Karsai, Mahadevan, & Ofsthun, 2009), to diagnose failures of physical systems that are instrumented with multiple local fast acting protection devices and controllers to isolate the faults. The TCD is a discrete abstraction that captures the causal and temporal relationships between failure modes (causes) and discrepancies (effects) in a system, thereby modeling the failure cascades taking into account propagation constraints imposed by operating modes, protection elements, and timing delays. Faults and their propagation are captured using TFPG models, the nominal and faulty operations of the components (controllers, protection devices etc.) are captured as Timed Discrete Event Systems (TDES). We also present a diagnosis reasoner that extends the TFPG diagnosis algorithm considering both the alarms and mode changes (as reported by the physical system), as well as the various event traces corresponding to the behavioral aspects of the mode. The uniqueness of the approach is that it does not involve complex real-time computations involving high-fidelity models, but performs reasoning using efficient graph algorithms based on the observation of various anomalies and events in the system. When fine-grained results are needed and computing resources and time are available, the diagnostic hypotheses can be refined with the help of the physics-based diagnostics.

The paper is organized as follows. The next section (Section 2) deals with the related research. Section 3 that describes the temporal causal diagrams. Section 4 documents the results of applying the solution to various fault scenarios in a power transmission system and Section 5 concludes the paper with a discussion of the future work. Notations used and an overview of Timed Failure Propagation Graphs (TFPG) are described in appendices.

2. RELATED RESEARCH

Fault diagnostics has been recognized as a critical task in electric grid operations (Coster, Myrzik, Kruimer, & Kling, 2011). A classic but excellent summary of power system fault diagnostics is provided in (Sekine, Akimoto, Kunugi, Fukui, & Fukui, 2002), including Bayesian approaches (Mengshoel

et al., 2010; Yongli, Limin, & Jinling, 2006), rule-based reasoning (Meléndez et al., 2004; Lee et al., 2004), expert systems (Talukdar, Cardozo, & Perry, 2007; Yang, Okamoto, Yokoyama, & Sekine, 1992), fuzzy-logic methods (W. Chen, Liu, & Tsai, 2000; Sun, Qin, & Song, 2004), Genetic Algorithm, search based techniques (Lin, Ke, Li, Weng, & Han, 2010), artificial neural network (Guo et al., 2010; Zhou, 1993), and Petri Nets by abstracting the power system as a discrete event system (Sun et al., 2004) (Ren, Mi, Zhao, & Yang, 2005). Problems similar to large electric system operations also occur in smaller systems such as Electric Ship (Bastos, Zhang, Srivastava, & Schulz, 2007) and Spacecraft (Poll et al., 2007; Daigle et al., 2010).

A pioneering paper (Fukui & Kawakami, 1986) reports a rule-based or logic-based system for location of line faults based on real time information acquired at the control center of a power system. (Sekine et al., 2002) compiled a comprehensive survey of the fault diagnostics systems developed using various knowledge-based system techniques. Model-based approaches based on logic behaviors of the protection devices are identified as valuable tools for fault analysis. The on-line alarm analyzer reported in (Miao, Sforna, & Liu, 1996) incorporates the cause-effect principles of protective devices into logic-based proof-oriented algorithms for the analysis of malfunctions. Cause-effect models are used for fault diagnostics of substations in (W.-H. Chen, Liu, & Tsai, 2000). Upon field-testing with real world data it was found that the proofs are difficult when uncertainties cannot be resolved. The proof algorithm in (Miao et al., 1996) had to be generalized in order to evaluate the credibility of potentially large number of hypotheses (W.-H. Chen et al., 2000).

The approach described in this paper differs from existing practice where fault analysis and mitigation relies on a logic-based approach that relies on hard thresholds and local information assisted by manual system level analysis. The causal model presented in this paper is based on the timed failure propagation graph (TFPG) introduced in (Misra, 1994; Misra, Sztipanovits, & Carnes, 1994), which is conceptually related to the temporal causal network approach presented in (Console & Torasso, 1991; Padalkar, Sztipanovits, Karsai, Miyasaka, & Okuda, 1991; Karsai, Sztipanovits, Padalkar, & Biegl, 1992; Mosterman & Biswas, 1999). The TFPG model was extended in (Abdelwahed, Karsai, & Biswas, 2004) to include mode dependency constraints on the propagation links, which can then be used to handle failure scenarios in hybrid and switching systems.

We have extended this work to be able to take local mitigation in a subsystem, especially in case of malfunction of protection devices results in a larger fault cascade, leading to a blackout into consideration. This is primarily done by considering the discrete behavior of the protection devices and using it in the diagnosis. The problem of fault diagnosis in discrete

event systems has been extensively studied. According to (Sampath, Sengupta, Lafortune, Sinnamohideen, & Teneketzi, 1996), the fault diagnosis problem can be described in terms of a description of a plant's behavior in the form of a finite automaton. Any behavior of the plant can be represented as a run of this automaton, i.e. a sequence of events. These events can be either *observable* or *unobservable*. If the fault event is observable then the diagnosis problem is trivial. However, usually one or more unobservable events correspond to the occurrence of a fault that may occur in the plant operation. The objective is to find a diagnoser that can detect the occurrence of a fault event within a bounded number of steps from the occurrence. However, we need to consider the possibility of timed failure propagation and faults in the controllers as well as plant.

Our approach can improve the effectiveness of isolating failures in large-scale systems such as Smart Electric Grids, by identifying impending failure propagations and determining the time to critical failure, which increases the system reliability and reduce the losses accrued due to power failures.

3. TEMPORAL CAUSAL DIAGRAMS

A Temporal Causal Diagram is a behavior augmented temporal failure propagation graph model. The TCD model of a component can describe the fault propagation and/or the behavior. The failure propagation is described in terms of Timed Failure Propagation Graphs (TFPG)¹. The component behavior under nominal and faulty conditions is captured through Timed Discrete Event Systems (TDES). A TDES is characterized as follows:

- Q : The set of discrete states of the component
- F : The set of failure modes internal to the component. As always, failures modes are not directly observable.
- D : The set of discrepancies, i.e. potentially observable anomalies, if any, associated with the component behavior. The discrepancy can be detected, or triggered by the component, or affect the component behavior.
- Σ : The set of events that correspond to controller commands, actuation, external mode commands, detection of the physical state of component, discrepancy detection or other internal events. The detection of a discrepancy, d , is written as $d\uparrow$, while $d\downarrow$ relates to the remission of a discrepancy.
- A mode map, $\mathbb{M} : Q \rightarrow 2^M$ captures the effect of a state in Q on the TFPG-mode in M . Thus, the system being in a discrete state affects the current modes of the TFPG, which in turn affects the propagation link.
- δ is the transition map. The transitions are written as $[Guard]Event(delay)/Actions$. The *Guard* condition can represent the presence of a local fault $f \in F$, written as $in(f)$ and absence of it, written as $!in(f)$. Note that

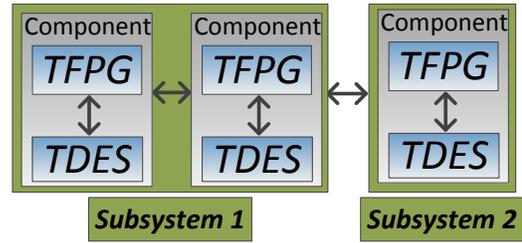


Figure 1. A TCD model of a system consists of interacting subsystems containing components, where each component consists of an interacting TFPG and TDES model.

for brevity, unless specifically required we will use the shorthand f and $!f$ in the guard conditions. *Actions* result in production of events that can be communicated to the rest of the system, and/or change the mode of the system. *delay*, if present declares that the transition will occur after the timeout. The rising edge of the event is described by appending the uparrow \uparrow to event. The falling edge of the event is shown using the downarrow \downarrow .

Figure 1 provides an overview of the TCD model of a system. The TCD model is hierarchical where a system model is composed of subsystem models which in themselves are composed of component models. The component model includes TFPG and/or TDES models. The TCD model captures the interactions between the TFPG and TDES models both within the component, as well as across component boundaries. The interactions between the TFPG and TDES models are captured implicitly through the state changes in the common modeling elements in the two models - failure modes, discrepancies, and modes. The behavioral model can be designed to consume and react to the updates of these common elements in the form of events (appearance, disappearance, change) and conditions (presence, absence). Likewise, the behavioral model can be designed to update these common elements that can be consumed by the failure propagation model. The cascading failure propagation effects across component boundaries is captured explicitly (as in TFPG) through failure propagation links between the discrepancy elements in each component. Interactions between the behavior models are based on the event generation and consumption paradigm. A TDES component can consume events corresponding to commands, detection, and mode changes generated by one or more component TDES models. It can also generate similar events to be consumed by other component TDES models.

Example 1 An example illustrative TCD model is shown in the Figure 2. The failure modes ($F1, F2, F3$) are shown as rectangular blocks and the discrepancies ($D1, D2, D3, D4, D5, D6$) as circular elements. The fault propagation across the TFPG model is captured by the edges between the faults and the discrepancies. The markers ($M1, M2$) on the edges

¹See appendix A for an overview on TFPG

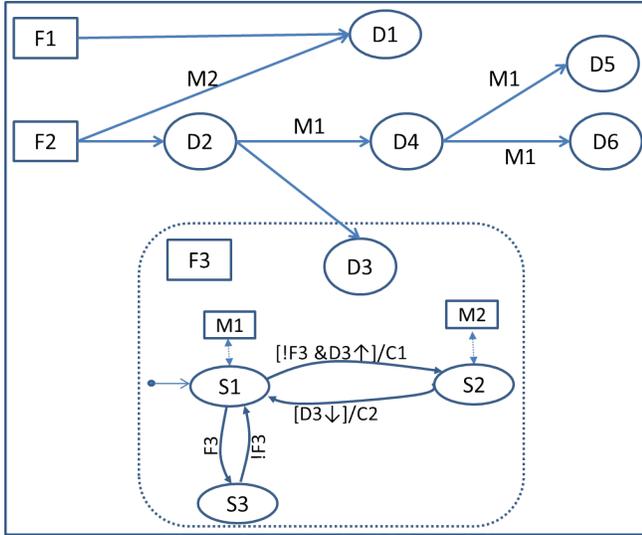


Figure 2. Example TCD model

capture the mode in which the fault could propagate via the edge. Edges that do not carry any mode marker are always enabled implying the faults can propagate in any mode (M1 or M2) across these edges.

The dotted-box captures a behavioral TDES model of a protection element. It captures three operational states: S1, S2, and S3. S1 is the initial state which maps to system mode M1. The protection element transitions from state S1 to S2 when it detects the presence of a discrepancy D3 and the fault F3 is not present (guard condition: $!F3 \& D3 \uparrow$) and issues a command (event) C1. The state transition results in a mode change to M2. This nominal operation of the protection element arrests the propagation of the failure effect due to fault F2, thereby preventing the anomalies related to discrepancies D4, D5, D6 from triggering in the system. However, it could happen that the anomaly related to discrepancy D1 is observed in the system.

Also, the TDES model shows that when the protection element detects the absence of the discrepancy D3 (transition: $D3 \downarrow$), it issues a command C2 (event) and transitions back to the state S1 (and restores the system mode back to M1). If the fault F2 were to reappear and trigger discrepancy D3, the protection element would react again to arrest the fault propagation.

Fault F3 captures an internal fault in the protection element with regards to detecting the presence of D3. The TDES model captures this as the protection element transitioning into state S3. When the fault F3 disappears, the protection element is automatically restored to the nominal state S1. However, when in S3 the protection element cannot react to the presence of the discrepancy D3 and hence cannot arrest the fault propagation leading to the triggering of anomalies related to discrepancies D4, D5, and D6.

3.1. Event Propagation Paths from the Behavioral Model

The TDES models in TCD are used to generate event propagation paths. An event propagation path is generated for each transition and state when the transition parameters (trigger, guard, action) or state parameters (entry/ exit/ during actions) include event variables that belong to any of the following categories: failure mode, discrepancy, or observable events: detection, command, and actuation. When these variables are present in the event and/ or guard condition, they are treated as (causal) source nodes of the event propagation path. When they are present in the transition actions and state actions (entry/during), they are treated as the destination (effect) nodes. The modes appear as source (destination) nodes, if they are mapped to the source (destination) state in the TDES model. Additional nodes in the event propagation path include composition nodes (*AND* and *OR*) that relate/combine the cause(s) (source nodes) and effect(s) (destination nodes), as well as *NOT* nodes that are used to mark absence or disappearance of faults (i.e. failure modes). Multiple event propagation paths can be chained together by tracing the state-transition model in the TDES and ignoring the internal, unobservable states and events.

Example 2 Event propagation paths for the protection element TDES model in Figure 2 are

- (a) $M1, !F3, D3 \uparrow \rightarrow C1, M2$, (b) $M2, D3 \downarrow \rightarrow C2, M1$, and (c) $M1, F3 \rightarrow \emptyset (NoObs)$.

3.2. Reasoning using TCD

The TCD reasoning algorithm relies on the fault propagation model (TFPG) and the event propagation models (generated from the TDES) to hypothesize the possible causes for the anomalies and event traces observed in the system. The algorithm tries to explain the observations in terms of a consistency relationship between the states of the nodes and edges in the fault propagation and event propagation model.

The TCD reasoning algorithm considers the *physical*, *observed* and *hypothetical* states of the nodes and edges in the fault propagation and event propagation model. A *physical* state corresponds to the current state of the set (V) of all the nodes and edges. At any time t , the physical state of the nodes and edges is given by a map $AS_t : V \rightarrow \{ON, OFF\} \times \mathbb{R}$. An ON state for a fault node indicates that the failure is present, otherwise it is set to OFF. For a discrepancy node, an ON state indicates that the failure (effect) has reached this node, otherwise it is set to OFF. An ON state for a failure propagation edge indicates that the edge can carry the failure (effect) from the parent to the child node, otherwise it is set to OFF. For the non-failure nodes from the event propagation models, an ON state indicates that the associated *event-variable* or *mode-variable* is set to the state represented by that node, otherwise the state is OFF.

The *observed state* at time t is defined as a map $S_t : V \rightarrow$

Algorithm 1 TCD Reasoner Update

```

1: INPUTS:  $t, HS_{t-1}, O_t$ .
2:  $HS_t = UpdateHypo(t, HS_{t-1})$ 
3: if  $O_t \neq \emptyset$  then
4:    $HS'_t = HS_t$ 
5:    $HS_t = \emptyset$ 
6:   for all  $H \in HS'_t$  do
7:     if  $Consis(H, O_t)$  then
8:        $HS_t \leftarrow HS_t \cup \{H\}$ 
9:     end if
10:  end for
11:  if  $HS_t \neq \emptyset$  then
12:    for all  $H \in HS'_t$  do
13:       $HS_t \leftarrow HS_t \cup ExplainHypo(H, O_t)$ 
14:    end for
15:  end if
16: end if
17: return  $HS_t$ 

```

$\{ON, OFF\} \times \mathbb{R}$, for all the observable nodes in the fault and event propagation model. The aim of the TCD reasoning process is to find a consistent and plausible explanation of the current system *physical* state based on the *observed* state. Such explanation is given in the form of a valid hypothetical state. A *hypothetical state* is a map that defines the states of the node (and edges) and the interval at which each node (and edges) changes its state. Formally a hypothetical state at time t is a map $H_t^{V'} : V' \rightarrow \{ON, OFF, UNKNOWN\} \times \mathbb{R} \times \mathbb{R}$ where $V' \subseteq V$.

A reasoner hypothesis is an estimate of the current state of all nodes in the system and the time period at which each node changed its state. An estimate of the current state is valid only if it is consistent with the TCD model. State consistency in TCD model is a node-parent relationship that can be extended pairwise to arbitrary subsets of nodes. The TCD reasoner uses the consistency relationships defined in (Abdelwahed et al., 2004; Abdelwahed, Karsai, & Biswas, 2005) (between the TFPG nodes and edges) for all the nodes and edges in the TCD model, i.e. it extends the consistency relationship to the non-fault nodes in the event propagation model as well. At any time, t , during the reasoning process, the TCD reasoner uses the Algorithm 1 to update the hypotheses based on the current set of observations. Algorithm 1 uses extended versions of the concepts and algorithms defined in (Abdelwahed et al., 2004, 2005) to account for event propagation and consistency in event nodes. The additional procedures invoked by the algorithm are briefly described in the appendix A.

Inputs to the TCD Diagnosis Algorithm 1 include the current time, t , the prior hypotheses set, HS_{t-1} , and the current alarm and event observations, O_t . The diagnosis algorithm (1) returns a set hypotheses that can consistently explain the current observed state of the TCD system. The algorithm starts by updating the existing hypotheses (HS_{t-1}) to the current time HS_t (line #2). Then, it identifies the set of hypotheses that can consistently explain the current alarm and event observations (lines #4-#9). In case none of the hy-

potheses are consistent with the observations, the algorithm generates new hypotheses from each of the old hypothesis to explain the current observations (lines #10 - #16). Across each update, the TCD reasoner keeps a score of the number of consistent, inconsistent, missing, and pending observations for each hypothesis and generates metrics (described later) to identify the best possible explanation, i.e. hypothesis.

Hypotheses Ranking

The quality of the generated hypotheses is measured based on three independent factors: (a) *Plausibility* is a measure of the degree to which a given hypothesis group explains the current fault and event signature. (b) *Robustness* is a measure of the degree to which a given hypothesis is expected to remain constant. (c) *#FM* is a measure of how many failure modes are listed by the hypothesis. The reasoner prefers parsimony principle (minimal number of failure modes) to report results. (d) *Failure rate* is a measure of how often a particular failure mode will occur. In case of multiple failures, the failure rates of failure modes are combined assuming independence.

3.3. Reasoner improvements

The improvements and updates in the TCD reasoning process over the TFPG reasoner include: (a) Observation evolution, i.e. tolerating the evolution or change in the *observed* state of the nodes. (b) Internal mode changes, i.e. accounting for mode changes that are not externally controlled but introduced by the dynamics of the protection systems. The mode change could be unobservable, but inferred based on other observations. (c) Fault negation, i.e. accounting for disappearance or absence of one or more faults based on certain observations.

Handling changes in the observations

In case of the TFPG reasoner, the *observed* state of a discrepancy node is either considered latched or intermittent (due to the nature of the fault or problems in the sensor). However in TCD, the dynamics of the protection system might prevent a certain failure propagation and hence result in an apparently consistent change to the *observed* state of an alarm (or discrepancy). It is also possible that the both appearance and disappearance of a fault can be accounted for when the *observed* state of the discrepancy is allowed to change. More importantly, since the protection systems are actively trying to arrest the failure effect propagation and also respond to the disappearance of faults, it is possible that the *observed* state of the non-fault event nodes could be updated over time based on the behavioral model of the protection system. If the events are observable, then the TCD reasoner updates the *hypothetical* states to be consistent with the update *observed* state of the fault and non-fault nodes. In the TCD example shown in Figure 2, it is possible that when the fault F2 happens, the

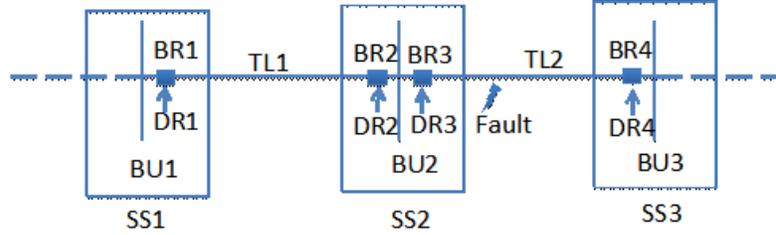


Figure 3. Segment of a Power Transmission System

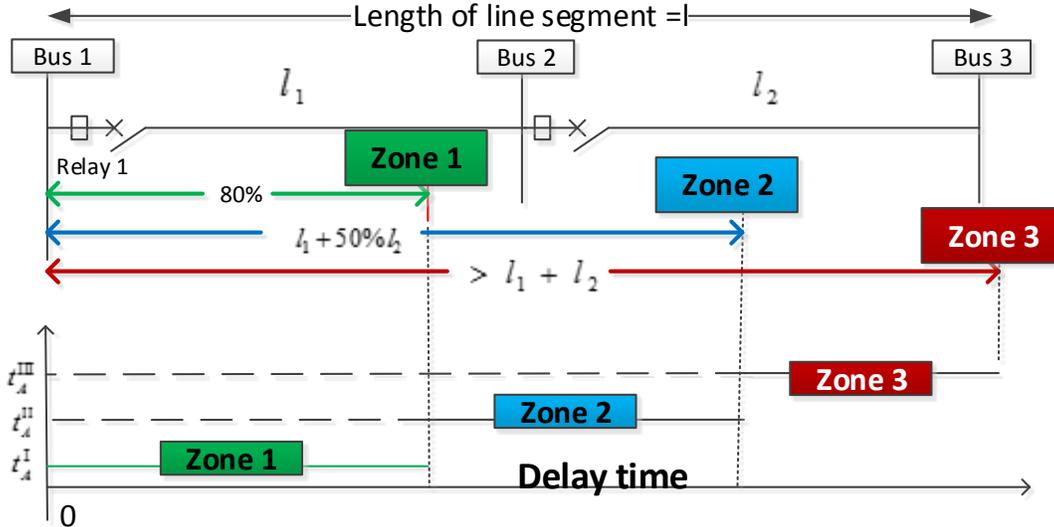


Figure 4. Protection Zone Configuration for Distance Relay. Zone 1 is set to protect 80% of the entire length of the line, and operates immediately (t_A^I) if the fault falls in the zone 1 protection region. Zone 2 is set to protect 100% of the entire line length plus at 50% of the adjacent line, and operates with time delay, t_A^{II} , 15-30 cycles. (0.5s). Zone 3 is set to protect 100% of the entire line length plus at 100% of the adjacent line, and operates with time delay, t_A^{III} (1.5s)

anomalies D4, D5, D6 could have triggered because the system was in mode M1. However, once the protection system completes its operation and the mode is changed to M2, the anomalies related to D4, D5, D6 should not be observable or detectable (based on the model). The TCD reasoner can account for this by changing the *hypothetical* states of these nodes to UNKNOWN. Further, later on if the mode is restored to M1 when D3 disappears (!D3), the reasoner can account for disappearance (or lack of observation) of D2, D4, D5 and D6. This is done by applying the consistency relationship to update the *hypothetical* state of fault F2, discrepancy D2, D4, D5, and D6 to OFF.

Mode changes introduced by protection system

The protection and control systems are actively involved in changing the mode of the physical system to arrest the fault propagation. The TCD reasoning algorithm accounts for this by allowing for a *hypothetical* state for each mode. The *hypothetical* state of the mode is updated based on other observations and the consistency relationship between the *hypothetical* states of the mode with other TCD nodes. The reasoning

algorithm updates the expected *hypothetical* states of other nodes if the *hypothetical* state of the mode changes. In the TCD example shown in Figure 2, the TCD reasoner updates the *hypothetical* states based on the mode changes introduced by the protection system. In case the mode is changed to M2 upon appearance of the fault F1, the updated *hypothetical* state for D1 can consistently explain any observation of anomaly related to D1. In case, the protection system fault F3 is present, then the lack of any observation (NULL) from the protection system and observations of discrepancy D4, D5, D6 would suggest that the system is still in mode M1 and the protection system has failed to act because of fault, F3.

Fault negation

The TCD reasoning algorithm can generate hypotheses that state that one or more faults are not present in the system. This is possible if the TDES model (and hence the event propagation model) includes specific conditions that state certain events can happen only if the fault is not present. The event propagation model accounts for the negated fault, and updates the hypothesis appropriately if the concerned events are ob-

Table 1. Fault Propagation: The faults in the transmission lines are categorized based on the segment where they occur along the length(L) of the line (from left to right) - F₂₀: [0, 0.2L), F₅₀: [0.2L, 0.5L), F₈₀: [0.5L, 0.8L), F₁₀₀: [0.8L, 1.0L), where L is the length of the transmission line. The row in the table should be read as described for the first row: A fault F₂₀ in transmission line TL1 will lead to a zone 1 fault (d.z1) in DR1, a zone 2 fault (d.z2) in DR2 and a zone 3 fault (d.z3) in DR3.

| Source Node (Transmission Line. Failure Mode) | Destination Node (Relay.zone) | Mode |
|---|----------------------------------|---------|
| TL1.F ₂₀ | DR1.d.z1, DR2.d.z2, DR4.d.z3 | M.Close |
| TL1.F ₅₀ | DR1.d.z1, DR2.d.z1, DR4.d.z3 | M.Close |
| TL1.F ₈₀ | DR1.d.z1, DR2.d.z1, DR4.d.z2 | M.Close |
| TL1.F ₁₀₀ | DR1.d.z2, DR2.d.z1, DR4.d.z2 | M.Close |
| TL2.F ₂₀ | DR1.d.z2, DR3.d.z1, DR4.d.z2 | M.Close |
| TL2.F ₅₀ | DR1.d.z2, DR3.d.z1, DR4.d.z1 | M.Close |
| TL2.F ₈₀ | DR1.d.z3, DR3.d.z1, DR4.d.z1 | M.Close |
| TL2.F ₁₀₀ | DR1.d.z3, DR3.d.z2, DR4.d.z1 | M.Close |

served. In the TCD example shown in Figure 2, the triggering of command C1 by the protection system indicates among other things the absence of fault, F3. Also, the triggering of command C2, indicates the disappearance of D3 (!D3) and hence the negation or disappearance of the fault F2.

4. EXAMPLE

The example system considered in this paper (Figure 3) is a segment of a power transmission system. Power system components such as buses, lines, transformers, are protected by relays and breakers. When a fault occurs, relays and breakers are designed to isolate the fault according to a pre-determined protection scheme. Additionally, the system includes back-up relays to account for any problems in the primary relays and breakers. The system in Figure 3 is part of a network and includes three substations(SS1, SS2, and SS3) and two transmission lines (TL1,TL2). Transmission line TL1 carries power between buses BU1 and BU2 while transmission line TL2 is between buses BU2 and BU3. Each transmission line is protected with a distance relay and breaker at its two ends.

The distance relays estimate impedance using the voltage and current measurement at the relay measurement point. The estimated impedance is compared with the reach point impedance. If the estimated impedance is less than the reach point impedance, it is assumed that a fault exists on the line between the relay and the reach point. The fault-zone (zone1, zone2, zone3) is determined based on the estimated impedance. Figure 4 shows the region corresponding to each protection zone relative to Relay DR1 and the relative time-scales for the relay operation in each zone. A distance relay has to perform the dual task of primary and back up protection depending on the fault zone. For faults in zone1 (80% of the entire length of the transmission line (L1)), it serves as the primary protection and acts fast without any intentional time delay ($t_A^1 = 5$ to 6 cycles). For faults in zone2 (up to 50% of the adjacent line) and zone3 (up to 100% of the adjacent line), the relay serves as a back-up and reacts with some time delay allowing for the primary relay to operate. In Zone2, the time delay (t_A^2) is approximately 15-30 cycles (0.5 sec), while in

Zone3 it acts with a delay (t_A^3) of about 1.5 sec. Additionally, to account for temporary faults in the transmission lines, the relays include a fast and delayed auto-reclosure function, wherein they check for the fault after 2 sec (fast reclosure) and after 2-3 minutes (delayed reclosure). In case the faults persist, the relay disconnects the circuit permanently until it is remotely commanded to reset.

Each substation has a remote terminal unit (RTU) as part of the SCADA system to send the breaker status and other measurements to control center's Energy Management System (EMS). Some of the details recorded by the Sequence Event Recorder (SER) at each substation include: (a) Zone information and start protection time (in case of zone 1) (b) Tripping command sent by relay to breaker (c) Breaker status: opened or closed (d) Phase discordance problem: when breaker tried to open three phases but did not succeed for all three phases (e) Reclosure command issued by the relay to reclose breaker (f) Reclosure blocked command issued by relay to reset breaker to open after failed reclosure.

4.1. TCD model

The TCD model of the system in Figure 3 includes a) fault propagation model for transmission line faults, b) the breaker behavioral model and (c) the distance relay behavioral model. *Fault Propagation Model:* Table 1 captures the propagation of the faults in the transmission lines (TL1, TL2) to the discrepancies in distance relays (DR1, DR2, DR3, DR4). The faults in the transmission lines are categorized based on the segment where they occur along the length(L) of the line (from left to right) - F₂₀: [0, 0.2L), F₅₀: [0.2L, 0.5L), F₈₀: [0.5L, 0.8L), F₁₀₀: [0.8L, 1.0L), where L is the length of the transmission line. Discrepancies correspond to the zone with respect to the relay - d.z1: zone1, d.z2: zone2, d.z3: zone3. All failure propagations are active in mode M.Close when the circuit is closed.

Breaker Behavioral Model: The breaker behavioral model (table 2) includes states Open, Close, and partially open. The Open state maps to the system mode M.Open, states Close

Table 2. Transitions in a breaker's behavior model. The model includes states Open, Close and partially open (P.Open). Close is the initial state. Rows 1-2 capture the nominal operation to close and open the breaker. Rows 3-11 deal with faulty operation - rows 3,4:stuck close fault, rows 5-6:stuck open fault, rows 7-11: partially open fault.

| # | Src. State | Dst. State | Trigger | Guard | Action |
|----|------------|------------|------------|-----------------------|----------|
| 1 | Open | Close | C_Close | !F_st_open & !F_part | St_Close |
| 2 | Close | Open | C_Open | !F_st_close & !F_part | St_Open |
| 3 | Open | Close | F_st_close | none | none |
| 4 | Close | Close | C_Open | F_st_close | St_Close |
| 5 | Close | Open | F_st_Open | none | none |
| 6 | Open | Open | C_Close | F_st_open | St_Open |
| 7 | Open | P.Open | F_part | none | none |
| 8 | P.Open | Open | !F_part | none | none |
| 9 | Close | P.Open | C_Open | F_part | St_Open |
| 10 | P.Open | P.Open | C.Open | F_part | St.Open |
| 11 | P.Open | Close | C.Close | none | St.Close |

Table 3. Transition Information for Distance Relay's behavioral model. Rows 1-7 deal with the anomaly detection in state Det (rows 1-3: Zone1, rows 4,5: Zone2, rows 6,7: Zone3). Rows 8,9 deal with wait (until timeout) operation in Wait state based on the wait time T_w set for different operations - fast-reclosure(TFR), delayed-reclosure (TDR), backup in zone2 (Tw2) and zone3 (Tw3). Row 10-12 deal with system mode conditions for anomaly detection (transition to state Det). Rows 13-16 handle resets. Rows 17-21 deal with anomaly detection fault (F_de).

| # | Src State | Dst State | Trigger | Guard | Action |
|----|-----------|-----------|-----------------------------|-----------------|----------------------------|
| 1 | Det | Wait | d.z1↑ | n=0 | Z1, C_Open, n=1, Tw=TFR |
| 2 | Det | Wait | d.z1↑ | n=1 | C_Open, FRBLK, n=2, Tw=TDR |
| 3 | Det | BLK | d.z1↑ | n=2 | C_Open, DRBLK |
| 4 | Det | Wait | d.z2↑ | n=0 | n=3, Tw=Tz2 |
| 5 | Det | BLK | d.z2↑ | n=3 | C_Open |
| 6 | Det | Wait | d.z3↑ | n=0 | n=4, Tw=Tz3 |
| 7 | Det | BLK | d.z3↑ | n=4 | C_Open |
| 8 | Wait | Ch_Det | $Timeout(T_w)$ | $n \leq 2$ | C_Close |
| 9 | Wait | Ch_Det | $Timeout(T_w)$ | $n > 2$ | none |
| 10 | Ch_det | Det | none | M.Close & !F_de | none |
| 11 | Ch_det | No_Det | none | M.Open | none |
| 12 | No_Det | Det | none | M.Close | none |
| 13 | No_Det | Reset | C_Reset | none | none |
| 14 | BLK | Reset | C_Reset | none | C_Close |
| 15 | Det | Reset | d.z1↓ & d.z2↓ & d.z3↓ & n>0 | none | none |
| 16 | Reset | Ch_det | none | none | n=0 |
| 17 | Ch_det | Det_Err | F_de | none | none |
| 18 | Det_Err | Ch_Det | !F_de | none | none |
| 19 | Det | Det_Err | F_de | none | none |

and P.Open (partially open) map to the mode M.Close. The breaker receives commands from its distance relay to open (C.Open) and close (C.Close). After executing the command, it reports the physical state of the breaker as St.open (for open) and St.close (close). The behavioral model includes breaker faults related to being stuck open (F_st.open), stuck close (F_st.close) and partially open (F_part). Table 2 shows the operation of the breaker in terms of the transitions between the states based on the events (commands) and fault conditions. Rows 1-2 capture the nominal operation to close and open the breaker when it receives the appropriate command. While rows 3-4 capture the breaker behavior when it is stuck close, rows 5-6 deal with a breaker with a stuck open fault. Rows 7-11 deal with a partially open breaker (which leads to phase discordance problems in the system).

Event propagation paths related to the transitions listed in Ta-

ble 2 capture the pre (source) and post (destination) conditions and observations to help analyze whether the breaker is operating nominally or is faulty. The generated event propagation paths are as follows:

- M.Close, C.Open, !F_st.close, !F_part → St.Open, M.Open
- M.Open, C.Close, !F_st.Open, !F_part → St.Close, M.Close
- M.Open, C.Close, F_st.Open → St.Open, M.Open
- M.Close, C.Open, F_st.Close → St.Close, M.Close
- M.Close, C.Open, F_part → St.Open, M.Close
- M.Close, C.Close, F_part → St.Close, M.Close

Distance Relay: The behavioral model states include: (a) Det: state when it is actively looking for anomalies and triggering appropriate action upon detection, (b) Wait: when it is waiting for a time-out to expire before taking the next set of actions (c) BLK: when it is blocking and waiting for a reset command as it has taken the necessary action to arrest

Table 4. Scenario 1: Distance Relays - Events and Hypotheses

| Time(s) | Comp | Event | Hypotheses |
|---------|------------|---------------|--|
| 100.02 | DR3 DR4 | Z1, C.Open | $H1_{DR3}=d.z1, M:1/1$ $H1_{DR4}=d.z1, M:1/1$ |
| | DR1 | Z2 | $H1_{DR1}=d.z2$ $H1_{sys}=TL2.F_{20}, M:2/3$ $H2_{sys}=TL2.F_{50}, M:3/3$ $H3_{sys}=TL2.F_{80}, M:2/3$ $H4_{sys}=TL2.F_{100}, M:1/3$ |
| 102.04 | DR3, DR4 | C.Close | |
| 102.07 | DR3, DR4 | FRBLK, C.Open | $H2_{sys}= TL2.F_{50}, M: 5/5$ |
| 222.09 | DR3, DR4 | C.Close | |
| 222.12 | DR3, DR4 | DRBLK, C.Open | $H2_{sys}= TL2.F_{50}, M: 7/7$ |

Table 5. Scenario 1: Breakers - Events & Hypotheses

| Time(s) | Comp | Event | Hypotheses |
|---------------------------|-------------|----------------------|--|
| 100.03/ 102.08/ 202.13 | BR3, BR4 | C.Open, St.Open | $H1_{BR3}=C.Open, M.Open$ $H1_{BR4}=C.Open, M.Open$ |
| 102.05/ 222.10 | BR3, BR4 | C.Close, St.Close | $H2_{BR3}=C.Close, M.Close$ $H2_{BR4}=C.Close, M.Close$ |

Table 6. Event trace and Hypotheses: Scenario 2

| Time (s) | Comp | Event | Hypotheses |
|----------|-------------|---------------------|---|
| 100.02 | DR3 DR4 | Z1 C.Open | $H1_{DR3}=d.z1, M:1/1$ $H1_{DR4}=d.z1, M:1/1$ |
| | DR1 | Z2 | $H1_{DR1}=d.z2$ $H1_{sys}=TL2.F_{20}, M:2/3$ $H2_{sys}=TL2.F_{50}, M:3/3$ $H3_{sys}=TL2.F_{80}, M:2/3$ $H4_{sys}=TL2.F_{100}, M:1/3$ |
| 102.07 | DR3, DR4 | NULL (No Obs) | $H1_{DR3}=d.z1, M:1/2$ $H1_{DR4}=d.z1, M:1/2$ $H2_{DR3}=d.z1\downarrow, d.z2\downarrow, d.z3\downarrow, M:1/1$ $H2_{DR4}=d.z1\downarrow, d.z2\downarrow, d.z3\downarrow, M:1/1$ $H2_{sys}= TL2.F_{50}, M: 3/5$ $H3_{sys}= !TL2.F_{50}, M: 2/2$ |

the fault propagation, (d) Det_Err: when it is unable to detect anomalies because of internal fault (F.de), (e) other miscellaneous states such as Ch_det (where it checks if detection is feasible), No_Det (when no detection is possible), Reset (when it is resetting).

The distance relays detects anomalies pertaining to faults in Zone1 (d.z1), Zone2 (d.z2) and Zone3 (d.z3) of the appropriate transmission line and reports these observations through output-events Z1 (Zone1), Z2 (Zone2) and Z3 (Zone3) respectively. It issues commands to the breaker to open (C.Open) and close (C.Close) and acts upon command to reset (C.reset). It reports unsuccessful fast and delayed re-closure through the output events FRBLK and DRBLK respectively. The faults considered as part of the distance relay include failure to detect the anomalies in transmission line impedance (F.de). While the distance relay states do not map to any system-modes, the system-modes determine if the distance relay is capable of detecting anomalies (mode: M.Close) or not (Mode: M.Open).

Tables 3 describe the transitions for the distance relay's be-

havioral model. The rows 1-3 deal with the nominal operation when discrepancy related to zone1 fault is detected (row 2: fast re-closure, row 3: delayed re-closure). Rows 4,5 deal with zone2 fault and rows 6,7 with zone3 fault. The wait time (T_w) in the Wait state are set for fast reclosure (TFR), delayed reclosure (TDR), backup wait time in zone2 fault (Tz2) and zone3 fault (Tz3). These wait times (T_w) are used in the $TIMEOUT(T_w)$ operation in rows 8 and 9. Rows 10,11,12 specify the system modes in which the distance relay can detect anomalies i.e. transition to Det state. Rows 13-16 deal with resetting the distance relay. Rows 17-21 deal with presence or disappearance of fault (F.de) related to problems in detecting anomalies.

Event propagation paths related to the transitions listed in Table 3 capture the pre (source) and post (destination) conditions and observations to help analyze whether the distance relay is operating nominally or is faulty. The generated event propagation paths are as follows:

- (a) M.Close, d.z1 \uparrow \rightarrow Z1, C.Open (b) M.Close, d.z1 \uparrow \rightarrow FRBLK, C.Open (c) M.Close, d.z1 \uparrow \rightarrow DRBLK, C.Open (d) M.Close, d.z2 \uparrow \rightarrow Z2 (e) M.Close, d.z2 \uparrow \rightarrow C.Open (f) M.Close, d.z3 \uparrow \rightarrow Z3

Table 7. Event trace and Hypotheses: Scenario 3

| Time (s) | Comp | Events | Hypotheses |
|----------|------|---------------|--|
| 100.02 | DR4 | Z1,C_Open | $H1_{DR4}=d.z1, M:1/1$ |
| | DR1 | Z2 | $H1_{DR1}=d.z2$ $H1_{sys}=TL2.F_50, M:2/2$ $H2_{sys}=TL2.F_80, M:1/2$ $H3_{sys}=TL2.F_100, M:1/2$ |
| 100.07 | DR1 | C_Open | $H1_{DR3}=F.de, M:1/1$ $H4_{sys}=TL2.F_50, DR3.F.de M: 3/3$ |
| 102.07 | DR4 | FRBLK, C_Open | $H4_{sys}=TL2.F_50, DR3.F.de, M: 4/4$ |
| 222.12 | DR4 | DRBLK, C_Open | $H4_{sys}=TL2.F_50, DR3.F.de, M: 5/5$ |

(g) M_Close, d.z3 \uparrow \rightarrow C_Open (h) F.de \rightarrow NULL (No Obs)

(i) d.z1 \downarrow & d.z2 \downarrow d.z3 \downarrow \rightarrow NULL (No Obs)

4.2. Case Study: Fault Scenarios and Diagnosis Results

This section considers a few of fault scenarios in the example power transmission system (Figure 3). The discrete behavioral and fault propagation model described in the Section 4.1 are used to simulate the system both in the nominal and faulty modes. The simulation is performed in Acumen (Taha et al., 2012) with a simulation time-step of 0.01 sec. The observable event-traces are collected and analyzed based on the algorithm 1. The reasoner uses the event propagation paths described in in Section 4.1 to reason about the events observed in the breakers (BR1, BR2, BR3, BR4) and distance relays (DR1, DR2, DR3, DR4). The fault propagation model captured in Table 1 is used to produce system-wide consistent hypotheses that can explain the observed anomalies and event traces.

In all the scenarios described below, the system is considered to be operating in nominal mode (mode=M_Close) until time t=100sec, when transmission line, TL2 experiences a line-to-ground-short fault, F_50.

Scenario 1: Permanent Fault In Transmission Line

In this scenario, the fault (TL2.F_50) is persistent. The simulator generated event-traces (similar to data from Sequence Event Recorders in real system) are fed to the TCD reasoner. Table 4, presents the events observed from the distance relays (DR1, DR3, DR4) and the hypotheses generated by TCD reasoner. The initial hypotheses point towards a zone1 discrepancy (d.z1) in DR3, DR4 and zone2 discrepancy in (d.z2) in DR1. System level hypotheses, $H2_{sys}$ (fault: TL2.F_50) has the maximum metric (3/3) with three consistent evidences from DR1, DR3, DR4. Moving forward, the observations of failed reclosure - fast (FRBLK) and delayed (DRBLK) - from DR3, DR4 further support $H2_{sys}$ (7/7), suggesting a diagnosis of fault in F_50 in TL2.

The events generated from the breaker and their associated hypotheses are presented in Table 5. The hypotheses suggest nominal operation and capture the mode-change. The multiple time values in each row of column 1 correspond to differ-

ent times when the same event (& hypotheses) are observed.

Scenario 2: Temporary Fault In Transmission Line Here, the fault (TL2.F_50) lasts for exactly 1 sec. DR3, DR4 come-up to test the fast re-closure 2 sec after detecting a zone 1 discrepancy (d.z1). Hypotheses $H2_{DR3}$, $H2_{DR4}$ identify the lack of any observations to be consistent with the event propagation path corresponding to the disappearance of discrepancies (d.z1 \downarrow , d.z2 \downarrow , d.z3 \downarrow). Thereafter system hypotheses $H3_{sys}$ suggests with a 100% (2/2) supporting evidences that there is no fault in TL2 (!TL2.F_50)

Scenario 3: Fault In Transmission Line and Relay This is a multi-fault scenario in which a distance relay fault, F_de, prevents DR3 from detecting discrepancies produced by transmission line fault, TL2.F_50. Lack of observations consistent with the predicted hypothetical state of DR3.d.z1 suggest problems with the event propagation path (M_Close, d.z1, !F_de) in DR3. Hypothesis $H1_{DR3}$ in Table 7 explains this observation (or lack of), with fault DR3.F_de. The multi-fault system hypothesis ($H4_{sys}$) best explains the observations.

5. DISCUSSION AND CONCLUSION

We have presented in this paper a new formalism: Temporal Causal Diagrams - with the objective of applying it to diagnose cyber-physical systems that include local fast-acting protection devices. Specifically, we have demonstrated the capability of the TCD model to capture the discrete fault propagation and behavioral model of a segment of a power transmission system protected by distance relays and breakers. Further, the paper presented the potential of the TCD-based reasoner to diagnose faults in the physical system and its protection elements.

As part of our future work, we wish to test and study the scalability of this approach towards a larger power transmission system including a far richer set of protection elements. Further, we wish to consider more realistic event traces from the fault-scenarios including missing, inconsistent, and out-of-sequence alarms and events.

ACKNOWLEDGMENT

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

NOMENCLATURE

| | |
|--------------|---|
| t | arbitrary time instant |
| A_t | Alarms observed at time t |
| Ev_t | Events observed at time t |
| O_t | Observations (Alarms and Events) at time t |
| H | Hypothesis - a data structure that captures the hypothetical states of all the nodes in the model. |
| HS_t | Hypotheses set at time t . |
| HS'_t | Temporary variable - hypotheses set. |
| \uparrow | rising edge of an event. Also used to describe the onset of a discrepancy. |
| \downarrow | falling edge of an event. If associated with a discrepancy it describes the event associated with the remission of the discrepancy. |

REFERENCES

- Abdelwahed, S., Karsai, G., & Biswas, G. (2004). System diagnosis using hybrid failure propagation graphs. In *The 15th international workshop on principles of diagnosis*. Carcassonne, France.
- Abdelwahed, S., Karsai, G., & Biswas, G. (2005). A consistency-based robust diagnosis approach for temporal causal systems. In *The 16th international workshop on principles of diagnosis*. Pacific Grove, CA.
- Abdelwahed, S., Karsai, G., Mahadevan, N., & Ofsthun, S. (2009). Practical Implementation of Diagnosis Systems Using Timed Failure Propagation Graph Models. *Instrumentation and Measurement, IEEE Transactions on*, 58(2), 240–247.
- Bastos, J. L., Zhang, Y., Srivastava, A. K., & Schulz, N. N. (2007). A design paradigm for integrated protection of shipboard power systems. In *Proceedings of the 2007 summer computer simulation conference* (pp. 3:1–3:10). San Diego, CA, USA: Society for Computer Simulation International.
- Chen, W., Liu, C., & Tsai, M. (2000). On-line fault diagnosis of distribution substations using hybrid cause-effect network and fuzzy rule-based method. *Power Delivery, IEEE Transactions on*, 15(2), 710–717.
- Chen, W.-H., Liu, C.-W., & Tsai, M.-S. (2000, Apr). On-line fault diagnosis of distribution substations using hybrid cause-effect network and fuzzy rule-based method. *Power Delivery, IEEE Transactions on*, 15(2), 710–717. doi: 10.1109/61.853009
- Console, L., & Torasso, P. (1991). On the co-operation between abductive and temporal reasoning in medical diagnosis. *Artificial Intelligence in Medicine*, 3(6), 291–311.
- Coster, E., Myrzik, J., Kruimer, B., & Kling, W. (2011, January). Integration issues of distributed generation in distribution grids. *Proceedings of the IEEE*, 99(1), 28–39. doi: 10.1109/JPROC.2010.2052776
- Daigle, M., Roychoudhury, I., Biswas, G., Koutsoukos, X., Patterson-Hine, A., & Poll, S. (2010). A Comprehensive Diagnosis Methodology for Complex Hybrid Systems: A Case Study on Spacecraft Power Distribution Systems. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, 40(5), 917–931.
- Fukui, C., & Kawakami, J. (1986, Oct). An expert system for fault section estimation using information from protective relays and circuit breakers. *Power Delivery, IEEE Transactions on*, 1(4), 83–90. doi: 10.1109/TPWRD.1986.4308033
- Garrity, T. (2008). Getting smart. *Power and Energy Magazine, IEEE*, 6(2), 38–45.
- Guo, W., Wen, F., Ledwich, G., Liao, Z., He, X., & Liang, J. (2010). An Analytic Model for Fault Diagnosis in Power Systems Considering Malfunctions of Protective Relays and Circuit Breakers. *Power Delivery, IEEE Transactions on*, 25(3), 1393–1401.
- Ilic, M., Allen, H., Chapman, W., King, C., Lang, J. H., & Litvinov, E. (2005, Nov). Preventing future blackouts by means of enhanced electric power systems control: From complexity to order. *Proceedings of the IEEE*, 93(11), 1920–1941. doi: 10.1109/JPROC.2005.857496
- Karsai, G., Sztipanovits, J., Padalkar, S., & Biegl, C. (1992). Model based intelligent process control for cogenerator plants. *Journal of Parallel and Distributed Systems*, 15, 90–103.
- Lee, S., Choi, M., Kang, S., Jin, B., Lee, D., Ahn, B., ... Wee, S. (2004). An intelligent and efficient fault location and diagnosis scheme for radial distribution systems. *Power Delivery, IEEE Transactions on*, 19(2), 524–532.
- Lin, X., Ke, S., Li, Z., Weng, H., & Han, X. (2010). A Fault Diagnosis Method of Power Systems Based on Improved Objective Function and Genetic Algorithm-Tabu Search. *Power Delivery, IEEE Transactions on*, 25(3), 1268–1274.
- Meléndez, J., Macaya, D., Colomer, J., Llanos, D., Gervas, P., & Gupta, K. (2004). Symptom based representation for dynamic systems diagnosis. Application to Electrical Power Distribution. In *Proceedings of the ecbr workshops*. edited by p. gervas and km gupta. university of madrid, madrid (pp. 311–327).
- Mengshoel, O., Chavira, M., Cascio, K., Poll, S., Darwiche, A., & Uckun, S. (2010). Probabilistic model-based

- diagnosis: An electrical power system case study. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, 40(5), 874–885.
- Miao, H., Sforza, M., & Liu, C.-C. (1996, Aug). A new logic-based alarm analyzer for on-line operational environment. *Power Systems, IEEE Transactions on*, 11(3), 1600-1606. doi: 10.1109/59.535703
- Misra, A. (1994). *Sensor-based diagnosis of dynamical systems*. Unpublished doctoral dissertation, Vanderbilt University.
- Misra, A., Sztipanovits, J., & Carnes, J. (1994). Robust diagnostics: Structural redundancy approach. In *Spie's symposium on intelligent systems*.
- Mosterman, P. J., & Biswas, G. (1999). Diagnosis of continuous valued systems in transient operating regions. *IEEE Trans. on Systems, Man and Cybernetics*, 29(6), 554-565.
- North American Electric Reliability Corporation. (2012). *2012 state of reliability* (Tech. Rep.). Retrieved from http://www.nerc.com/files/2012_sor.pdf
- Padalkar, S., Sztipanovits, J., Karsai, G., Miyasaka, N., & Okuda, K. C. (1991). Real-time fault diagnostics. *IEEE Expert*, 6(3), 75–85.
- Poll, S., Patterson-Hine, A., Camisa, J., Garcia, D., Hall, D., Lee, C., ... others (2007). Advanced diagnostics and prognostics testbed. In *Proceedings of the 18th international workshop on principles of diagnosis (dx-07)* (pp. 178–185).
- Pourbeik, P., Kundur, P., & Taylor, C. (2006). The anatomy of a power grid blackout-root causes and dynamics of recent major blackouts. *Power and Energy Magazine, IEEE*, 4(5), 22–29.
- Ren, H., Mi, Z., Zhao, H., & Yang, Q. (2005). Fault diagnosis for substation automation based on Petri nets and coding theory. In *Power engineering society general meeting, 2004. IEEE* (pp. 1038–1042).
- Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., & Teneketzis, D. (1996, March). Failure diagnosis using discrete-event models. *IEEE Transactions On Control System Technology*, 4(2), 105–124.
- Sekine, Y., Akimoto, Y., Kunugi, M., Fukui, C., & Fukui, S. (2002). Fault diagnosis of power systems. *Proceedings of the IEEE*, 80(5), 673–683.
- Sun, J., Qin, S., & Song, Y. (2004). Fault diagnosis of electric power systems based on fuzzy Petri nets. *Power Systems, IEEE Transactions on*, 19(4), 2053–2059.
- Taha, W., Brauner, P., Zeng, Y., Cartwright, R., Gaspes, V., Ames, A., & Chapoutot, A. (2012, June). A core language for executable models of cyber-physical systems (preliminary report). In *Distributed computing systems workshops (icdcs), 2012 32nd international conference on* (p. 303-308). doi: 10.1109/ICDCSW.2012.72
- Talukdar, S., Cardozo, E., & Perry, T. (2007). The operator's assistant—an intelligent, expandable program for power system trouble analysis. *Power Systems, IEEE Transactions on*, 1(3), 182–187.
- Tholomier, D., Richards, S., & Apostolov, A. (2007, Aug). Advanced distance protection applications for dynamic loading and out-of step condition. In *Bulk power system dynamics and control - vii. revitalizing operational reliability, 2007 irep symposium* (p. 1-8). doi: 10.1109/IREP.2007.4410560
- Yang, C., Okamoto, H., Yokoyama, A., & Sekine, Y. (1992). Expert system for fault section estimation of power systems using time-sequence information. *International Journal of Electrical Power & Energy Systems*, 14(2-3), 225–232.
- Yongli, Z., Limin, H., & Jinling, L. (2006). Bayesian networks-based approach for power systems fault diagnosis. *Power Delivery, IEEE Transactions on*, 21(2), 634–639.
- Zhang, Y., Ilic, M., & Tonguz, O. (2011, January). Mitigating blackouts via smart relays: A machine learning approach. *Proceedings of the IEEE*, 99(1), 94 -118. doi: 10.1109/JPROC.2010.2072970
- Zhou, G. (1993). A neural network approach to fault diagnosis for power systems. In *Tencon'93. proceedings. computer, communication, control and power engineering. 1993 IEEE region 10 conference on* (pp. 885–888).

BIOGRAPHIES



Nagabhushan Mahadevan is a Senior Research Engineer at the Institute for Software Integrated Systems, Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN. His work involves research in model-based diagnostics, verification and validation of health management systems, resilience in cyber-physical systems. He received his M.S. degree in Computer Engineering and Chemical Engineering from the University of South Carolina, Columbia, and B.E.(Hons.) degree in Chemical Engineering from Birla Institute of Technology and Science, Pilani, India.



Dr. Abhishek Dubey is a Research Scientist at the Institute for Software Integrated Systems, Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN. His research interests are related to resilient cyber-physical systems and fault diagnosis in distributed software systems. He received his PhD. in Electrical Engineering from Vanderbilt University in 2009 and B.Tech. in Electrical Engineering from Indian Institute of Technology, BHU, Varanasi, India in 2001.



Dr. Gabor Karsai is a Professor of Electrical Engineering and Computer Science at Vanderbilt University, and Senior Research Scientist at the Institute for Software-Integrated Systems. He conducts research

in the design and implementation of cyber-physical systems, in programming tools for model-driven development environments, in the theory and practice of model-integrated computing, and in real-time fault diagnostics. He received his B.Sc., M.Sc., and Dr. Techn degrees from the Technical University of Budapest, Hungary, in 1982, 1984 and 1988, respectively, and his PhD from Vanderbilt University in 1988. Dr. Karsai has worked several large DARPA projects in the recent past: advanced scheduling and resource management algorithms, fault-adaptive control technology that has been transitioned into aerospace programs, and model-based integration of embedded systems whose resulting tools are being used in embedded software development tool chains.



Dr. Anurag K. Srivastava is an assistant professor of electric power engineering at Washington State University and the director of the Smart Grid Demonstration and Research Investigation Lab (SGDRIL). He received his Ph.D. degree in electrical engineering from the Illinois Institute of Technology in 2005. His research interests include power system operation and control using smart grid data. Dr. Srivastava is a senior member of the IEEE, an associate editor of the IEEE Transactions on Smart Grid, and an IEEE distinguished lecturer. He is author of more than 130 technical publications including a book on power system security.



Dr. Chen-Ching Liu is Boeing Distinguished Professor at Washington State University (WSU), Pullman, USA. At WSU, Professor Liu serves as Director of the Energy Systems Innovation (ESI) Center. During 1983-2005, he was a Professor of EE at University of Washington, Seattle. Dr. Liu was Palmer Chair Professor at Iowa State

University from 2006 to 2008. From 2008-2011, he served as Deputy/Acting Principal of the College of Engineering, Mathematical and Physical Sciences at University College Dublin, Ireland. Professor Liu received an IEEE Third Millennium Medal in 2000 and the Power and Energy Society Outstanding Power Engineering Educator Award in 2004. In 2013, Dr. Liu was awarded a Doctor Honoris Causa by Polytechnic University of Bucharest, Romania. Professor Liu is a Fellow of the IEEE.

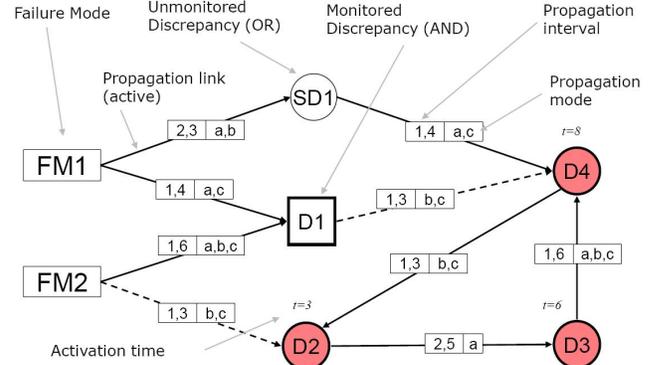


Figure 5. TFGP model ($t = 10$, Mode=A $\forall t \in [0, 10]$).

APPENDIX

A. TIMED FAILURE PROPAGATION GRAPH (TFGP)

A TFGP (Abdelwahed et al., 2004, 2005) is a labeled directed graph. The root nodes are failure modes (fault causes). The other nodes are discrepancies (off-nominal conditions that are the effects of failure modes). Edges between nodes in the graph capture the causality of failure propagation. The edge labels capture the time-interval and operating modes when the failure propagation edge is active. Formally, a TFGP is represented as a tuple (F, D, E, M, ET, EM, DC) , where:

- F is a nonempty set of failure nodes.
- D is a nonempty set of discrepancy nodes.
- $E \subseteq V \times V$ is a set of edges connecting the set of all nodes $V = F \cup D$.
- M is a nonempty set of system modes. At each time instance t the system can be in only one mode.
- $ET : E \rightarrow I$ is a map that associates with every edge in E a time interval $[t_{min}, t_{max}] \in I$ that represents the minimum (t_{min}) and maximum (t_{max}) time for failure propagation over the edge.
- $EM : E \rightarrow \mathcal{P}(M)$ is a map that associates with every edge in E a set of modes in M when the edge is active. For any edge $e \in E$ that is not mode-dependent (i.e. active in all modes), $EM(e) = \emptyset$.
- $DC : D \rightarrow \{AND, OR\}$ is a map defining the class of each discrepancy as either AND or an OR node. An OR (AND) type discrepancy node will be activated when the failure propagates to the node from any (all) of its parents.
- $DS : D \rightarrow \{A, I\}$ is a map defining the monitoring status of the discrepancy as either A for the case when the discrepancy is active (monitored by an online alarm) or I for the case when the discrepancy is inactive (not monitored).

Figure 5 shows a graphical depiction of a failure propagation graph model. Rectangles in the graph model represent

the failure modes while circles and squares represent OR and AND type discrepancies, respectively. The edges between the nodes represent failure propagation. Propagation edges are parameterized with the corresponding interval, $[e.tmin, e.tmax]$, and the set of modes at which the edge is active. Figure 5 also shows a sequence of active discrepancies (alarm signals) identified by shaded discrepancies. The time at which the alarm is observed is shown above the corresponding discrepancy. Dashed lines are used to distinguish inactive propagation links.

The TFPG reasoning algorithm attempts to explain the current observations (states of monitored discrepancy nodes) by hypothesizing the faults that could have occurred in the system. Each hypothesis assigns a hypothetical state to each node in the graph. In case of failure modes, an ON state indicates that the failure is present, otherwise the state is OFF. The state of a discrepancy node could be set to ON or OFF depending on whether the failure-effect has reached the node or not. Alternately, an UNKNOWN state indicates that there is not enough information to figure out if the failure-effect has definitely reached the node.

The TFPG failure propagation semantics is used to identify and update the hypothetical states of the TFPG nodes. For an OR discrepancy v' and an edge $e = (v, v') \in E$, once a failure effect reaches v at time t it will reach v' at a time t' where $e.tmin \leq t' - t \leq e.tmax$. On the other hand, the activation period of an AND discrepancy v' is the composition of the activation periods for each link $(v, v') \in E$. For a failure to propagate through an edge $e = (v, v')$, the edge should be active throughout the propagation, that is, from the

time the failure reaches v to the time it reaches v' . An edge e is active if and only if the current operation mode of the system, m_c is in the set of activation modes of the edge, that is, $m_c \in EM(e)$. When a failure propagates to a monitored discrepancy node (or alarm) v' ($DS(v') = A$) its physical state is considered to be ON, otherwise it is considered to be OFF. If the link is deactivated any time during the propagation (because of mode switching), the propagation stops. Links are assumed to be memory less with respect to failure propagation so that current failure propagation is independent of any (incomplete) previous propagation. Also, once a failure effect reaches a node, its state will change permanently and will not be affected by any future failure propagation.

While a detailed description of the TFPG diagnosis algorithm may be found in (Abdelwahed et al., 2004, 2005), in the interest of self-containment a brief description of the procedures referenced in this paper is provided below.

- *Consis*(H, O_t) : This procedure checks if the hypothetical states of nodes as captured in the hypothesis H are consistent with the observations O at time t .
- *UpdateHypo*(t, HS_{t-1}): This procedure takes in as input the current time, t , and the set of hypotheses at the previous time-stamp, HS_{t-1} and outputs an updated set of hypotheses, HS_t which include any updates to the state of the nodes based on the time elapsed.
- *ExplainHypo*(H, O_t): This procedure generates new hypotheses to explain the current observations (O_t) relative to an existing hypothesis H that explains the past observations.