Failure Prognosis Using Timed Failure Propagation Graphs

Sherif Abdelwahed [1], **Gabor Karsai** [2]

[1] *Electrical and Computer Engineering Department, Mississippi State University, Mississippi State, MS 37203*
sherif@ece.msstate.edu
[2] *Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN, 37203.*
gabor@isis.vanderbilt.edu

ABSTRACT

Timed failure propagation graph (TFPG) is a causal model that captures the causal and temporal aspects of failure propagation in a wide variety of engineering systems. In this paper we investigate the problem of failure prognosis within the TFPG model settings. The paper introduces a formal definition for system reliability based on measures of failure criticality, proximity between alarm observations, and plausibility of the estimated current system condition. An algorithm to compute the time to reach a given criticality level of the system, referred to as time to criticality, based on the current conditions of the system is introduced. The time to criticality, also known as the system's Remaining Useful Life (RUL), can be used as a measure for system reliability at any given time in the future.

1 INTRODUCTION

Large engineering systems such as manufacturing systems, power networks, and chemical plants are usually designed for autonomous or semi-autonomous operation. With age, these systems become vulnerable to failures and degradations, and therefore requires extensive and expensive maintenance. A proactive maintenance approach in which operation problems can be predicted and handled at an early stage can significantly reduce the cost of operation and enhance the system performance. One of the key enabling technique for proactive maintenance is failure prognosis.

Failure prognosis is the process of evaluating the reliability of the system at certain time in the future by assessing the consequence of degradation and deviation of the system from its expected normal operating settings. The ISO standard (ISO-13381-1, 2004) corresponds failure prognosis to the estimation of the operating time until failure and to the risk of existence or future appearance of one or more failure modes. This operating time until failure is known in the health management community as the Remaining Useful Life (RUL). Failure prognosis for engineering systems provides data that can be used to meet several vital and safety-critical goals, including giving advance warning of potential failures, minimizing unscheduled maintenance, extending maintenance cycles, and maintaining system effectiveness through timely repair actions, and reducing the life-cycle cost of equipment by decreasing inspection costs, downtime, and inventory (Vichare and Pecht, 2006).

Three main prognosis approaches are proposed in the literature (Vachtsevanos *et al.*, Wiley Sons) and (Lebold and Thurston, 2001): model-based prognosis, data-driven prognosis, and experience-based prognosis. The first approach depends on the availability of a mathematical model of system failure which is used to estimate the future evolution of degradation (Luo *et al.*, 2003; Chelidze *et al.*, 2002; Provan, 2003). The second approach uses data provided by the data collection (sensors) infrastructure to predict future faults and degradation (Medjaher *et al.*, 2009). Tools and techniques employed in this approach are generally those used by the artificial intelligence community. The third approach proposes an estimation of the RUL by using reliability models obtained from the historical data of the machine. A survey of the techniques used in each approach can be found in (Medjaher *et al.*, 2009; Jardine and Lin, 2006; Muller *et al.*, 2008).

In earlier work (Abdelwahed *et al.*, 2004) a model-based diagnosis approach was developed for a general class of engineering systems based on the timed failure propagation graph (TFPG) model. Timed failure propagation graphs (Misra *et al.*, 1994; Padalkar *et al.*, 1991) are causal models that describe the system behavior in presence of faults. The TFPG structure captures the effect of time delays and switching dynamics on the propagation of failures in practical discrete event and hybrid systems. A TFPG-based modeling and reasoning tool has been developed as a part of an integrated fault diagnoses and process control system toolsuite (Karsai *et al.*, 2003) and has been successfully used in practical real-time vehicle subsystems (Ofsthun and Abdelwahed, 2007).

This paper addresses the prognosis problem for TFPG models. The proposed technique falls within the model-based approach, in which a mathematical model of the degradation (in our case the TFPG model)

is used to estimate the RUL. We define the prognosis problem for this class of real-time systems based on notions of failure criticality, measures of distance between alarms (monitored discrepancies), and plausibility of state estimation based on current observed discrepancies. These measures are then used to define the time-to-criticality metric which corresponds to the minimum time to reach a known critical failure condition from the current state of the systems. The time-to-criticality, which is semantically equivalent to RUL, can be used as a measure for system reliability at any future time.

The paper is organized as follows. In Section 2, the timed failure propagation graph model is introduced. Section 3 presents an overview of the consistency based diagnosis approach for TFPG models. Section 4 introduces the formal definitions for the main aspects of failure prognosis problem within the TFPG model settings and provides an algorithm to compute the time-to-criticality for a given TFPG model at any given state. Conclusion and future works are discussed in Section 5.

2 TIMED FAILURE PROPAGATION GRAPHS

A TFPG is a labeled directed graph where nodes represent either failure modes, which are fault causes, or discrepancies, which are off-nominal conditions that are the effects of failure modes. Edges between nodes in the graph capture the effect of failure propagation over time in the underlying dynamic system. To represent failure propagation in multi-mode (switching) systems, edges in the graph model can be activated or deactivated depending on a set of possible operation modes of the system. Formally, a TFPG is represented as a tuple $(F, D, E, M, \mathsf{ET}, \mathsf{EM}, \mathsf{DC})$, where:

- F is a nonempty set of failure modes.
- 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.
- $\mathsf{ET} : E \to I$ is a map that associates every edge in E with a time interval $[t_1, t_2] \in I$.
- $\mathsf{EM} : E \to \mathcal{P}(M)$ is a map that associates every edge in E with a set of modes in M. We assume that $\mathsf{EM}(e) \neq \varnothing$ for any edge $e \in E$.
- $\mathsf{DC} : D \to \{\texttt{AND}, \texttt{OR}\}$ is a map defining the class of each discrepancy as either AND or an OR node.
- $\mathsf{DS} : D \to \{\texttt{A}, \texttt{I}\}$ 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)[1].

[1]In this paper we will use the terms alarms and monitored discrepancies interchangeably as they mean the same thing.

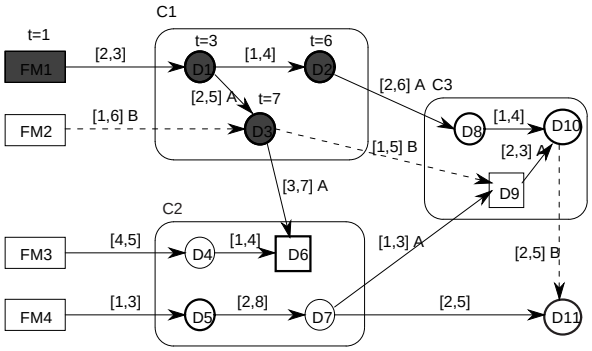

Figure 1: A TFPG model ($t = 10$, Mode = A for $t \in [0, 10]$)

In the above model, the map ET associates each edge $e \in E$ with the minimum and maximum time for the failure to propagate along the edge. For an edge $e \in E$, we will use the notation $e.\mathrm{tmin}$ and $e.\mathrm{tmax}$ to indicate the corresponding minimum and maximum time for failure propagation along e, respectively. That is, given that a propagation edge is enabled (active), it will take at least (at most) tmin (tmax) time for the fault to propagate from the source node to the destination node. The map EM associates each edge $e \in E$ with a subset of the system modes at which the failure can propagate along the edge. Consequently, the propagation link e is enabled (active) in a mode $m \in M$ if and only if $m \in \mathsf{EM}(e)$. The map DC defines the type of a given discrepancy as either AND or OR. An OR type discrepancy node will be activated when the failure propagates to the node from any of its parents. On the other hand, an AND discrepancy node can only be activated if the failure propagates to the node from all its parents. We assume that TFPG models do not contain self loops and that failure modes are always root nodes, i.e., they cannot be a destination of any edge. Also, a discrepancy cannot be a root node, that is, every discrepancy must be a successor of another discrepancy or a failure mode.

Figure 1 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 arrows between the nodes represent failure propagation. Propagation edges are parameterized with the corresponding interval, $[e.\mathrm{tmin}, e.\mathrm{tmax}]$, and the set of modes at which the edge is active. Figure 1 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 model captures observable failure propagations between discrepancies in dynamic systems. In this model, alarms capture state deviations from nom-

inal values. The set of all observed deviations corresponds to the monitored discrepancy set in the TFPG model. Propagation edges, on the other hand, correspond to causality (for example, as defined by energy flow) in the system dynamics. Due to the dynamic nature of the system, failure effects take time to propagate between the system components. Such time in general depends on the systems time constants as well as the size and timing of underlying failure. Propagation delay intervals can be computed analytically or through simulation of an accurate physical model.

Failure propagation in a TFPG system has simple semantics. The state of a node indicates whether the failure effects reached this node. For an OR type node 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 $e.\text{tmin} \leq t' - t \leq e.\text{tmax}$. On the other hand, the activation period of an AND alarm 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, $m_c \in \mathsf{EM}(e)$. When a failure propagates to a monitored node v' ($\mathsf{DS}(v') = \texttt{A}$) its physical state is considered ON, otherwise it is OFF. If the link is deactivated any time during the propagation (because of mode switching), the propagation stops. Links are assumed memoryless with respect to failure propagation so that current failure propagation is independent of any (incomplete) previous propagation. Also, once a failure effect reaches a discrepancy its state will change permanently and will not be affected by any future failure propagation.

3 THE CONSISTENCY-BASED REASONING APPROACH

The reasoning algorithm for TFPG model diagnosis is based on a consistency relationship defined using three state mappings for the graph nodes of the TFPG model: physical, observed, and hypothetical.

A *physical system* state corresponds to the current state of all nodes in the TFPG model. At any time t the physical state is given by a map $AS_t : V \rightarrow \{\texttt{ON}, \texttt{OFF}\} \times \mathbb{R}$, where V is the set of nodes in the TFPG model. An ON state for a node indicates that the failure (effect) reached this node, otherwise it is set to OFF. The physical state at time t is denoted $AS_t(v).\text{state}$, while $AS_t(v).\text{time}$ denote the last time at which the state of v is changed. Failure effects are assumed permanent, therefore, the state of a node once changed will remain constant after that. A similar map is used to define the state of edges based on the current mode of the system.

The *observed state* at time t is defined as a map $S_t : D \rightarrow \{\texttt{ON}, \texttt{OFF}\} \times \mathbb{R}$. Clearly, observed states are only defined for discrepancies. The observed state of the system may not be consistent with the failure propagation graph model temporal constraints, due to potential failures in the alarm monitors. However, we assume that monitored discrepancy indicators are permanent so that once the observed state of a discrepancy is changed, it will remain constant after that.

The aim of the diagnosis reasoning process is to find a consistent and plausible explanation of the current system 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 node states and the interval at which the node changes its state. Formally a hypothetical state at time t is a map $H_t^{V'} : V' \rightarrow \{\texttt{ON}, \texttt{OFF}\} \times \mathbb{R} \times \mathbb{R}$ where $V' \subseteq V$. Similar to actual states, hypothetical states are defined for both discrepancies and failure modes. The estimated earliest (latest) time of state change is denoted $H(v).\text{terl}$ ($H(v).\text{tlat}$).

A hypothetical state is an estimation of the current state of all nodes in the system and the time period at which each node changed its states. An estimation of the current state is valid only if it is consistent with the TFPG model. State consistency in TFPG models is a node-parents relationship that can be extended pairwise to arbitrary subsets of nodes. Formally, let $\text{Pr}(v)$ denotes the set of parents of v in a TFPG model G. We can define *observable consistency* at time t as a relation $\text{OCons}_t \subset \mathcal{P}(V) \times V$ such that $(V', v) \in \text{OCons}$ if and only if $V' = \text{Pr}(v)$ and the observable state of v is consistent with that of all its parents V' based on the map S_t and the failure propagation semantics. The observable state consistency relationship can be directly extended to any set of nodes representing a subgraph of G. In this case we overload the relationship OCons so that $\text{OCons}_t \subseteq \mathcal{P}(V)$, where for each $V' \subseteq V$:

$$V' \in \text{OCons}_t \;\; \Leftrightarrow \;\; \forall v \in V' \; (\text{Pr}_{V'}(v), v) \in \text{OCons}$$

where $\text{Pr}_{V'}(v)$ is the set of parents of v restricted to V'. The set of maximally consistent set of nodes is denoted by Φ_t where $V' \in \Phi_t$ if and only if

$$V' \in \text{OCons}_t \text{ and } (\forall V'' \subseteq V) \; V' \subset V'' \Rightarrow V'' \notin \text{OCons}_t$$

The set Φ_t can be efficiently computed incrementally based on Φ_{t-1} based on a new event e_t. The event e_t corresponds to either a new triggered monitored discrepancy or a time-out event generated when a sensor alarm is not observed with state ON while it is supposed to be based on its current hypothetical state. The underlying procedure will be denoted $\mathsf{UpdateMCO}(\Phi_{t-1}, e_t)$. Note that initially $\Phi_0 = \{V\}$.

Based on the semantics of failure propagation it is possible to define a constructive notion of *hypothetical consistency* such that given a consistent hypothetical state $H_t^{V'}$ it is possible to extend this map forward (procedure $\mathsf{BProp}(H_t^{V'}, v)$)by assigning the maximal

hypothetical state of the node v based on the hypothetical state of its parents in V', or backward (operation $\mathsf{FProp}(H_t^{V'}, v)$) by assigning the maximal hypothetical state for v' based on the state of its children in V'. The following algorithm outlines the incremental reasoning procedure.

Algorithm 1 The diagnosis procedure $\mathsf{Diag}(\Phi_{t-1}, e_t)$

$\Phi_t \leftarrow \mathsf{UpdateMCO}(\Phi_{t-1}, e_t)$
$HS_t \leftarrow \varnothing$
define
$\mathsf{In}(X) := \{v \in X | (\forall v' \in X)\ (v, v') \notin E\}$
$\mathsf{PSet}(X) := \{v \in V - X | (\exists v' \in \mathsf{In}(X))\ (v, v') \in E\}$
$\mathsf{ODC}(X) := \cup_{v \in X} \mathsf{Reach}(v) - X$
$\mathsf{TSet}(X) := \{v \in V - X | \mathsf{ODC}(X) \times v \cap E = \varnothing\}$
$\mathsf{CSet}(X) := \{v \in \mathsf{TSet}(X) | (\exists v' \in X)\ (v', v) \in E\}$
end define
for all $V' \in \Phi_t$ **do**
  $H \leftarrow S_t|_{V'}$
  while $\mathsf{PSet}(V') \neq \varnothing$ **do**
    select v from $\mathsf{PSet}(V')$
    $H \leftarrow \mathsf{BProp}(H, v)$
    $V' \leftarrow V' \cup \{v\}$
  end while
  while $\mathsf{CSet}(V') \neq \varnothing$ **do**
    select v from $\mathsf{CSet}(V')$
    $H \leftarrow \mathsf{FProp}(H, v)$
    $V' \leftarrow V' \cup \{v\}$
  end while
  for all $v \in V - V'$ **do**
    $H(v).\mathrm{state} \leftarrow \mathtt{OFF}$
    $H(v).\mathrm{terl}, H(v).\mathrm{terl} \leftarrow 0$
  end for
  $HS_t \leftarrow HS_t \cup \{H\}$
end for
return Φ_t, HS_t

In the above algorithm, for a given subset, X, of the TFPG nodes, $\mathsf{In}(X)$ is the set of all nodes in X that do not have children in X. These nodes forms the interior boundary for X. $\mathsf{PSet}(X)$ is the set of all nodes outside X that are connected (as children to the interior boundary of X, $\mathsf{In}(X)$. $\mathsf{ODC}(X)$ is the set of nodes outside X that is reachable from nodes inside X ($\mathsf{Reach}(v)$ is the set of nodes reachable from v). $\mathsf{TSet}(X)$ is the set of terminal nodes (those without children in the TFPG model) outside of X that are reachable from X. $\mathsf{CSet}(X)$ is the set of terminal nodes outside of X that are directly connected (as a child) to a node from X.

The above diagnosis algorithm returns a set of new hypotheses that can consistently explain the current observed state of the TFPG system. A failure report is then generated from the computed set of hypotheses HS_t. The failure report enlists the set of all consistent state assignments that maximally matches the current set of observations. Any observed state that does not match the current hypothesis is considered faulty. A detailed description and analysis of the diagnosis algorithm can be found in (Abdelwahed *et al.*, 2005).

3.1 Hypotheses Ranking

The quality of the generated hypotheses is measured based on three independent factors:

- *Plausibility* is a measure of degree to which a given hypothesis group explains the current fault signature. Plausibility is typically used as the first metric for sorting the hypotheses, focusing the search on the failure modes that explain the data that is currently being observed.
- *Robustness* is a measure of the degree to which a given hypothesis is expected to remain constant. Robustness is typically used as the second metric for sorting the hypotheses, helping to determine when to take action to repair the system.
- *Failure Rate* is a measure of how often a particular failure mode has occurred in the past.

The plausibility metric considers two independent factors, namely, alarm consistency and failure mode parsimony. The alarm consistency factor is defined as the ratio of the active consistent alarms to that of all (currently) identified alarms. The failure mode factor is defined as the ratio of identified failure modes (according to the underlying hypothesis) to the total number of failure modes in the system. This factor is a direct representation of the parsimony principle (a hypothesis with the least number of failed components is more plausible). Hypotheses plausibility metrics are ordered, with the alarm consistency factor being the most dominant.

The diagnoser selects the current set of hypothesis incrementally in an attempt to improve the current plausibility measure. In other words, the diagnoser will update a given hypothetical state map only if such update can increase the plausibility of the underlying hypothesis. In addition, changes are restricted so that the updated hypothesis remains valid.

4 ASPECTS OF FAILURE PROGNOSIS IN TFPG MODELS

In general, the aim of failure prognosis is to estimate the system reliability, given a set of conditions and observations, by assessing how close the system is to a critical manifestation of current failures. The reliability estimation can then be used to reconfigure the system, change the operating settings, or schedule specific maintenance procedures targeting the faulty components. In the TFPG modeling and reasoning settings, the prognosis problem and the associated reliability measure can be defined based on three main factors, namely failure criticality levels, diagnosis or hypothesis plausibility, and the time distance from the current state to the critical failure.

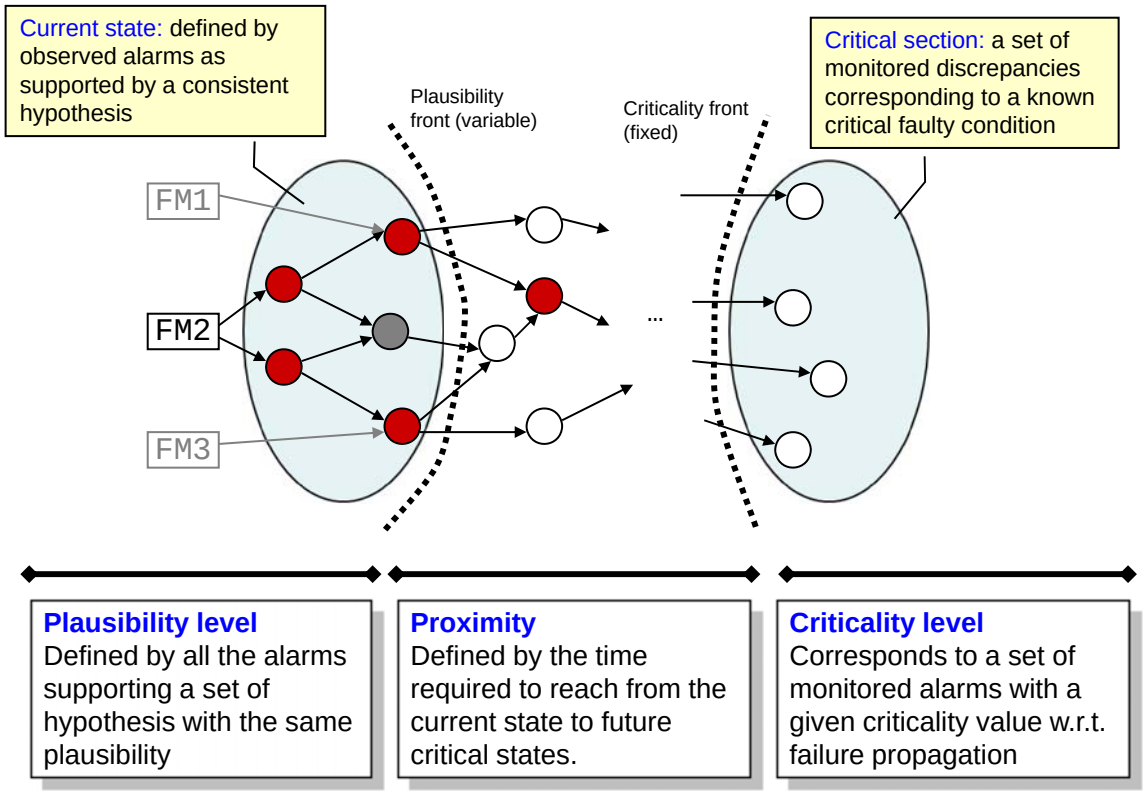

Figure 2: The main factors affecting the evaluation of the system reliability for TFPG models.

The first factor addresses the fact that different sections of the system may correspond to different levels of criticality with respect to system operation. These sections can be identified using a measure of criticality level for all discrepancies in the systems. The second factor address the current estimated (diagnosed) condition of the system and the plausibility of the corresponding hypothesis. The third factor, is the timing proximity of the current estimated state relative to a given critical region of the system. All these factor directly contribute to the reliability of the system at a given time. These three factors as illustrated in Figure 2. We will discuss these factors in details in the reminder of this section.

4.1 Failure Criticality

In typical practical situations, failure progresses starting from the initial failure modes into several stages with increasing level of criticality. To capture this situation, we define the map $\mathsf{CL} : D \to \mathbb{N}$ that assign to each discrepancy, $d \in D$, a criticality level $\mathsf{CL}(d)$. The lowest criticality level, 0, is reserved for non-critical discrepancies and all failure modes. To capture the increasing criticality with respect to propagation depth, we assume that

$$(\forall d', d \in D) \quad (d', d) \in E \longrightarrow \mathsf{CL}(d') \leq \mathsf{CL}(d)$$

The above condition states that if d' is a parent of d in a TFPG model then the criticality level of d' should be less than of equal to that of d. As a consequence, the criticality levels along any given path in a TFPG model form a monotonically increasing sequence. Note that we only assign a criticality level to all monitored and non-monitored discrepancies D and assign failure modes the default 0.

Based on the definition of criticality levels, we can define *criticality fronts* associated with a given TFPG model by the map, $\mathsf{CF} : \mathbb{N} \to \mathcal{P}(D)$, as follows.

$$(\forall d \in D) \quad d \in \mathsf{CF}(n) \quad \longleftrightarrow \quad \mathsf{CL}(d) \geq n \text{ and } (\forall (d', d) \in E)\ \mathsf{CL}(d') \leq n$$

The set of criticality fronts are essentially the codomain of the above map, and the set of criticality front levels CFL are the set $\{n \in \mathbb{N} \mid \mathsf{CF}(n) \neq \varnothing\}$. It can be shown that CFL corresponds bijectively to the codomain of CL. Based on the above definitions, a criticality front level, $n \in \mathbb{N}$, corresponds to a graph cut of the TFPG model in which the nodes on one side of the cut have criticality levels less than n and the remaining nodes have criticality level greater than or equal to n. Figure 3 shows an example TFPG model with assigned criticality levels and the corresponding criticality fronts.

Criticality levels are typically assessed based on the requirements for system operation and functionality. In particular, the criticality value for a given discrepancy depends on the operation cost associated with the

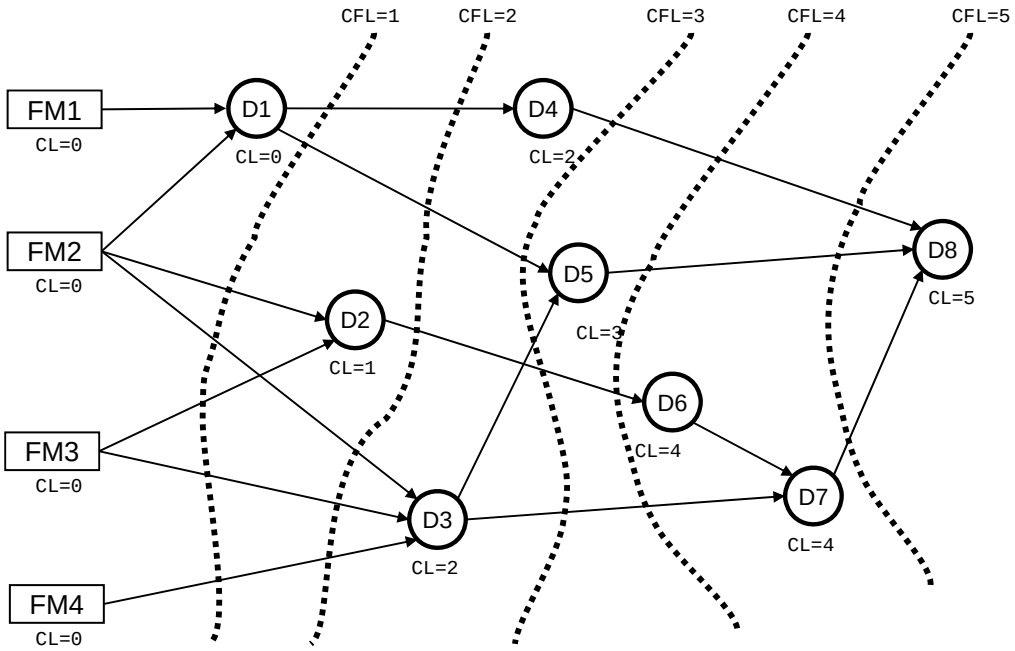

Figure 3: A TFPG model with assigned criticality levels and the corresponding criticality fronts.

fault reaching and progressing from the discrepancy. This will include the cost of maintenance, reconfiguration, and recovery when applicable. However, in some situations, it is not possible to have a precise value for the criticality of a sensor. In such situations, an enumeration of criticality levels (ex. low, medium, and high) can be used to distinguish between sensors with respect to fault severity. Such enumeration can be assigned an approximate integer value, that reflects its relative importance, which can be used later to compute a reliability measure for the system, in terms of the remaining useful life (RUL) or the time to criticality, as discussed later in this paper.

4.2 State Estimation Plausibility

As discussed in the previous section, the TFPG reasoning algorithms relies on sensor signals (alarms) and the TFPG model structure to identify the most plausible estimates of the current system condition as a set of state hypotheses. The plausibility of each hypothesis is defined based on the number of supporting sensor signals (alarms) versus the inconsistent and missing ones. We will write $A(H)$ for the set of discrepancies (monitored or not) that are presumed active (ON) according to the H and $I(H)$ for the set of discrepancies (monitored or not) that are presumed inactive (OFF) according to H. That is,

$$A(H) = \{d \in D \mid H(d).\text{state} = \texttt{OFF}$$

The state front of a hypothesis H is denoted SF_H and is defined as a set of discrepancies $D' \subseteq D$ such that $(\forall d \in \mathsf{SF}_H)$

$$d \in A(H) \text{ and } (\exists (d, d') \in E)\ d' \in I(H)$$

That is, the state front SF_H is the set of discrepancies that are currently active as estimated by H but some of their children discrepancies are not active according to H. Given that any discrepancy in D can either be in $A(H)$ or $I(A)$ but not both. The set SF_H is well-defined and the boundary line between D' and $D - D'$ forms a graph cut for the underlying TFPG model.

The intuitive meaning of the state front for a hypothesis, is that all the discrepancies on this front are have the same likelihood of being active at the current time and they are forming the front of fault propagation in the sense that they are the discrepancies that could become active based on the next set of alarms as the fault propagation continues to progress.

The plausibility of a state front is equal to the plausibility of the underlying hypothesis. As it is possible that several hypotheses can have the same plausibility level, several state front may have the same plausibility level.

4.3 Time Proximity

The time proximity factor measures how close the current state of the system is to a future failure. As discussed earlier, future failures are identified by their criticality level front as defined by the map CF. Each front is defined as a set of discrepancies at the boundary of a graph cut for the TFPG model. Similarly, the current state is defined by a set of hypotheses with a given plausibility level and is identified by the discrepancies at the boundaries of the cut formed by the underlying hypothesis level state front. Accordingly, the time proximity factor is a measure for the temporal

distance between two fronts (graph cuts) each corresponding to a set of discrepancies in the TFPG model.

To define such distance, consider two sets of discrepancies $D_1, D_2 \subseteq D$. Assuming that all discrepancies in D_1 are either ancestors of some discrepancies in D_2 or not connected to any discrepancy in D_2, we define the propagation time between D_1 and D_2 with respect to a hypothesis H, denoted $t_H(D_1, D_2)$ as the minimum time to trigger discrepancy in D_2 as a result of a set of failure propagation from discrepancies in D_1. We write $D_1 \prec D_2$ if the above condition is satisfied.

To compute $\hat{t}_H(D_1, D_2)$, we consider the set of all discrepancies that are children of D_1. We computer the earlier propagation time to these discrepancies based on the activation times of their parent nodes according to H. The computation of the earliest propagation time for all subsequent nodes continues as the earlier propagation times becomes available for their parents. The computation will continue until the earlier propagation time is computed for all the nodes in D_2. The minimum time is selected as the output. Algorithm 2 outlines the computation procedure.

Algorithm 2 The propagation time procedure $\hat{t}_H(D_1, D_2)$

assumption: $D_1 \prec D_2$
if $D_1 \cap D_2 \neq \varnothing$ **then**
  return 0
end if
define $\mathsf{RSet}(X) := \{d \in D - X | (\forall d' \in D)\ (d', d) \in E \rightarrow d' \in X\}$
$\mathtt{TNodes} = \{(d, H(d).\mathrm{terl}) \mid d \in A(H)\}$
$t_{\min} = \infty$
while $D_2 \not\subset \mathtt{TNodes}.\mathrm{nodes}$ **do**
  select d from $\mathsf{RSet}(D_1)$
  compute $\mathrm{terl}(\mathtt{TNodes}, d)$
  if $d \in D_2$ **then**
    $t_{\min} = \min(t_{\min}, \mathrm{terl}(d))$
  end if
end while
return $t_{\min}$

In algorithm 2, for a given subset of nodes X in the TFPG model, $\mathsf{RSet}(X)$ is the set of discrepancies outside of X where all their parents belongs to X. The function $\mathrm{terl}(\mathtt{TNodes}, d)$ computes the earliest time for d to be activated based on the earlier time the parents of d are activated. This function can be directly computed based on the semantics of failure propagation in TFPG models.

4.4 Time to Criticality

Given a set of criticality levels, the associated criticality fronts can be computed directly from the earlier definition. The state front for a given hypothesis can be directly computed based on the given definition. Let Y be the set of hypothesis with the highest plausibility value at a time t. We define the time to criticality level n at a give time t, denoted $\mathsf{TTC}(Y, n)$, as follows

$$\mathsf{TTC}(Y, n) = \min\{\hat{t}_H(\mathsf{SF}_H, \mathsf{CF}(n)) \mid H \in Y\}$$

That is, the time to criticality level n is the minimum of all propagation times for all hypotheses with the maximum plausibility. In practice, there are typically few enumerated criticality levels. The time to criticality, therefore, follows the increasing order of the criticality. That is, the time to reach a high criticality level is usually longer than the time to reach a lower criticality level, as expected. However, this is not always the case as shown the in Figure 4. In this example, there are three different paths from the state (estimation) front SF_H to the criticality front level 1 (CFL=1), where H is the most plausible hypothesis in which D2, D3, D4 are assumed active and D1 is assumed faulty. In this example, the time to criticality to the first level is 3 (time units) while the time to criticality for the next higher level is 1.

5 CONCLUSION

In this paper we addressed a model-based prognosis problem in the TFPG settings. We presented the three main factors that directly affect the system reliability at a given state, namely, criticality levels, current state front, and time proximity. Based on the formal definitions of these factors, we introduced an algorithm to compute the time to reach a given critical level based on the current conditions of the system. The time to criticality can be used as a measure for system reliability.

In future work we will consider a more general concept of system reliability that integrate different criticality levels as well as states with different plausibility values. We will also investigate the reliability assessment for systems in which propagation times are not provided. In another research direction we will investigate the problem of sensor assignment to achieve certain minimum time to criticality levels at specific system conditions.

ACKNOWLEDGMENTS

The authors would like to thank Timothy J. Wilmering and Stanley Ofsthun for their helpful comments and discussions regarding the problem of diagnosis for TFPG models. This work is funded, in part, by Boeing.

REFERENCES

(Abdelwahed *et al.*, 2004) S. Abdelwahed, G. Karsai, and G. Biswas. System diagnosis using hybrid failure propagation graphs. In *The 15th International Workshop on Principles of Diagnosis*, Carcassonne, France, 2004.

(Abdelwahed *et al.*, 2005) S. Abdelwahed, G. Karsai, and G. Biswas. A consistency-based robust diagnosis approach for temporal causal systems. In *The*

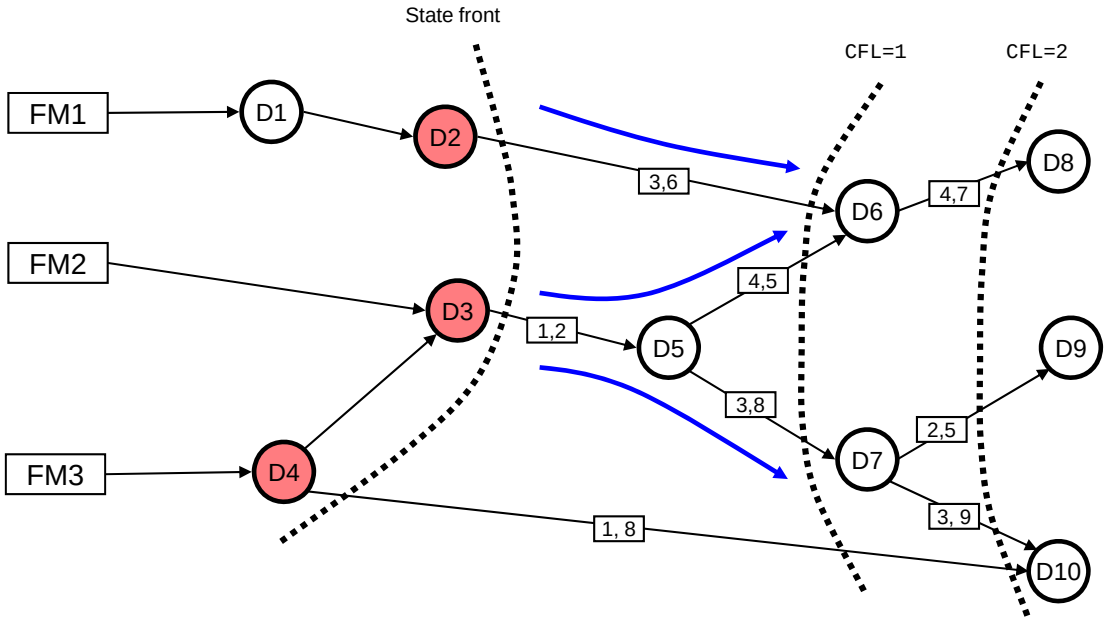

Figure 4: Time to criticality example

16th International Workshop on Principles of Diagnosis, Pacific Grove, CA, 2005.

(Chelidze *et al.*, 2002) D. Chelidze, J.P. Cusumano, and A. Charterjee. A dynamical systems approach to damage evolution tracking, part 1: The experimental method. *Journal of Vibration and Acoustics*, 124:250–257, 2002.

(ISO-13381-1, 2004) ISO-13381-1. Condition monitoring and diagnostics of machines - prognostics - part1: General guidelines. Int. Standard, 2004.

(Jardine and Lin, 2006) A. K. S. Jardine and D. Lin. A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mechanical Systems and Signal Processing*, 20(7):1483–1510, 2006.

(Karsai *et al.*, 2003) G. Karsai, G. Biswas, and S. Abdelwahed. Towards fault-adaptive control of complex dynamic systems. In T. Samad and G. Balas, editors, *Software-Enabled Control: Information Technology for Dynamical Systems*, chapter 17. IEEE publication, 2003.

(Lebold and Thurston, 2001) M. Lebold and M. Thurston. Open standards for condition-based maintenance and prognostic systems. In *5th annual maintenance and reliability conference*, Gatlinburg, USA., 2001.

(Luo *et al.*, 2003) J. Luo, M. Namburu, K. Pattipati, L. Qiao, M. Kawamoto, and S. Chigusa. Model-based prognostic techniques. In *Proc. of IEEE AUTOTESTCON*, pages 330–340, 2003.

(Medjaher *et al.*, 2009) K. Medjaher, J.-Y. Moya, and N. Zerhouni. Failure prognostic by using dynamic bayesian networks. In *2nd IFAC Workshop on Dependable Control of Discrete Systems, DCDS'09*, Bari, Italy, 2009.

(Misra *et al.*, 1994) A. Misra, J. Sztipanovits, and J. Carnes. Robust diagnostics: Structural redundancy approach. In *SPIE's Symposium on Intelligent Systems*, 1994.

(Muller *et al.*, 2008) A. Muller, M.C. Suhner, and B. Iung. Formalisation of a new prognosis model for supporting proactive maintenance implementation on industrial system. *Reliability Engineering and System Safety*, 93:234–253, 2008.

(Ofsthun and Abdelwahed, 2007) S. Ofsthun and S. Abdelwahed. Practical applications of timed failure propagation graphs for vehicle diagnosis. In *IEEE Systems Readiness Technology Conference, Autotestcon'07*, pages 250–259, Baltimore, MD, September 2007.

(Padalkar *et al.*, 1991) S. Padalkar, J. Sztipanovits, G. Karsai, N. Miyasaka, and K. C. Okuda. Real-time fault diagnostics. *IEEE Expert*, 6(3):75–85, 1991.

(Provan, 2003) G. Provan. Prognosis and condition-based monitoring: an open systems architecture. In *5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, 2003.

(Vachtsevanos *et al.*, Wiley Sons) G. Vachtsevanos, F. L. Lewis, M. Roemer, A. Hess, and B. Wu. *Intelligent Fault Diagnosis and Prognosis for Engineering Systems*, volume 2006. Intelligent Fault Diagnosis and Prognosis for Engineering Systems., New Jersey, Hoboken, Wiley & Sons.

(Vichare and Pecht, 2006) N. Vichare and M. Pecht. Prognostics and health management of electronics. *IEEE Transactions on Components and Packaging Technologies*, 29(1):222–229, 2006.

Sherif Abdelwahed is an Assistant Professor with Electrical and Computer Engineering Department at Mississippi State University. He received his Ph.D. degree in Electrical and Computer Engineering from the University of Toronto, Canada, in 2002. From 2000 to 2001, he was a research scientist with the system diagnosis group at the Rockwell Scientific Company. From 2002 to 2007 he worked as a research assistant professor with the Institute for Software Integrated Systems at Vanderbilt University. He conducts research on model-based design and analysis of self-managing computation systems. His research interests also include modeling and analysis of distributed real-time systems, automated verification, model-based fault diagnosis and prognosis techniques, and model-integrated computing. He has published over 75 publications. He is a senior member of the IEEE and member of Sigma Xi.

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 has over twenty-five years of experience in software engineering. He conducts research in the design and implementation of embedded systems, in programming tools for visual programming environments, in the theory and practice of model-integrated computing. He received his BSc, MSc, and Dr. Techn. degrees from the Technical University of Budapest, in 1982, 1984 and 1988, respectively, and his PhD from Vanderbilt University in 1988. He has published over 100 papers, and he is the co-author of four patents. He has worked on several large projects in the recent past, including one on fault-adaptive control technology that has been transitioned into aerospace applications, and another one on the model-based integration of embedded systems whose resulting tools are being used in embedded software development tool chains worldwide.