A Novel Framework for Integrating Discrete Event System Control and Diagnosis

Gregory Provan*
Rockwell Scientific Company
1049 Camino Dos Rios, Thousand Oaks, CA 91360

1 Towards an Integrated Control/Diagnosis Framework

Diagnosis of discrete event systems (DES) is an important task, with several desiderata that include the ability to (1) encode both control and diagnosis properties within a single representation, and (2) to compose system models from component models in a simple and efficient manner, e.g., without the kind of state explosion that can occur during parallel composition of component Finite State Machines (FSMs).

Many formalisms have been proposed for the Model-Based Diagnosis (MBD) of a DES, but each has drawbacks. The representations based on FSMs, e.g., [Sampath *et al.,* 1995], have a clear control semantics but suffer from incompletely-specified diagnostic semantics and state explosion during model composition. MBD representations, e.g., [Darwiche, 1998], have been used to model DESs using space-efficient compositional methods [Darwiche and Provan, 1996], but lack well-developed control-theoretic specifications.

This article proposes a framework based on FSMs that has a clear control and diagnostics semantics, yet enables model composition without state-space explosions. We propose a two-level modeling framework, based on a system hypergraph *H* that can serve as a generator for MBD and FSM models. *H* specifies the component causal relations using the graphical framework described within causal networks (CN) [Darwiche, 1998], whereby we can clearly specify independence relations for system variables, and as a consequence compose system models with system state spaces limited through independence relations. Our representation is not significantly more complex than that of either FSM or CN alone, yet is equivalent to both these representations. We introduce to MBD modeling additional requirements for specifying control transitions, and to FSM modeling requirements on state descriptions and causal independence of components.

2 A Discrete Event Modeling Framework

We adopt a representation that is a hybrid of two key modeling approaches, an MBD approach, Causal Networks (CN) [Darwiche, 1998], and an FSM control/diagnosis approach [Sampath *et ai.,* 1995].

*email: gprovan@rwsc.com

We propose a two-level, component-based framework to model complex discrete event systems.' Our higher level system representation, termed System Causal Graph (SCG), provides a well-defined approach (based on bond graphs) for describing the high level component (or sub-system) configurations and the physical/causal inter-relations of the components (or sub-systems). We model the behaviors of individual components using a lower level representation, called a Control Causal Network (CCN). The CCN models can be converted into regular Finite State Machines or Propositional Logics for further analysis using FSM-based discrete event system techniques *(e.g.,* supervisory control theory) or model-based reasoning techniques *(e.g.,* CN diagnostics), respectively [Provan and Chen, 2003]. The behaviors of the complete system are described by (the composition of) the individual component models.

2.1 Component-Based Modeling Approach

This section describes the CCN framework we adopt for modeling the components of a system. This representation adopts the CN graphical structure and diagnostics specifications, and encodes propositional equations for each node in the graph based on an extension of FSMs. To explain our framework, we first briefly introduce CNs and FSMs.

We adopt the CN model specification [Darwiche, 1998], called a *system description* Φ, which defines a tuple $(P, \mathcal{G}, \Psi)$, where (a) *P* is a finite set of discrete-valued variables comprising two disjoint variable types: P_m represents the failure modes of the components, and $P_{\tilde{m}}$ represents system properties other than failure modes; (b) $\mathcal{G}$ is a directed acyclic graph that defines the causal relations over the variables in P; (c) Ψ is a set of propositional sentences, the *domain axioms,* constructed from members in *P.* This approach has a number of important properties, such as compositional modeling based on the independence properties specified in $\mathcal{G}$: if component i has behavior equations Ψ_i, then the system behavior is specified simply by the union of the component equations, i.e., $\Psi = \cup_i \Psi_i$ [Darwiche, 1998], Specifications of, and algorithms for computing a diagnosis, minimal diagnosis, etc., are all well-defined [Darwiche, 1998].

An FSM is defined as $G = (Q, \Sigma, \delta, q_0)$, where Q is the state space, Σ is the set of events, δ is the partial transi-

'Our approach can be easily expanded into a multi-level nested hierarchical structure to accommodate more complex systems.

tion function $\delta : Q \times \Sigma \rightarrow Q$ (and defines the transitions between states in Q), and q_0 is the initial state of the system. This framework has been extended for failure diagnosis through the use of unobservable failure transitions and auto-construction of an observer G_{diag} [Sampath *et al.*, 1995].

In our hybrid representation, we model each component using a control causal network (CCN) consisting of a tuple $(P, \{\Sigma, Q, \Gamma, \delta, (q_o, p_o), Q_m\}, \mathcal{G}, \Psi)$, where *P* is the set of parameters, Σ is the event set, *Q* the state set, T the set of guards (or pre-conditions), $\delta : \Sigma \times Q \times \Gamma \times P \rightarrow Q \times P$ the transition function, q_o the initial state, p_o the initial value of parameters, Q_m the marked states, $\mathcal{G}$ a graph, and Ψ a set of propositional equations.[2] Parameters in the parameter set *P* are discrete-valued, and guards $\gamma \in \Gamma$ are predicates on the parameters in *P*. We can view δ as a set of transitions. An equation describing transition $\tau \in \delta$, denoted $\gamma_\tau \wedge \sigma_\tau \Rightarrow f_\tau(p)$, can be interpreted as follows: If at state *q* the guard γ_τ is true and the event σ_τ occurs, then the next state is q' and the parameters at q' will be updated to $f_\tau(p)$. We call the functions $f_\tau(p)$ the *actions* of the transition τ. The set of all sequences of event labels (traces) of a CCN given initial parameter setting p_Q is the language *L* it generates. We have shown in [Provan and Chen, 2003] that this representation possesses the control-theoretic properties of the finite state machine with parameters representation, and is based on standard propositional logic with well-known semantics.

2.2 System Causal Graph

An SCG $\mathcal{H} : (\mathcal{N}, \mathcal{E})$ is a directed graph whose nodes in $\mathcal{N}$ represent the components of the system and whose edges in $\mathcal{E} : \mathcal{N} \times \mathcal{N}$ denote the causal relations between the components. A node $N_i \in \mathcal{N}$ is associated with a CCN component model A_i which represents the component's behaviors.

The SCG's graph $\mathcal{H}$ has properties similar to those of the graph G of a CCN. $\mathcal{H}$ must preserve a number of control and simulation/diagnostics properties.[3] As an example, in order to prevent possible ambiguity and direct circularity in the causal semantics, we assume that the system represented in an SCG should be structured such that any component in the SCG may not be *both* the (direct) predecessor *and* the (direct) successor of the same component in the SCG.

3 Properties of Integrated Representation

In the full paper [Provan and Chen, 2003 J, we prove a number of important properties of the SCG. One key property involves the sound FSM and CN models that can be generated, where by sound we mean that the model obeys the syntactic and semantic requirements of the (FSM or CN) representation in question:

[2]The definition is a discrete-parameter restriction of Finite State Machines with Parameters [Chen and Lin, 2000], such that we use a logical representation for state transitions. Our representation extends the representation and control semantics of the causal network models defined in [Darwiche and Provan, 1996] by adding an explicit transition framework for each CN sentence in Ψ.

[3]The full paper, [Provan and Chen, 2003], discusses $\mathcal{H}$ and its properties in detail.

Lemma 1 *Mapping an SCG into an FSM (CN) produces a sound system-level FSM (CN), respectively.*

To show the CN model created by the above procedure is equivalent to the FSM model, we show that they generate the same language.

Theorem 1 *Given an FSM G and a CN model Φ generated from an SCG with initial setting (q_0, p_0), the FSM and CN languages are equal, i.e., $L(G, q_0) = L(\Phi, p_0)$.*

From a control perspective, this means that the FSM and CN possess the same control properties, e.g., livencss, correctness, etc. From a plant modeling perspective, we can use the logical representation of the SCG to validate a plant model using a theorem prover.

In addition, [Provan and Chen, 2003] shows the equivalence of diagnostic capabilities of the generated models. We assume that, to perform fault isolation, for the FSM (CN) approach we use a diagnoser G_{diag} (CN model Φ), respectively.

Theorem 2 *If we map an SCG into a FSM G and a CN model Φ, then: (a) Given observation set Θ, G is diagnosable (i.e., we can isolate failure events) iff Φ is diagnosable; (b) Given observation set Θ, the set of diagnoses for G is equivalent to the set of diagnoses for Φ.*

This result means that we can now establish equivalent diagnostic capabilities between an FSM and a CN representation, if they can be encoded by the same SCG. Hence, the important MBD properties, e.g., completeness and soundness of diagnostics given a model Φ, can be inherited by an appropriate FSM model.

In summary, these properties indicate that this approach acquires the control semantics of FSMs, and the diagnostic semantics of CNs. On the practical side, although we can generate and use algorithms for either FSM or CN models, further research is necessary to identify the model type most appropriate to a particular class of applications, since model/algorithm efficiency is domain-dependent. In addition, we need to analyze the tradeoffs associated with the extra modeling requirements of the SCG graphical framework versus the linear (rather than worst-case exponential, as in an FSM) growth associated with system model composition.

References

[Darwiche and Provan, 1996] A. Darwiche and G. Provan, Exploiting system structure in model-based diagnosis of discrete event systems. In *Proc. 7th Intl. Workshop on Principles of Diagnosis,* pages 95-105 1996.

[Darwiche, 1998] Adnan Darwiche. Model-based diagnosis using structured system descriptions. *Journal of Artificial Intelligence Research,* 8:165-222 1998.

[Chen and Lin, 2000] Y.-L. Chen and F. Lin. Modeling of Discrete Event Systems using Finite State Machines with Parameters. In *Proc. IEEE Confon Control Applications*, pages 941-946, Anchorage, AK, September 2000.

[Provan and Chen, 2003] G. Provan and Y-L. Chen. A general modeling framework for model-based reasoning and discrete event systems analysis. Technical Report SCTR-03-21, Rockwell Scientific Company, March 2003.

[Sampath *et al.,* 1995] M. Sampath, R. Sangupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosibility of discrete event systems. *IEEE Transactions on Automatic Control,* 40(9): 1555-1575, September 1995.