Annual Reviews in Control 000 (2018) 1–10

Contents lists available at ScienceDirect

Annual Reviews in Control

journal homepage: www.elsevier.com/locate/arcontrol

# On the history of diagnosability and opacity in discrete event systems☆

Stéphane Lafortune[a,*], Feng Lin[b], Christoforos N. Hadjicostis[c]

[a] Department of EECS, University of Michigan, Ann Arbor, USA
[b] Department of ECE, Wayne State University, Detroit, USA
[c] Department of ECE, University of Cyprus, Nicosia 1678, Cyprus

ARTICLE INFO

*Article history:*
Received 11 January 2018
Revised 12 March 2018
Accepted 3 April 2018
Available online xxx

*Keywords:*
Discrete event systems
Fault diagnosis
Diagnosability
Opacity
Petri nets
History of discrete event systems

ABSTRACT

This paper presents historical remarks on key projects and papers that led to the development of a theory of event diagnosis for discrete event systems modeled by finite-state automata or Petri nets in the 1990s. The goal in event diagnosis is to develop algorithmic procedures for deducing the occurrence of unobservable events, based on a formal model of the system and on-line observations of its behavior. It also presents historical remarks on the early works on the property of opacity, which occurred about ten years later. Opacity can be seen as a strong version of lack of diagnosability and it has been used to capture security and privacy requirements. Finally, diagnosability is connected with the property of observability that arises in supervisory control. This paper is part of set of papers that review the emergence of discrete event systems as an area of research in control engineering.



## 1. Introduction

We were invited to provide historical remarks on the emergence of the theories of diagnosability and opacity for event-driven dynamic systems, in the context of the special section in *Annual Reviews in Control* on the emergence of discrete event systems as an area of research in control engineering. The discussion herein is not meant to be a survey of these theories. The two papers Zaytoon and Lafortune (2013) and Jacob, Lesage, and Faure (2016) should be consulted in that regard. Instead, our focus is on presenting key events and papers from the 1990s that led to the definition of a formal notion of diagnosability, and later opacity, which have withstood the test of time and are still the object of current research.

We start by presenting the emergence of fault diagnosis and diagnosability using automata models of discrete event systems. We then transition to similar historical remarks on the notion of opacity and its verification when using automata models. Opacity, which is closely related but stronger than non-diagnosability, originated in the formalization of information flow security properties in computer systems in the early 2000s (cf. Mazaré, 2004a; Ryan & Peacock, 2006) and since then it has attracted considerable attention in the control engineering community. In a subsequent section, we also include brief historical remarks on parallel activities on fault diagnosis and opacity using Petri net models of discrete event systems. We conclude with a discussion on (i) the relationship between diagnosability and the property of observability that arises in supervisory control, and (ii) recent efforts on networked discrete event systems.

Our presentation is focused on events that we personally experienced or witnessed. In the discussion that follows, whenever possible, we cite the first journal paper on the topic being discussed; quite often, this first journal paper was preceded by one or more conference papers that are not cited.

This paper is an expanded version of Lafortune and Lin (2017), with additional discussions throughout, as well as the inclusion of a new section on diagnosability and opacity for Petri net models.

## 2. History of diagnosability

### 2.1. The beginning

From our own perspectives, the development of the theory of diagnosability reviewed in this paper was highly influenced by two key events: (i) the extended visit of Feng Lin at Ford Motor Co. in Dearborn, US, in the summer of 1992; and (ii) the year-long

☆ The authors' research is principally supported by the US National Science Foundation and the European Commission.

* Corresponding author.
*E-mail addresses:* stephane@umich.edu (S. Lafortune), flin@wayne.edu (F. Lin), chadjic@ucy.ac.cy (C.N. Hadjicostis).

https://doi.org/10.1016/j.arcontrol.2018.04.002
1367-5788/

sabbatical visit of Kasim Sinnamohideen of the research group of Johnson Controls Inc. (Milwaukee, US) at the University of Michigan in Ann Arbor in academic year 1992-93, where he collaborated with Stéphane Lafortune, Demosthenis Teneketzis, and two doctoral students at the time, Meera Sampath and Raja Sengupta.

At the time, the two main approaches for fault diagnosis were the quantitative approach in control engineering based on continuous models and the qualitative approach used in artificial intelligence based on static models.

At Ford Motor Co., there was interest in on-board diagnostics to detect and isolate (i.e., diagnose) component faults in complex processes such as the exhaust gas recirculation system, during the operation of the vehicles, i.e., "on-line". At Johnson Controls Inc., there was similar interest for Heating, Ventilation, and Air Conditioning (HVAC) systems, where faulty components are typically difficult to access. Common to these applications of interest was the fact that sensor information was limited and hence diagnosis would require inferencing from limited sensor data using a suitable model of the dynamic system under consideration. Sinnamohideen advocated that using dynamic but high-level "discrete-transition-based" models of HVAC systems, rather than detailed continuous models based on differential equations, was the right approach for diagnosing "sharp" faults, such as valves that get stuck open or closed, pumps that fail on or off, controller modules that fail on or off, and so forth. The thesis was that such discrete-event model-based inferencing would be complementary to other diagnostic approaches that would track "finer" faults, such as slow drifts of sensors for instance.

The work of Lin at Ford Motor Co. lead to a framework of diagnosis using states to model faults (Lin, 1994). The state set is divided into subsets or cells. Some cells represent normal operation, other cells represent various faults. The goal of diagnosis is to determine which cell the system is in after observation of some observable events. This approach was later used in mixed-signal circuit testing, where both digital circuits and analog circuits are modelled as discrete event systems in a uniform way (Lin, Lin, & Lin, 1997).

The group at the University of Michigan, inspired by the work of Lin (1994) and aptly guided by the practical expertise of Sinnamohideen, formulated and investigated a notion of *diagnosability* for discrete event dynamic systems modeled in the framework of regular languages and their finite-state automata representations. This effort led to the doctoral dissertation of Sampath and to the two companion journal papers (Sampath, Sengupta, Lafortune, Sinnamohideen, & Teneketzis, 1995; 1996). We now discuss some aspects of that work.

**Definition of Diagnosability:** First, we state the definition of diagnosability. Consider a system modeled by an automaton, denoted by $G$, and where $\mathcal{L}(G)$ is the language generated by $G$, and where natural projection $P$ erases the unobservable events. There are several fault events to diagnose, corresponding to the set $\Sigma_f$, which is partitioned in several fault types according to $\Pi_f$. Formally, as originally stated in Definition 1 in Sampath et al. (1995), we have:

**Definition 1** (Diagnosability (Sampath et al., 1995))**.** A prefix-closed and live language $L$ is said to be *diagnosable* with respect to the projection $P$ and with respect to the partition $\Pi_f$ on $\Sigma_f$ if the following holds

$$(\forall i \in \Pi_f)(\exists n_i \in \mathbb{N})[\forall s \in \Psi(\Sigma_{fi})](\forall t \in L/s)[\ ||t|| \geq n_i \Rightarrow D\ ]\ , \tag{1}$$

where the diagnosability condition $D$ is

$$\omega \in P_L^{-1}[P(st)] \Rightarrow \Sigma_{fi} \in \omega\ . \tag{2}$$

Explanation of notation: (i) $\Psi(\Sigma_{fi})$ is the set of strings that end with a fault event of type $i$; (ii) $L/s$ is the set of all strings $t$ such that $st \in L$; (iii) $||t||$ is the length (number of events) of $t$; (iv) $P_L^{-1}[P(st)]$ is the set of all strings in $L$ whose projection under $P$ is the same as that of $st$; (v) $\Sigma_{fi} \in \omega$ means that string $\omega$ contains a fault event of type $i$.

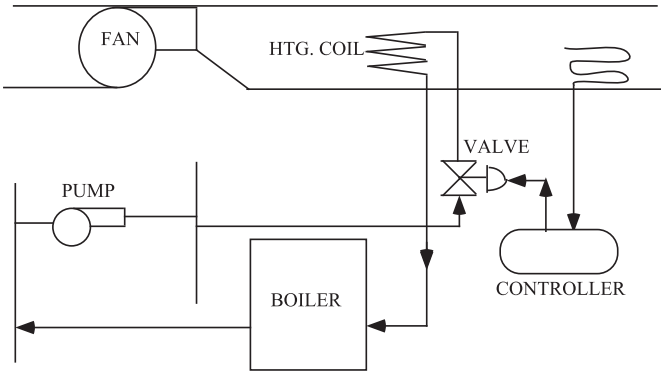


**Fig. 1.** Heating part of an HVAC system, as studied in Sampath et al. (1995).

Simplifying the above definition to eliminate "fault types" and considering a single event $f$ to diagnose, we get:

**Definition 2 (Diagnosability of event *f*).** Event $f$ is diagnosable in live language $L = \mathcal{L}(G)$ w.r.t. projection $P$ if the following holds

$$(\exists n \in \mathbb{N})(\forall s : f \in s)(\forall t \in L/s)[\ ||t|| \geq n \Rightarrow D\ ]\ , \tag{3}$$

where the diagnosability condition $D$ is

$$\omega \in P^{-1}[P(st)] \cap \mathcal{L}(G) \Rightarrow f \in \omega\ . \tag{4}$$

The set $P^{-1}[P(st)] \cap \mathcal{L}(G)$ is the best estimate of what the system could have done based on observing $st$. In words, the definition of diagnosability for a single event $f$ is then:

> An unobservable (fault) event $f$ is diagnosable in language $\mathcal{L}(G)$ if *every* occurrence of $f$ can be detected with *certainty* in a *bounded* number of events *after* its occurrence.

This notion of diagnosability is strong and invokes the universal quantifier twice: *for every* trace of events that ends with a fault event and *for every* continuation of that trace, the fault in question must *eventually* be diagnosed. Since logical discrete event models were employed, "eventually" was quantified by counting the number of events (either observable events or all events as in the above definitions) after the fault event; the existential quantifier captures the existence of such a bound, denoted by $n$, over the entire system language.

This language-based definition of diagnosability proved to be adaptable to extensions to different modeling formalisms and diagnostic architectures, as the ensuing work performed in the control engineering and artificial intelligence communities shows.

**Model-Building for Diagnosability:** During the development of the results in Sampath et al. (1995, 1996), the authors spent significant efforts on building suitable discrete event models for the purpose of fault diagnosis, using the application area of HVAC systems as a guide. The objective was to capture all available information for nominal behavior and for faulty behavior, including information from sensor readings, in the form of traces of events generated by a finite-state automaton, i.e., in a regular language. The initial example that was analyzed was the heating part of an HVAC system, as depicted in Fig. 1, where the system components of interest were: controller, valve, pump, boiler, fan, and heating coil. The sensors available (not indicated in the figure) were a flow sensor for the heating coil and a pump pressure sensor.

Faults (not their symptoms) were explicitly modeled by *unobservable* events; this included potentially faulty sensors themselves. Faulty behavior was also modeled, including: (i) the be-