DIAG-IPF: A Software Tool for Fault Diagnosis of Discrete Event Systems

Abderraouf Boussif, Mohamed Ghazel

DIAG-IPF: A Software Tool for Fault Diagnosis of Discrete Event Systems

Abderraouf Boussif[1] and Mohamed Ghazel[1]

IFSTTAR, Cosys/Estas, F-59650 Villeneuve d'Ascq, France
{abderraouf.boussif, mohamed.ghazel}@ifsttar.fr

Abstract

DIAG-IPF is the acronym that stands for ***DIAG****nosability analyzer of discrete event systems - for* ***I****ntermittent and* ***P****ermanent* ***F****aults*. This software tool has been developed in order to demonstrate/illustrate several academic researches which handle the basis issues in fault diagnosis of discrete event systems [1, 2, 3], namely diagnosability analysis and online diagnosis. Diagnosability is an intrinsic property of the system to be diagnosed. It refers to the ability of the diagnosis/monitoring device to infer, from the observable part of the system behavior, the occurrence of faults. Online diagnosis consists in inferring the occurrence of predetermined faults from the online observed behavior of the system using either a compiled diagnoser (*synthesized offline*) or an interpreted one (*computed online*).

DIAG-IPF implements several approaches for analyzing diagnosability and/or synthesizing diagnosers regarding permanent and intermittent faults. A fault is considered as permanent when it occurs but does not disappear, i.e., the system remains in faulty behavior until repairing measures are undertaken. In contrary, an intermittent fault corresponds to the case where the fault occurs and then suddenly disappears and this process continues happening in a repeated manner. Therefore, the system switches between normal and faulty behaviors.

Actually, almost all of the approaches/algorithms implemented in the software tool were developed in Boussif's thesis [4]. Hereafter, we give a succinct description of the implemented approaches:

• *A twin-plant based approach, to analyze diagnosability of permanent/intermittent faults* [5, 6]*:* the approach is based on the computation of a non-deterministic automaton called twin-plant. In fact, the twin-plant simply consists of two synchronized copies of the system model, i.e., a strict parallel composition according to observable events. The twin-plant structure is then exploited to analyze diagnosability by seeking for '*bad*' cycles (*called F-confused cycles, of infinite critical pairs*). An F-confused cycle is composed exclusively of ambiguous states, i.e., a twin-plant states which contain one normal and one faulty system states. Using the twin-plant, diagnosability of permanent faults can be checked using a polynomial algorithm, while the algorithms complexities for intermittent faults diagnosability depend on the property to be checked.

• *A diagnoser-based approach to analyze diagnosability of permanent faults* [4]: the approach is based on the computation of a new diagnoser variant (a deterministic automaton) that explicitly separates the normal states from the faulty ones in each diagnoser state. Such a diagnoser structure allows us to independently track the normal and the faulty traces directly in the diagnoser. The diagnoser is used for (on the fly) analyzing diagnosability properties by checking the absence of ambiguous cycles, called indeterminate cycles. Once a system model is checked to be diagnosable, the diagnoser is then used to perform the online diagnosis. Such an approach checks diagnosability properties using an exponential algorithm.

• *A diagnoser-based approach to analyze diagnosability of intermittent faults* [4, 7] *(in progress):* this approach is an extension of the diagnoser-based approach in order to deal with various intermittent fault diagnosability properties.

• *A model-checking reformulation for verifying diagnosability of permanent and intermittent faults (in progress)* [8, 9, 10, 11]: this approach extends the Cimatti's work [12]. It allows the actual verification of various diagnosability concepts pertaining to permanent/intermittent based on the twin-plant structure. The main idea is to reformulate and express the diagnosability issues as temporal logics and then to tackle them using the model-checking engines (NuSMV model checker in our case).

The tool is a command-line software developed in *C#* programming language (available for Windows and Linux OSs). The tool takes as inputs: the system model as an "*.fsm" file, a parameter indicating the approach to be used, the set of faults to be diagnosed (permanent or intermittent faults). The tool outputs the diagnosability verdict and the (generated) intermediate model, i.e., the twin-plant or the diagnoser. It is worth noticing that in the case of diagnosable models, the diagnoser generated can be used to perform the online diagnosis.

References

[1] M. Sampath, R. Sengupta, and S. Lafortune. Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 40(9):1555–1575, 1995.

[2] C.G. Cassandras and S. Lafortune. Introduction to discrete event systems. *Springer*, 2008.

[3] J. Zaytoon and S. Lafortune. Overview of fault diagnosis methods for discrete event systems. *Annual Reviews in Control*, 37(2):308–320, 2013.

[4] A. Boussif. Contributions to fault diagnosis of discrete-event systems. *Ph.D. Thesis, Université de Lille 1 - IFSTTAR*, 2016.

[5] S. Jiang, Z. Huang, V. Chandra, and R. Kumar. A polynomial algorithm for testing diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 46(8):1318–1321, 2001.

[6] A. Boussif and M. Ghazel. Diagnosability analysis of input/output discrete event system using model checking. 5^{th} *IFAC International Workshop on Dependable Control of Discrete Systems*, 48(7):71 – 78, 2015.

[7] A. Boussif and M. Ghazel. A diagnoser-based approach for intermittent fault diagnosis of discrete-event systems. *the 2017 American Control Conference*, 2017.

[8] A. Boussif and M. Ghazel. Using model-checking techniques for diagnosability analysis of intermittent faults -a railway case-study. *Proceedings of the* 10^{th} *International Workshop on Verification and Evaluation of Computer and Communication Systems*, pages 93–104, 2016.

[9] A. Boussif and M. Ghazel. Intermittent fault diagnosis of industrial systems in a model-checking framework. *IEEE International Conference on Prognostics and Health Management*, pages 1–6, 2016.

[10] A. Boussif and M. Ghazel. Une approche par décomposition de modèles pour l'analyse de la diagnosticabilité des seds par model-checking. 10^{eme} *Colloque sur la Modélisation des Systèmes Réactifs*, 2015.

[11] A. Boussif, B. Liu, and M. Ghazel. A twin-plant based approach for diagnosability analysis of intermittent failures. In *13th International Workshop on Discrete Event Systems*, pages 237–244, 2016.

[12] A. Cimatti, C. Pecheur, and R. Cavada. Formal verification of diagnosability via symbolic model checking. *Int. Conference on Artificial Intelligence*, pages 363–369, 2003.