8th IFAC Symposium on Fault Detection,
Supervision and Safety of Technical Processes (SAFEPROCESS)
August 29-31, 2012. Mexico City, Mexico

Qualitative Event-based Diagnosis with Possible Conflicts Applied to Spacecraft Power Distribution Systems ⋆

Matthew Daigle * **Anibal Bregon** ** **Indranil Roychoudhury** ***

* *NASA Ames Research Center, Moffett Field, CA, 94035, USA (e-mail: matthew.j.daigle@nasa.gov).*
** *Department of Computer Science, University of Valladolid, Valladolid, 47011, Spain (e-mail: anibal@infor.uva.es)*
*** *SGT Inc., NASA Ames Research Center, Moffett Field, CA, 94035, USA (e-mail: indranil.roychoudhury@nasa.gov)*

Abstract: Model-based diagnosis enables efficient and safe operation of engineered systems. In this paper, we describe two algorithms based on a qualitative event-based fault isolation framework augmented with model-based fault identification that are applied to spacecraft power distribution systems. Although based on a common framework, the fundamental difference between the two algorithms is that one uses a global model for residual generation, fault isolation, and fault identification; whereas the other uses a set of minimal submodels computed using Possible Conflicts. We describe the implementation of the two algorithms and compare their diagnosis results on a representative spacecraft power distribution system.

Keywords: model-based diagnosis, spacecraft power systems, possible conflicts.

1. INTRODUCTION

Fault diagnosis methodologies are motivated by the need for increased performance, safety, and reliability of complex engineering systems. This paper presents a model-based, qualitative, event-based fault diagnosis scheme that performs the functions of fault detection, isolation, and identification. The diagnosis scheme has its foundations in the TRANSCEND diagnosis approach (Mosterman and Biswas, 1999), but can diagnose abrupt, incipient, and intermittent single faults. Our diagnosis scheme has two instantiations, QED (Qualitative Event-based Diagnosis), and QED-PC (QED with Possible Conflicts).

The general approach extends the TRANSCEND diagnosis scheme. In this scheme, fault isolation is achieved through analysis of the transients produced by faults, manifesting as deviations in observed behavior from predicted nominal behavior. QED extends TRANSCEND by including relative measurement orderings, which provide a partial ordering of measurement deviations for different faults, leading to an enhanced event-based fault isolation scheme (Daigle et al., 2009). Further, TRANSCEND deals only with abrupt faults, so we incorporate methods for incipient faults (Roychoudhury, 2009) and intermittent faults (Daigle and Roychoudhury, 2010).

QED-PC uses the Possible Conflicts (PCs) diagnosis approach (Pulido and Alonso-González, 2004) within the general QED framework. The PCs approach is a dependency-compilation technique from the DX community similar to the derivation of Analytical Redundancy Relations from the FDI community. The approach decomposes the global system model into minimal submodels containing sufficient analytical redundancy to generate fault hypotheses from observed measurement deviations. With QED-PC, residuals are computed using the PCs (instead of the global system model) and measurement deviations are analyzed following the TRANSCEND ideas as in QED. For fault identification, the algorithm uses minimal parameter estimators computed from PCs for each faulty parameter, as described in (Bregon et al., 2011b).

As a case study, we adopt a subset of the Advanced Diagnostic and Prognostic Testbed (ADAPT) (Poll et al., 2007), which is functionally representative of a spacecraft power distribution system. We apply our diagnosis algorithms to this system, evaluate the results, and compare and contrast algorithm performance.

The paper is organized as follows. Section 2 overviews the diagnosis approaches. Section 3 provides the system model. Sections 4, 5, and 6 describe fault detection, isolation, and identification, respectively. Section 7 presents the diagnosis results, and Section 8 concludes the paper.

2. DIAGNOSIS APPROACH

Our diagnosis approach performs the tasks of (*i*) fault detection, i.e., determining if a fault is present in the system, (*ii*) fault isolation, i.e., determining which fault has occurred, and (*iii*) fault identification, i.e., estimating the parameters that define the fault behavior.

The diagnosis architecture is shown in Fig. 1, and reflects the implementation of both algorithms. The system receives inputs $\mathbf{u}(t)$ and produces outputs $\mathbf{y}(t)$. The system

⋆ Anibal Bregon's work has been funded by the Spanish MCI DPI2008-01996 and TIN2009-11326 grants.

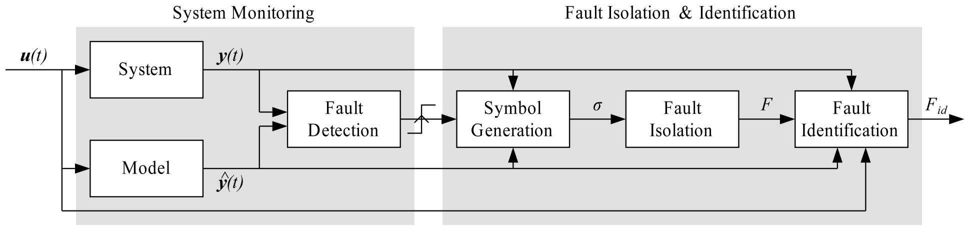

Fig. 1. Diagnosis architecture.

model, given inputs $\mathbf{u}(t)$, computes predicted values $\hat{\mathbf{y}}(t)$. The fault detection module decides whether a measurement has deviated from its nominal value in a statistically significant manner, triggering the fault isolation and identification modules. Measurement deviations, viewed as events, are abstracted into a symbolic representation using the symbol generator. The sequence of these symbols, where a symbol is denoted by σ, is used to isolate faults F. Fault isolation consists of candidate generation at the point of fault detection and hypothesis refinement as new symbols are provided. Each fault $f \in F$ is associated with a component, a fault mode, and a set of fault parameters. Fault identification computes, for each fault $f \in F$, the values of the fault parameters.

For both QED and QED-PC, we compute residuals as the difference between an observation, $\mathbf{y}(t)$, and the predicted nominal behavior of the output, $\hat{\mathbf{y}}(t)$, with the only difference coming from the way the predicted behavior is computed by each algorithm. For QED, the predicted values $\hat{\mathbf{y}}(t)$ are computed based on a global model of the system. For QED-PC, the system model is decomposed, using the Possible Conflicts approach (Pulido and Alonso-González, 2004), into minimal over-determined subsystems, each with a single output, that suffice for fault diagnosis. In this approach, the predicted values $\hat{\mathbf{y}}(t)$ are computed based on these subsystem models. The submodels are decoupled from each other by using measured values as inputs to the submodels.

3. SYSTEM MODELING

Our diagnosis approach is model-based, requiring a model of both nominal and faulty behavior for use throughout the diagnosis process. As described in the previous section, the two algorithms implement the nominal model in a different way. For QED, the nominal model is a global model of the system, $\mathcal{M}$, and its inputs are those of the global system. For QED-PC, the nominal model is composed of a set of 11 minimal submodels, with each submodel $\mathcal{M}_i$ estimating the value of sensor i using a subset of the system measurements as input variables. In the following, we describe the models of nominal and faulty behavior of the ADAPT system for QED and QED-PC, indicating their similarities and differences.

3.1 Nominal Model

A schematic of the selected subset of ADAPT is given in Fig. 2. Sensors prefixed with an "E" are voltage sensors, those with an "IT" are current sensors, and those with "ISH" or "ESH" are for sensing the states of circuit breakers and relays. TE228 is the battery temperature

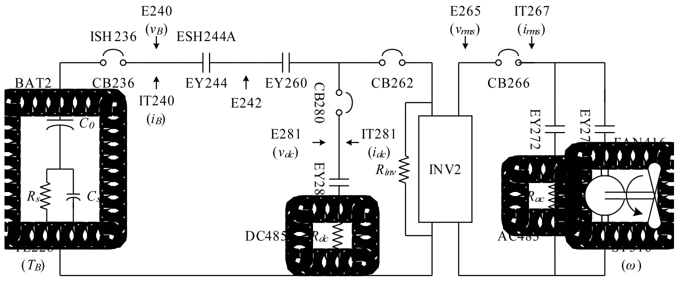

Fig. 2. ADAPT subset schematic.

sensor, and ST516 is the fan speed sensor. Note that the inverter (INV2) converts DC power to AC, and E265 and IT267 provide rms values of the AC waveforms.

Most of the equations of the global model and the corresponding PCs are summarized in Table 1. Details may be found in (Daigle and Roychoudhury, 2010). Here, v_B and i_B are the battery voltage and current, v_0 is the voltage across C_0, v_s is the voltage across C_s, e is the inverter efficiency, v_{inv} is the inverter voltage on the DC side, R_{inv} is the DC resistance of the inverter, R_{dc} is the DC load resistance, J_{fan} is the fan inertia, and B_{fan} is a damping parameter. Both QED and QED-PC assume TE228, ISH236, and ESH244A are constant. The PCs for E242 and E281 are simply other measured voltages with a bias term added.

Most of the PCs are derived directly from the global model, but in some cases, the PCs have to account for additional dynamics. For example, the fan speed (ω) has no dynamics during nominal operation because it is always operated at the same speed. So, QED models the fan speed as a constant. QED-PC, on the other hand, must model the dynamics, because some faults independent of the fan submodel will cause the fan speed to decrease through a decrease in E265, which is an input to the PC.

A key difference, then, compared to the global model, is that the behavior of each PC has to be nominal not only for the nominal situation, but also for those faulty situations where the fault parameters are independent of a PC. This decoupling requires a more detailed modeling of the system for the QED-PC algorithm. This introduced some modeling difficulties, especially concerning IT240. In nominal operation, the measured value averages around 16 ± 2 A. When faults occur, however, the value takes on a much wider range, and the IT240 PC must accurately predict values in the entire range due to faults that are decoupled from the PC. This made the system identification task more complex. System identification was also more complex for QED-PC because sensor biases had to be considered for the inputs to the PCs.