

How to diagnose a modern car with a formal B model?

Guilhem Pouzancre

ClearSy, Europarc de Pichaury, 1330 Av. J.R. G. Gautier de la Lauziere, 13856
Aix-en-Provence Cedex 3

1 Introduction

We introduce a modern method to diagnose vehicles. The method has been studied for Automobiles Peugeot. The classical methods to diagnose a car are based on technician's experience and failure knowledge (e.g., diagnostic trees). However cars become more and more complex and failures less and less predictable.

The modern cars are increasingly complex due to electronic components and services: lights and wipers turn on automatically, engine controller manages efficiently the torque and car radio manages the sound depending on the car speed.

Therefore, diagnostic of deficient components is complex, because of the car complexity and distributed functionalities: for example wheel sensors deficiency can induce effects on the car radio. On the other hand, deficiencies are mostly unpredictable, due to a wide variety of suppliers, car options and the short component life-cycle. Furthermore, garage mechanics have to diagnose bugs, which are, by definition, unpredictable.

However, all failures have a similar characteristic: a functional component does not respect its nominal specification. In our diagnosis method, event B models formalize the nominal functional specification and a B model interpreter (BI) checks which component does not match its specification.

To diagnose a car with this method we need:

- Correct and complete description of every vehicle component (vehicle B model)
- A rigorous link between the concrete car and the B models (dictionaries)
- A method to compare the components behaviour with their specification (record analysis)

2 Vehicle B model

We build the vehicle model with the event B method, because BI requires a non-ambiguous language and automatic proofs. Moreover, refinement and proof obligations guide model engineers in building correct models. The model only addresses the nominal behaviour of the components.

A car is described by 50 B models, 7000 events and 2000 abstract variables. Actually 98 percent of the proof obligations are discharged automatically, but

invariant and abstract models are weak, so the correctness of the model is not sufficient to make a fully automatic diagnostic. Anyway progress in this way.

We build independent models for each vehicle component, because the vehicle component is the smallest unit of repair. Thus BI will signal defects at the smallest granularity that is relevant for repairing.

3 Dictionaries

To find the deficient component, BI compares vehicle parameters with abstract B variables and abstract B events. This comparison is possible only if a link is specified with a rigorous precision.

So, first, we introduce the notion of *observable parameters* of vehicle components. These parameters correspond to physical measures or input values that are relevant to a description of the component behaviour. Their value can be either quantitative (e.g., car speed) or qualitative (e.g., "Normal", "Absent", "Important").

Their counterpart in the B model are some variable declarations. The dictionary gives an informal but rigorous definition for those B variables. That definition describes the link between the variable value and some observable parameter value. Moreover, those definitions must be such that from any set of observable parameter values, one can either deduce the values of the B variables or conclude that the vehicle is deficient.

In addition, the event dictionary is used to synchronise the observable parameters evolution with the B variable evolution. We define an event with observable parameters value. A B event definition sounds like: "B event Alert occurs when the oil temperature gets above 120°".

BI uses the variable and event definitions to compare the evolution of observable parameters with the B model, which specify the expected evolution.

4 Record analysis

It would take too much time to check all components in all contexts. Therefore, the technician reproduces the failure effect in a scenario. BI would then record all concrete event occurrence and observable parameter values continually during the scenario (vehicle recording). BI would use the technician observations for subjective and non-recorded parameters.

But, it would still take too much time and resources to record all observable parameter values, so we defined specific rules to deduce, from the B event guard and body, the significant variables, and thus a list of parameters to record. This point is very important because B models allow to differentiate simulation (which needs to affect a value for each parameter) and animation (which only asks the value of relevant parameters).

To diagnose the deficient components, BI checks the vehicle recording. BI searches abnormal observable parameter values, unexpected B variable modifications or unexpected component reactions.

BI finds abnormal observable parameters value when the variable definition specifies a deficient situation. It finds an unexpected B variable modification when a B variable value changes but no concrete event is recorded. An unexpected component reaction corresponds to the case where an event is recorded but its guard is false or its substitution does not match to the evolution of observable parameters.

5 Conclusion

Currently, two vehicles have been fully modeled and a third is being worked on. The BI theory has been completely studied and it is owned by PSA.

Intermediate tools and methods have been derived from that theory to assist Peugeot expert to define diagnosis tests. The B models (translated into french) are also used everyday by the experts of the second level hotline of PSA.

Some more investigation is particularly needed in the following directions:

- Reduce the development cost of B models.
- Increase the B models correctness.
- Implement BI as an integrated application.

In the end, the use of the B interpreter will allow garage employees to diagnose directly hidden causes of failure and bugs, thus reducing the burden on the second level experts.