

Verification of Diagnosability using Model Checking



Joint work with IRST (Trento, Italy)
Alessandro Cimatti, Roberto Cavada

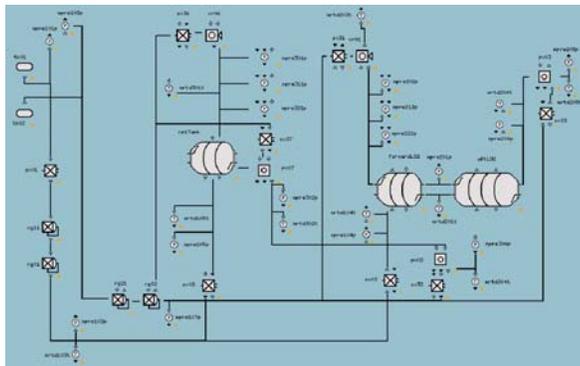
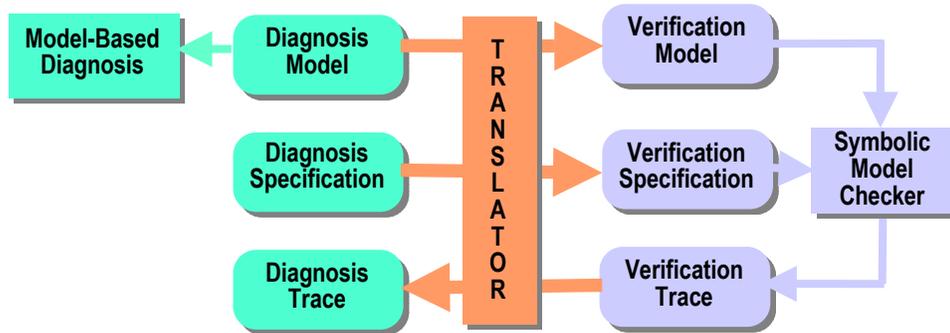
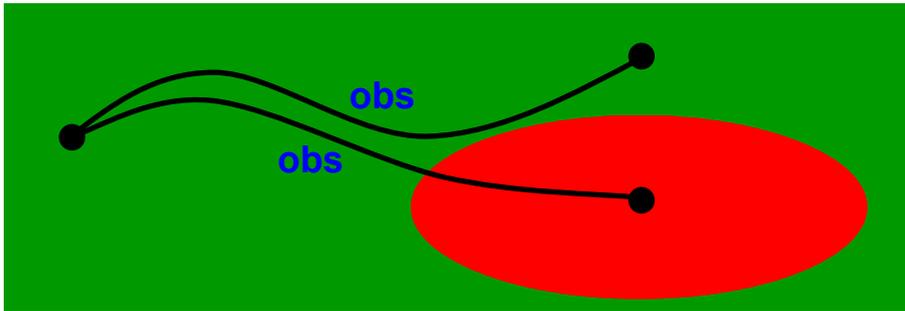
Goal: Verify that a physical system has sufficient observables that a diagnosis system can detect and identify all faults.

Approach:

- We analyze a model of the system, searching for distinct execution traces with identical **observations** leading to different fault diagnoses (e.g. **no fault** vs. **fault**).
- This search can be efficiently performed using **symbolic model checking** (e.g. SMV).

Output:

- Conclusive experiments were performed on a large Livingstone model (X-34 propulsion feed subsystem), using automated translation to the model checker. A diagnosability error in the model was found and fixed.
- Paper at IJCAI'03 (Acapulco, 9-15 Aug 03): Alessandro Cimatti, Charles Pecheur, Roberto Cavada, *Formal Verification of Diagnosability via Symbolic Model Checking*.



Explanation of Accomplishment



- **POC:** Charles Pecheur (RIACS) pecheur@email.arc.nasa.gov
- **Program funding this work:** ECS
- **Background:** A *diagnosis* system locates the faults in a physical system (such as a spacecraft) based on observations from sensors and actuators. An important characteristic of a physical system is its *diagnosability*; i.e., whether there are sufficient observables to pinpoint faults. Our work involves a novel approach to verifying that a system can be properly diagnosed. We use a model of the system and advanced symbolic model-checking techniques that allow the exhaustive analysis of all possible executions of that system, even for very large state spaces. In our case, we apply this analysis to models used by the Livingstone model-based diagnosis system, which was developed in Code IC.
- **Shown on slide:** The principle, illustrated in the top picture, is to search for execution traces (sequences of states of the model) with identical **observations** leading to different diagnoses (e.g. **no fault** vs. **fault**). If such a pair of traces is found, it means that the two different situations cannot be distinguished; i.e., the fault cannot be detected. We have applied this principle to models used with Livingstone using our automated translator from Livingstone to the SMV model checker (center picture). We have successfully demonstrated that technology on a real-size model (X-34 propulsion feed subsystem, 800+ variables, bottom picture). The model checker analyzed the X-34 model in less than 2 seconds and found a minor diagnosability error. The error was acknowledged as an inaccuracy in the model and fixed by the developers of the X-34 model.
- **Accomplishment/Relation to Milestone and ETO:** The approach, implementation and experiments were summarized in a paper that was presented at the International Joint Conference on Artificial Intelligence (IJCAI) in August, 2003. This paper follows a workshop paper in July 02 and a technical report (RIACS TR 03.03) on the experiments. This work contributes to the milestones of our ongoing project "Verification for Model-Based Hazard Analysis", funded under the ECS Program.
- **Future Plans:** In the short term, we are adding specific support to our translator to generate the twin models and process and display the pairs of traces resulting from the verification. In the longer term, we will perform more extensive experiments on real applications, to tune up our approach to the concrete needs of diagnosis application designers.