



Richard Dearden, Juhan Ernits and Jeremy Wyatt
 School of Computer Science, University of Birmingham, Edgbaston, Birmingham, UK
 Email: {rwd,ernitsj,jlw}@cs.bham.ac.uk

In collaboration with the Autosub 6000 Team at
 National Oceanography Centre, University of Southampton, Southampton, UK

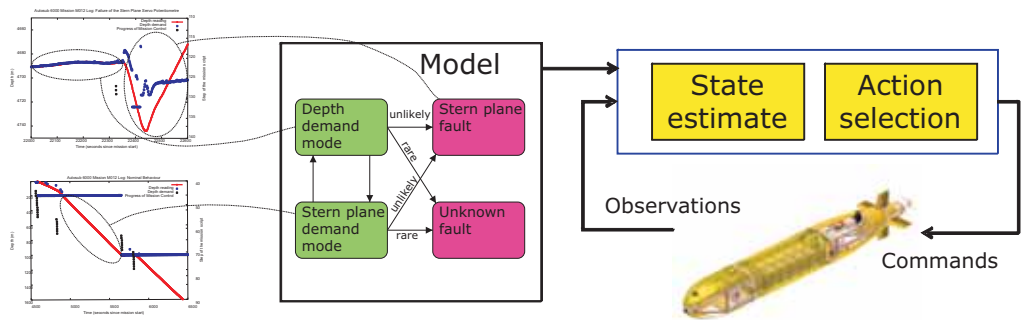
Project Objectives

- To model a critical Autosub 6000 system suitable for constraint based diagnosis techniques.
- To use the model with the Livingstone 2 automated diagnosis system to diagnose faults in the system.
- To integrate a Livingstone 2 based diagnosis system into Autosub 6000.
- To demonstrate the correctness of the diagnoses made on the bench and in the field.
- To design and integrate robust mitigations for fault recovery. These will take account of the likelihood and cost of recovery strategies for false alarms or possible misdiagnoses.
- To gather statistical evidence of the potential improvement in vehicle performance in the field. This and the bench testing will support the Autosub 6000 risk management process.

Modelling Autosub 6000 in Livingstone 2

Livingstone 2 (L2) is designed to assist complex systems to operate robustly in the face of hardware failures or unexpected events. L2 diagnoses the current state of the system and can recommend commands or repair actions. L2 is a model-based diagnosis and recovery engine based on a constraint solver.

L2 is a mission-ready technology developed at NASA that has been successfully flown on the Deep Space 1 and EO/1 Spacecraft. We use and further develop the tools to provide a lasting legacy for the Autosub.



Key features of L2:

- Ability to diagnose multiple faults
- Ability to provide justification for diagnosis
- Ability to detect unforeseen faults

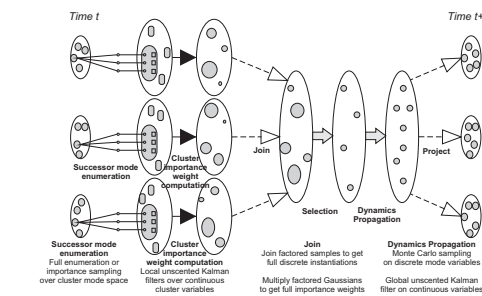
through the use of unknown modes

- Ability to synthesize mitigation actions (commands) to recover from diagnosed faults measured through sensors.

Tracking Hybrid State

Autosub also features a number of continuous variables that are important for the purpose of diagnosis.

We model the continuous dynamics using particle filtering to track the state. Particle filtering algorithms maintain a state estimate as a set of samples, each of which represents a possible state the system might be in. The algorithms are Monte Carlo, with each sample



predicting a possible future state of the system to be compared with observations.

Fault states have a low probability of occurring, so it is possible that when a fault occurs in the system, there is no matching sample. We solve this using a technique called *look-ahead* where each sample predicts a future possible system state, rather than simply applying the system dynamics model to the sample. Each sample is thus conditioned on the new observation of the conditional future states.

Recent Publications

- Minlue Wang and Richard Dearden. Detecting and learning unknown fault states in hybrid diagnosis. 20th International Workshop on Principles of Diagnosis, DX-09, Stockholm, Sweden, June 2009.
- Juhan Ernits, Richard Dearden and Miles Pebody. Formal methods for automated diagnosis of Autosub 6000. NASA Formal Methods Symposium, Mountain View, CA, USA, April 2009.