Proceedings of the Peradeniya University Research Sessions, Sri Lanka, Vol.11, November 30, 2006

TOWARDS DISTRIBUTED DIAGNOSIS OF REACTIVE SYSTEMS USING STATECHART BASED CONTROLLER DESIGN

S. DEVAPRIYA DEWASURENDRA

Department of Production Engineering, Faculty of Engineering, University of Peradeniya

A **fault** is an unexpected change in a system's function and a **failure** is a complete breakdown of a system component or function. **Fault diagnosis** is a process of detecting and isolating faults (fault types): based on event sequences (symptoms). In safety critical applications each possible fault that can result in a symptom is reported as a fault candidate: model based diagnosis is preferred here. In Finite State Machine models of the system to be diagnosed the event set is partitioned as $\Sigma = \Sigma_0 \cup \Sigma_{uo}$: the observable and unobservable event sets. $\Sigma_f \subseteq \Sigma_{uo}$ denotes the set of fault(y) events. Types of faults *fi, (i=1,p)* can be identified with associated disjoint alphabets Σ_{fi}, forming a partition, Π_f on Σ_f. A language L is **diagnosable** with respect to Π_f, if $(\forall i \in \Pi_f)(\exists n_i \in N)(\forall s \in \Psi(\Sigma_{fi}))\ (\forall t \in L/s)(\|t\| \geq n_i \Rightarrow (\forall w \in P_L^{-1}(P(st)))(\Sigma_{fi} \in w))$; $\Psi(\Sigma_{fi}) = \{s\sigma_f \in L \mid \sigma_f \in \Sigma_{fi}\}; P: \Sigma^* \to \Sigma_o^*; P_L^{-1}(y) = \{s \in L \mid P(s) = y\}$. This applies only to centralised diagnosis.

However, centralised diagnosis can become impracticable for real-sized systems. Hence, a distributed reference model can be defined as a set of closed languages $\{L_i \subseteq \Sigma_i^* \mid i \in I\}$ where L_i and Σ_i are local components and local event alphabets, respectively. The observable, unobservable and fault event sets for the local component i are, $\Sigma_{io}, \Sigma_{iuo}, \Sigma_{if} \subseteq \Sigma_i$, respectively: $i \neq j \not\Rightarrow \Sigma_{io} \cap \Sigma_{jo} = \Phi; i \neq j \Rightarrow \Sigma_{if} \cap \Sigma_{jf} = \Phi$. The distributed diagnosis problem is then posed as, Local computation: $(\forall i \in I) M_i := P_{io}^{-1}(u_i) \cap L_i$: given observation $u_i (i \in I)$ find all strings that can exhibit u_i; and Global consistency: $E := Sup\Delta(\{M_i \mid i \in I\})$: given the local estimates, use the notion of supremal global support to capture "agreement" among them. Checking for global consistency can be very time consuming. A set of local languages $L = \{L_i \subseteq \Sigma_i^* \mid i \in I\}$ is globally consistent if $\forall i \in I, L_i = P_{I,i}(\|_{j \in I} L_j)$. Here, $P_{J,i} : \Sigma_J^* \to (\Sigma_J \cap \Sigma_i)^*$ and $\|$ represents the synchronous product of languages. L is locally consistent if $\forall i, j \in I, P_{i,j}(L_i) = P_{j,i}(L_j)$. Global consistency (GC) implies local consistency(LC), but not vice-versa. Our distributed diagnosis strategy uses conditions that make this latter equality possible: let graph Gr (Ver, Edg) be constructed with local event sets as vertices *(Ver = I)* and edges connecting event sets with non-disjoint alphabets. Then, Gr is a tree $\Rightarrow$ {LC $\Rightarrow$ GC}. We were also inspired by a statechart based approach using structures called D-Holons to represent superstates with associated diagnosers built as Reachability Transition Systems (RTS) of observation-adjacent states. However, their approach is very restrictive in that they only consider **failures** and also single-failure scenarios. We manage to overcome the restrictions by adopting Drusinski-Harel decomposition on statechart models of the system to be controlled using an approach we have developed for modular verification of Logic/supervisory control: this decomposition satisfies the "Tree" condition required for the graph Gr, to make LC $\Rightarrow$ GC.