Robust Supervisory Synthesis for Automated Manufacturing Systems

An automated manufacturing system (AMS) is composed of limited resources and can process different kinds of parts based on resource sharing and a specified sequence of operations. On the one hand, resource sharing may lead to deadlocks in which the global or local system is crippled. On the other hand, an AMS often suffers from unreliable resource failures that may also cause processes to halt. Thus, it is a necessary requirement to develop an effective and robust deadlock control policy to ensure that deadlocks cannot occur even if some resources in a system break down. As a graphical and mathematical tool, Petri nets provide a uniform paradigm for modeling and formal analysis of AMS. They are well suitable to describe AMS' behavior and characteristics such as concurrency, conflict, and causal dependency. They can be used to reveal behavioral properties such as liveness and boundedness. Over the past three decades, a variety of deadlock control policies based on Petri nets have been proposed for AMS. However, there is a lack of research in Petri nets regarding the impacts of unreliable resources on AMS under the supervisory control of deadlocks. In fact, resource failures are a common problem in real-world systems, which pose challenges in supervisory control of discrete event systems including AMS. In case of resource failures, the existing deadlock control policies are always no longer in force and deadlocks in the disturbed system may be caused. Therefore, reanalysis of the disturbed system is usually necessary. Robustness analysis provides an alternative way to determine whether the operation of a disturbed system or a part of it can still be maintained in case of resource failures. In this thesis, we try to enforce liveness and robustness via a supervisor by adding monitors and recovery subnets. This implies that both a plant and its supervisor are unified in a Petri net formalism. An interesting issue is how to make the existing deadlock control policies possess a desirable robust property to cope with resource failures. Specifically, the desirable robustness is a system property to keep a controlled system live as some resources break down. For an uncontrolled system of simple sequential processes with resources, monitors and recovery subnets are designed for strict minimal siphons that may be emptied and unreliable resources, respectively. Monitors, complementary places of monitors, and recovery subnets are connected by normal arcs in case of necessity. By adding monitors for siphons, deadlocks in original Petri nets can be controlled and by adding recovery subnets, complementary places of monitors, and necessary arcs for unreliable parts, deadlocks in the disturbed systems can be controlled. We also find that complementary places of monitors and related arcs can be replaced by inhibitor arcs. In order to analyze the robustness of a supervisor, we propose a new pause state called a waiting-for-repair state, which is different from a deadlock state. The supervisor designed for a Petri net by the proposed method has the following characteristics: (1) it can prevent deadlocks for a plant model when all resources work normally; (2) deadlocks are prevented even if some resources fail to work and are removed to repair at any time; and (3) waiting-for-repair states disappear after the repaired resources are returned. Then reanalysis of the original Petri net is avoided and a robust liveness-enforcing supervisor is derived.