1. Record Nr. UNINA9910795570403321

Autore	Missal Dirk
Titolo	Formal synthesis of safety controller code for distributed controllers / / by Dirk Missal
Pubbl/distr/stampa	Berlin : , : Logos Verlag, , [2012] ©2012
ISBN	3-8325-9974-6
Descrizione fisica	1 online resource (156 pages)
Collana	Hallenser Schriften zur Automatisierungstechnik
Disciplina	670.4275
Soggetti	Automatic control - Standards
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	PublicationDate: 20120510
Sommario/riassunto	Long description: Modern control systems in manufacturing are characterized by rising complexity in size and functionality. They are highly decentralized and constitute a network of physically and functionally distributed controllers collaborating to perform the control tasks. That goes along with a further growing demand on safety and reliability. A distributed control architecture supporting functional decomposition of large systems as well as accommodating flexibility of modular systems is defined. This work describes the formal synthesis of distributed control functions for the sub area of safety requirements. The formal synthesis is applied to avoid the potentially faulty influence of human work through the whole process from the formal specification to the executable control function. Starting points are a formal model of the uncontrolled plant behavior and a formal specification of forbidden behavior. The formulation of the specification and the modeling is exemplified on a manufacturing system in lab-scale. The introduced synthesis methods produce controller models describing the correct control actions to achieve the given specification. The methods use symbolic backward search from a forbidden state to determine the last admissible state before entering an uncontrollable trajectory to a forbidden state. Hence, the determination of the reachable state space is avoided to reduce the

computational complexity. The use of partial markings leads to a further reduction. The complexity is an important obstacle for the use of formal methods on real-scale applications. The monolithic synthesis approach is proven to result in maximally permissive results. The modular approach is not maximally permissive but the more efficient way to distributed control functions. The implementation of the generated controller model as executable Function Blocks according to IEC61499 is addressed in the last part of this work. The distributed control predicates are embedded as structured text instruction into different interacting Function Block types according to the distributed control structure. This last step finalizes the sequence from a formal model and the specification to fully automatically-generated executable control code. Moderne Steuerungssysteme sind durch zunehmende Komplexität und Funktionalität gekennzeichnet. Sie sind stark dezentralisiert und formen ein Netzwerk von physisch und funktional verteilten Steuerungen, die eine gemeinsame Steuerungsaufgabe erfüllen. Diese geht einher mit einem weiter steigenden Anspruch an Sicherheit und Zuverlässigkeit. Es wird eine verteilte Steuerungsarchitektur definiert, welche die funktionale Zerlegung großer Systeme und die Flexibilität modularer Systeme unterstützt. Diese Arbeit beschreibt die formale Synthese verteilter Steuerungsfunktionen für das Teilgebiet der Sicherheitsanforderungen. Die Anwendung der formalen Synthese vermeidet den potenziell fehlerverursachenden Einfluss menschlicher Arbeit durch den gesamten Prozess von der formalen Spezifikation bis zu Erzeugung ausführbarer Steuerungsfunktionen in Form von Basic Function Blocks nach IEC61499. Die beschriebenen Methoden nutzen die symbolische Rückwärtssuche und die Abstraktion von Systemzuständen zu partiellen Markierungen um die Berechnungskomplexität zu verringern. Eine der Methoden liefert minimal einschränkenden Steuerungsfunktionen. Die einzelnen Schritte der Synthese sind an einem Produktionssystem in Labormaßstab beispielhaft erläutert.