Publication Series of the Institute of Automation
University of Bremen

Series 3-Nr.6

Leila Fotoohi

Dependable Service Robot – from Hazard Identification to Formal Verification of Safety Requirements

D 46 (Diss. Universität Bremen)

Shaker Verlag
Aachen 2012

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Bremen, Univ., Diss., 2012

Publication Series of the INSTITUTE OF AUTOMATION, UNIVERSITY OF BREMEN:

1 Colloquium of Automation
2 Automation
3 Robotics
4 Control Theory
5 Image Processing
6 Virtual and Augmented Reality
7 Brain Computer Interface

Printed in Germany.

ISBN 978-3-8440-1435-8
ISSN 1861-5457

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • e-mail: info@shaker.de

Zusammenfassung

Der Service-Roboter arbeitet in unmittelbarer Nähe des menschlichen Körpers. Um seine Aufgaben zu erfüllen, hat er außerdem eine enge Interaktion mit dem Endbenutzer. Daher ist die Zuverlässigkeit des Service-Roboters entscheidend für seine gesellschaftliche Akzeptanz. Neueste Forschungen in der Sicherheit und Zuverlässigkeit der Service-Robotik beschäftigen sich mit der physischen Sicherheit und der Entwicklung leichter Roboter. Die Reduzierung der Risiken in der Service-Robotik können nicht nur durch die Berücksichtigung physischer oder dynamischer Sicherheit erreicht werden. Um ein akzeptables Maß an Zuverlässigkeit in der Service-Robotik zu erreichen, muss die Integration von Komponenten zu einem vollständig sicheren Betriebssystem mehr im Fokus stehen.

In dieser Arbeit werden Methoden zur sicheren Entwicklung von Service-Roboter vorgeschlagen. Diese Methoden sind in der Avionik und bei Kernkraftwerken gut bekannt und können auf die sicherheitskritischen Service-Roboter übertragen werden. Sie zeigen aller möglichen Gefahren an Systemen und deren Einzelkomponenten auf. In diesem Zusammenhang werden buttom-up und top-down Verfahren zur Gefahrenerkennung genutzt um die Sicherheitsanforderungen für das FRIEND-System zu bestimmen. FRIEND ist ein Assistenzroboter, der am Institut für Automatisierungstechnik (IAT) an der Universität Bremen entwickelt wird. Die Sicherheitsanforderungen ergeben ein unabhängiges Sicherheitsüberwachungssystem, das parallel zur eigentlichen Kontrolleinheit des Robotersystems läuft. Das Sicherheitsüberwachungssystem erfüllt die Sicherheitsanforderungen und erlaubt eine ausfallsichere Steuerung des Roboters. Um die funktionale Richtigkeit des Sicherheitsüberwachungssystem zu gewährleisten, wird ein formales, modellbasiertes Verfahren verwendet, das auf ereignisdiskretes Steuerungssystem angewendet wird. Im Rahmen dieser Arbeit wird eine neue Anwendung des Ramadge Wonham (RW) Rahmenwerkes präsentiert, wobei der Schwerpunkt auf der sicheren Steuerung eines Assistenzroboters liegt.