Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnLine 50-1 (2017) 1983–1990

Certifiable Software Architecture for Human Robot Collaboration in Industrial Production Environments ⋆

Stefan Brending * **Michael Lawo** * **Jürgen Pannek** ** **Tobias Sprodowski** ** **Patrick Zeising** *** **Daniela Zimmermann** ***

* *Center for Computing and Communication Technologies (TZI), University of Bremen, 28359 Bremen, Germany (e-mail:* [brending|mlawo]*@tzi.de).*
** *LogDynamics - Bremen Research Cluster for Dynamics in Logistics, Faculty of Production Engineering, University of Bremen, 28359 Bremen, Germany (e-mail:* [pan|spr]*@biba.uni-bremen.de)*
*** *neusta mobile solutions GmbH, 28217 Bremen, Germany (e-mail:* [p.zeising|d.zimmermann]*@neusta.de)*

Abstract: Existing concepts for Human-Machine-Collaboration in industrial production require either the temporal or spacial separation of work places or are only applicable for small loads. By introducing a concept for the combination of work places of humans and machines we show how the temporal and spatial overlapping form of collaboration can be realized. The concept was implemented in a prototype setting by means of an intelligent software environment dynamically evaluating all available sensor data of commonly employed safety components. The required precision for certifying the safety of the core software system is shown empirically.

Keywords: Cyber-Physical Systems, Human-Robot-Collaboration, Intelligent controllers, Sensor signal consolidation, Manufacturing

1. INTRODUCTION

For decades position-controlled industrial robots have been used in industrial mass production. These ensure an increasing degree of automation and productivity in manufacturing processes at reasonable costs. Moreover, robots replace manual labor by accurate and reliable task performance even for heavy payloads. Hence, industrial robots facilitate work processes unfavorable for humans from both an ergonomic and economic perspective, but are not flexible enough to replace humans completely.

In practice, a number of safety and security norms such as ISO 10218 (ISO, 2011a,b) as well as ISO/IEC 15026 and ISO 27005 (ISO, 2015, 2011c) together with technical specifications defined in ISO TS 15066 (ISO, 2016), IEC 61508 for functional safety (IEC, 2013) and IEC 15408 for establishing security techniques in IT-based systems (ISO, 2009) need to be addressed by the manufacturers of production lines with human-robot-collaboration (HRC). The purpose of these guidelines is to avoid risks for humans. To guarantee safe operation, each manufacturer adds (more) specific individual guidelines for occupational safety including a risk assessment. Upon delivery, the manufacturer declares that the product meets the requirements of the applicable EC directives by assigning the CE marking.

Currently, the working spaces of humans and robots are separated in space and time to ensure the required occupational safety. Passive safety devices like safety fences, dead man handles, or two-hand control ensure this strict separation. A temporal and spatial merge of the working spaces of humans and robots is favorable as it may allow to eliminate interruptions and non-productive time. Additionally, more efficient and ergonomic tasks may improve the performance of HRC, which may lead to reduced floor space. In this context, however, passive safety equipment is unsuitable as it typically requires an emergency stop of the robot. This automatically leads to an interruption of the production process and causes a restart.

For smooth operation without interruptions, an active sensor based control system surveilling HRC is needed. This system must be able to control the robot, observe the human in the merged working environment. As one cannot control humans without restrictions, activities of robots and humans are monitored to control the robots and inform the humans on the specific situation.

As the system has to avoid any collision between the position-controlled industrial robot and humans, modifications on concepts for controlling production processes with HRC are necessary. These need to be complemented by new, active, context-based and networked safety systems requiring a step beyond extensions of the usual passive safety systems as well as the approach of single purpose safety devices.

⋆ This research is part of the joint project InSA (www.insa-projekt.de) funded by the Federal Ministry of Economy and Energy in the context of the initiative Autonomik Industry 4.0.

2405-8963
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2017.08.171

In this work and as part of the joint project InSA (www.insa-projekt.de), we consider an information technology (IT) driven approach for a collaborative HRC workplace. We show that utilizing cyber-physical systems as key enabler technology, a real-time adaptation of working processes is achievable. Existing technology becomes part of an intelligent working environment operated by a new form of networked control allowing to adjust the working process and protection zone context-based in real-time. Next to the new form of networked control, rules of operation and tests in real industrial environments are required. This allows to derive not only a working prototype but also an economically concise approach accepted by the employers mutual insurance association or technical inspection agency and the market. To this end, we consider relevant mentioned standards for such systems and the involved software development processes.

In Section 2 we present the state of the art for HRC, which directly leads us to the approached open issue formulated in Section 3. In the ensuing Sections 4 and 5, we describe the hardware and software setup considered in this case study. In Section 6 we discuss our experimental results before providing an outlook to conclude the paper.

2. STATE-OF-THE-ART

Today, the utilization of robots in mass production is widespreaded and still increasing (World Robotics, 2016). In contrast to the setting of the last decades, where most robotic systems in an assembly line were isolated and controlled each by a single PLC (Programmable Logic Controller), we now face connected and distributed systems. These approaches are known by the IT driven *Internet of Things* (Ashton, 2009) and the technology driven *Industrie 4.0* (Federal Ministry for Economic Affairs and Energy, 2016) initiatives. Additionally, with the availability of computing power of controllers, accurate sensors and actuators allow a more granular interaction between robots and humans.

Considering safety issues, assembly lines are still isolated by passive safety systems, e.g., a protection fence as a fixed safe bounding box from humans, and are shutting down if a worker enters this safety zone. These fixed zones are on the one hand inflexible as the infrastructure of an assembly line cannot be easily changed. On the other hand, the demand of floor space is high. To decrease costs by shrinking the necessary floor space and increasing productivity, collaboration between human and robots becomes a necessity. As flexibility and changeability of products is needed in many assembly lines, a full automation is not always feasible due to costs or technical restrictions. To overcome this problem and to incorporate needed human flexibility to avoid cost-intensive solutions, new approaches induce the human factor as a fixed component to reach the desired degree of flexibility. This can be rotation principles for workers to operate several workstations with support of interactive information equipment (Michalos et al., 2010) or fine granular classification to describe the human factor as controller, data source or commander for the overall system described in Fantini et al. (2016) as *Human-in-the-loop*. Furthermore, as maintenance is done mostly in a shut down system, a possible coexistence of working robots and humans in the same work space depends on the possibility of recognizing and flexibly reacting to a dynamic environment. This leads to the necessity of open interfaces to access measured sensor data and the possibility to apply control methods not only by the embedded controller but also from external systems. To this end, these described necessary properties are covered by the definitions of a cyber-physical system (Lee, 2006).

The idea of collaboration between human and robots was introduced firstly as *cobots* (Akella et al., 1999) as Intelligent Assist Devices (IAD) to reduce the physical load or to support the operators by utilizing power assistance or force amplification. The authors distinguish between manual (executed by human), automated (executed by robots) and hybrid systems (collaborated tasks) and give examples for hybrid systems especially in the automotive industry. Shi et al. (2012) refine the interaction of human-robot collaboration (HRC) in three levels: The low level can be described as the conservative level. Each robot device has to be fixed if the operator enters the safety region for loading or maintenance operations and continue after the operator has left the safety region and confirmed that. In the medium level the robot operating mode is active while the drives are de-energized and extended to their widest range while the operator can perform his tasks. The high level describes the interaction with a working robot via modified speed or trajectories. This allows incorporation of dynamic environments with an interacting operator utilizing a dynamic and varying safety bounding box.

To refine the high level of HRC, Krüger et al. (2009) focus on hybrid assembly lines and distinguish the kind of HRC in workplace and time sharing systems. Workplace sharing is defined as spatial overlap of operator and robot, which execute different tasks at disjunct time steps. The interaction level is therefore mostly concerned about collision avoidance. In time sharing systems, both are jointly performing a task and therefore a higher interaction level is required, e.g. the incorporation of force-torque sensors that recognize the movement by an external force (operator). This was demonstrated by the PowerMate project developed by Fraunhofer IPA (Schraft et al., 2005). As most of these approaches consider HRC with a minimum safety distance, Bicchi et al. (2008) strike out the challenges of physical HRC, which includes physical contact between robot and operator.

Achieving a high level of human-robot-collaboration induces high costs due to the development of a new robot generation. To solve this issue for small or medium sized enterprises (SME), Nilsson and Johansson (2005) investigated the development of a flexible robot system in the SMErobot^{TM} project. They implemented Plug-and-Play tooling, pre-installed human recognition and a lightweight programming interface based on position and gesture recognition. Dietz et al. (2013) developed a cost model to incorporate not only the original costs of a robot, but additionally installation, programming and maintenance costs to estimate a worst- and best-case scenario.

In parallel to these schemes new safety and security definitions are required. Burns et al. (1992) presented the computer science perspective as *safety critical problem*, which describe the failure of a system occurring direct