The 2009 IEEE/RSJ International Conference on
Intelligent Robots and Systems
October 11-15, 2009 St. Louis, USA

Development of a Safety Module for Robots Sharing Workspace with Humans

Yoshihiro Nakabo*, Hajime Saito**, Takuya Ogure*, Seong Hee Jeong* and Yoji Yamada*

***Abstract*— Although the need for humans and robots to work together in close proximity is increasing, this is currently not allowed with conventional industrial robots for reasons of safety. Next generation robots that can work safely in close proximity with humans must not only be highly functional, but must also be highly reliable with built in safety features. With this aim in mind, we have developed a safety module that integrates safety functions required for robots to work side by side with humans. The safety module is designed to be compliant with international safety standards and Japanese law. Redundant sensory signal processing by an external hardware module and plug-in software installed in the robot controller ensure high-reliability and flexibility. This paper describes the concept and design of the safety module and shows some evaluation results of its safety functions.**

I. INTRODUCTION

Conventional industrial robots are not allowed to work in close proximity with human workers for safety reasons. For example, Japanese law on industrial safety and health [1] states that a robot that has a motor power of more than 80 W has to be separated from human workers by a fence that surrounds the maximum movement area of the robot. In other words, the working areas of humans and robots have to be segregated. This, in turn, creates wasted stock between the processing units, and also takes up a large area of the workspace. Using one human worker to assemble a product on their own from start to finish, cell production systems solve the problem of space and overhead stock. However, it is known that the production can be improved by offloading the tedious repetitive tasks to robots.

If robots could coexist with human workers, the robots could carry out monotonous and repetitive tasks with accuracy and at high-speed. Human workers could use their skills to do more complex tasks, such as assembly and preparation, post-processing tasks for the robots. This compensation of each others disadvantages holds promise for cooperation between human workers and robots.

To realize this cooperation, we must achieve a high level of safety for the human workers from any risk posed by robots in the workspace. Principles stated by recent international standards and a new guideline issued by the Japanese government[2], require proper safety techniques including risk assessment, a risk-reduction process, and regulated motor power be applied to next generation robots that coexist with human workers. Moreover, specific measures and procedures for human-robot cooperation in a shared space are determined by newly revised international safety standards for industrial robots ISO 10218:2006 [3]. These show an increasing momentum toward human-robot cooperative work.

For human-robot cooperation a new safety technology, consistent with safety standards and laws based upon state of the art technology, is required. In this study, we discuss the safety functions required for this type of next generation robot, and propose a safety modules which uses a new architecture comprised of hardware and software, in which these safety functions are integrated. To evaluate the functionality of the module, we have developed an experimental system and implemented an actual human cooperative robot.

The reminder of the paper is composed as follows. The requirements from the viewpoint of safety issues based on an actual example of a human robot cooperation based cell production, and related safety standards are discussed in Section II. Section III describes the actual specifications of the safety module and goes over details of the proposed architecture and its implementation. In Section IV, the result of the evaluation of the safety module and the production robot is shown.

II. HUMAN ROBOT COOPERATION AND SAFETY STANDARDS

A. Realization of cell production robot sharing workspace with human

In recent years, there have been many demonstrations of human-robot cooperating cell production systems. Yaskawa Electric Co. exposed that a human and robot co-existence will be introduced in a cell production system for its servo motor production process in the spring of 2009. Panasonic Electric Works Co., Ltd. showed in 2008 an evaluation toward a hybrid production system that had started by setting up cell production and line production, in which human workers and robots are combined.

In the New Energy and Industrial Technology Development Organization (NEDO) project for strategic development of advanced robotics elemental technologies (from FY2006 to FY2010) two groups - one consisting of Fanuc Ltd. and the University of Tokyo and the other AIST, Kawada Industries, Inc. and THK Co., Ltd. - competed developing a new robot for human-robot co-existing cell production systems. Fanuc and the University of Tokyo developed an assembly-support system for a cable-insert task using two robot manipulators aimed to improve assembly performance of a human operator

*Y. Nakabo, T. Ogure, S. Jeong and Y. Yamada is with Safety Intelligence Research Group, Intelligent Systems Research Institute, National Institute of Advanced Industrial Science and Technology (AIST), 1-1-1 Umezono Tsukuba, Japan nakabo-yoshihiro@aist.go.jp

**H. Saito is with General Robotix, Inc., #A30, 2-1-6, Sengen, Tsukuba, Japan h.saito@generalrobotix.com

Fig. 1. SP-02 robot with humanoid upper-body for cell production line

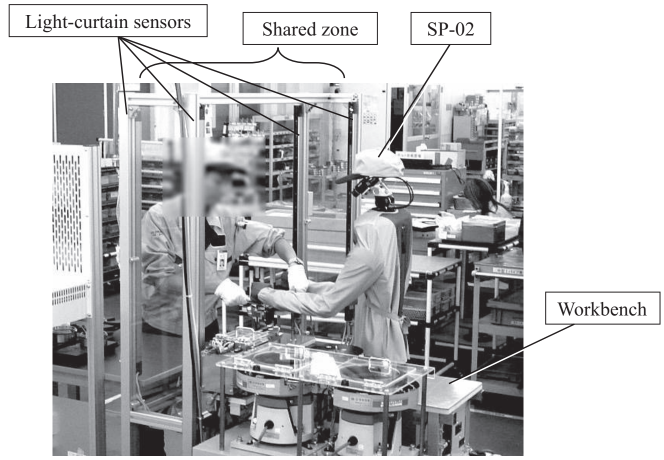

Fig. 2. Component exchange between human worker and SP-02

[4]. AIST, Kawada Industries and THK manufactured a cell production robot with a humanoid upper body called SP-02, as shown in Fig. 1.

B. Intrinsic safety of human space sharing cell production robot

The SP-02 robot enabled human and robot co-existence by reducing its motor power to meet regulations under stated by Japanese law. In addition, the robot complies with the international standard of ISO 12100:2003 [5], which is the most basic standard covering machine safety, by applying risk assessment, elimination of potential origins of hazards, and risk reduction to ensure the safety of the robot.

For example, the SP-02 has almost no sharp edges and has been designed to eliminate the possibility of a shearing accident. It also is designed to use a minimal movement area and motor power for carrying out its tasks. However, the sharp "fingertips" of the robot's hands are necessary for the cell production tasks it was given, and cannot be covered (Fig. 1). Because of this, a risk to human eyes, for example, remains, and intrinsic safety is not completely realized. The next step in risk reduction is to implement a control safeguard, by achieving "functional safety."

C. Functional safety of human space sharing robot

In a revised version published in 2006, the international safety standard for industrial robots, ISO 10218 [3], which is a lower level of ISO 12100, explains detailed requirements and several preconditions for a particular machine or robot, be allowed human interaction. The standard shows that the collision risk to the human worker can be avoided by detecting the human's position and restricting the movement area of the robot through control.

In the cell production procedure using the SP-02, as shown in Fig. 2, light-curtain sensors detect the presence of a human to prevent a collision with the robot when a component is exchanged between human and robot in the shared zone. In addition to the light curtains, there is a control panel and other switches used by human operators to control the robot so as to prevent any risk. The control of the robot is explained in detail later in this paper.

Some of the other conditions for human-robot cooperation shown in ISO 10218 are, restrictions on speed or output force of the end effector of the robot. Olesya [6] illustrate several implementations of such safety functions. These examples show that beyond conventional industrial robots, which are isolated from humans by a fence and whose only safety function is an emergency shutdown, cooperative robots require more complex functions such as the ability to recognize its situation or work phase through cues from control signals or safety sensors, and to switch safety functions depending on their situation.

D. Realizing safety functions with high reliability

When such complex safety functions are incorporated in a safety system, in addition to the functionality of the safety functions, realization of the safety functions with high reliability is essential to ensure the safety of the workers around the robot. In this regard, a Category 3 or higher safety level is required in ISO 10218. This in turn requires redundant signal transfer and processing, under system safety standard ISO 13849:1999 [7].

There exist some commercial products that satisfy these conditions. An example in which the movable area of the robot is restricted in adherence to safety standards is "Safe robot technology" from KUKA Roboter GmbH [8]. This realizes a robot area restriction system called "Safe operation," and has a system with built-in Category 3 safety certification. However, the Category 3 safety certification comes at a cost and this built-in safety is wasted if the robot is re-deployed to an area which does not require human interactive operation.

Elan Schaltelemente GmbH & Co. KG. has developed a human-robot cooperation technique called "ESALAN Safety Controller" [9]. In this system, an optional external module executes the safety functions such as restrictions on the movable area of a robot. However in this case, to achieve Category 3 safety levels, the module itself is made redundantly with two processing units. We therefore assume that it would be at much higher cost than just one processing unit.

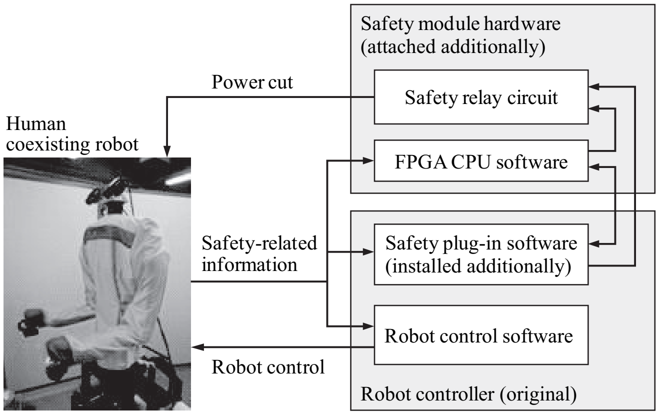

Fig. 3. Block diagram of safety module

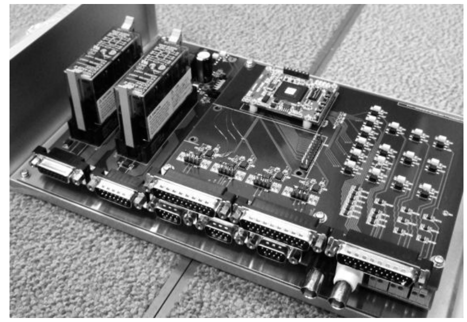

Fig. 4. Safety module hardware

To overcome these problems, we propose a different architecture for module based safety function integration for safe human-robot interaction.

III. Safety module

A. Required specifications of safety module

Continuing our discussion from the previous section, the requirements for module based safety function integration can be summarized as follows.

First, based on international safety standards, Category 3 or higher level of safety is necessary. To realize this, redundant implementation and execution of safety functions is essential.

Second, considering the complexity of the cell production based work environment, and to realize efficient cooperation with human workers, the system will have to interface with a multitude of safety sensors and control interfaces. In addition to this, the system will also have to deal with multiple restriction patterns and safe guards for various parameters such as work area, and tool point velocity, depending on the state of human workers around the robot.

Finally, it is desirable that this safety related functionality be flexible, extensible and also detachable, so as not to interfere with the robot's deployment and cost effectiveness.

B. Architecture of safety module

In this research, we propose a new architecture in which we can fulfill the safety requirements stated above. This architecture consists of an optionally added hardware module and plug-in software installed in the robot controller. A block diagram of the proposed architecture is shown in Fig. 3.

Sensor information and control signals from an operator are sent to both the external safety hardware module and safety plug-in software so that the processing is executed in the CPUs of both the external module and the robot controller in parallel.

As shown in Fig. 3, all safety-related signal-handling and transfer is duplicated to meet Category 3 requirements of safety system redundancy.

C. Safety relay system

We have developed an experimental hardware module as shown in Fig. 4.

In this module, a safety-relay circuit is implemented by using a well-known Category 4 level circuit. Commercially available forced-guided contact relays, referred to as safety relays, cut the motor power of an industrial robot in the event of an emergency to avoid accidents. By using the safety relays, dangerous failures, such as an undetected welding of a relay contact or unexpected restart of the robot can be prevented. If the power to the safety module fails, the power to the robot is also shut off, ensuring safety.

In the SP-02, the relay circuit in the safety hardware module is used to shut off the power to the robot using redundant signals from both independent processing of the hardware module and the plug-in software. When applying the module to a robot that has a built-in safety relay circuit, external signals from the hardware module can be sent to the relay circuit to achieve redundant power control.

D. Logic circuit using FPGA

We used an Field Programmable Gate Array (FPGA) chip for processing logical operations of the safety functions. By using an FPGA, various types of Input and Output(IO)s such as a parallel IO or serial IO can be implemented as needed, and also it is easy to extend or modify the FPGA for IOs or processing functions subsequently. In this system, we have implemented parallel IO ports for control by operators, and for sensor inputs such as the light curtain sensors. A serial IO also is used to communicate with the plug-in software.

E. Using soft processor core

A soft processor core is used in the FPGA to realize flexible software processing of safety functions. By detecting and processing input signals from sensors and user operation, the appropriate safety function is selected and risk is avoided.

One important advantage of a soft processor core is that the circuit and the software implemented in the FPGA do not need to be changed in the event of an FPGA upgrade. It is not permitted to subsequently change certified software, as shown in ISO standards, however an FPGA chip can be upgraded using the exact same software.

F. Sensor data acquisition of joint angles

To realize operational area limitation of the robot to provide safety features, the joint angles of the robot's actuators are needed. To further ensure the joint angle sensors data is reliable, the joint angle sensors should be redundant. The SP-02 has two independent sources of joint angle information, and both sets are sent to the hardware module and the plug-in software. We feel that it will become important for next generation robots that share workspace with the human workforce have redundant sensors for reliability.

G. Implementing safety plug-in software

A precondition of our proposed architecture is that additional software should be installed in the robot controller. Controllers for conventional industrial robots are not designed to allow subsequent installation of software. However, we can expect an open architecture- such as the recently developed and improved RT middleware [10]- to be used as the controller of next-generation service robots. Plug-in modular software on demand should be available to robots in the near future.

H. Function of safety plug-in software

The safety plug-in software not only implements safety functions duplicate to the hardware module, but also has its own original functions.

First, the plug-in software is invoked by the control software and the user interface of the robot. The robot controller calls the plug-in software to check the safety status of the robot and decides whether to start moving. When a potentially dangerous situation is detected, the robot can move to avoid the danger or just stop. After confirming the risk has been eliminated, a recovery process comes up. These functions also can be activated by direct user control through switches or control panels.

Second, the plug-in software calls the functions of the control software, such as posture calculation of the robot for moving-space limitation and/or hand-speed control. In this manner, plug-in software can execute a complex calculation by using the high-performance processing of the robot controller. On the other hand, an FPGA processor core is typically low in processing power, but redundant calculation of essential safety functions can be executed with lower precision in a simplified way.

I. Coordination and observation of duplicated systems

As described above, the safety plug-in software and hardware module acquire the same information so that they work synchronously and simultaneously. Each unit also constantly checks the status of the other, and if an unexpected or unknown status comes up, robot motion is not permitted and an emergency stop take place. A watchdog signal also is used by each unit to observe whether the other is alive.

IV. Evaluation of safety module

A. Implementation of safety module to coexisting robot

We implemented and evaluated a safety module, shown in Fig. 4, to the humanoid torso robot SP-02. The safety plug-in software is installed in the robot controller of the SP-02 and the robot control software is modified to call the plug-in software and check the safety status and activate safety monitoring functions on startup and during a motion. Safety related hardware I/O, including an emergency stop button and control switches, are implemented with dual contact switches and sensors. These are also connected to the safety hardware module.

B. Evaluating startup, stop and restart

After fitting an SP-02 robot with the safety module and going through the proper start up procedure, we confirmed that the robot motion stops immediately after the emergency stop button is pushed, and the power supply to the servo controller is shut off by the redundant safety relays. To restart the robot, both the hardware module and the safety plug-in software need to be reset for further to motion, so any unexpected reboots will be detected.

C. Safe space sharing of human and robot

The rectangular frame between a human worker and robot, enclosed by the light-curtain sensors as shown in Fig. 2, is the shared zone for component exchange in the cell production process. The light curtains are commercial products and certified as Category 3 safety devices. The two independent sensor outputs from the light curtains are connected to the safety hardware module and the robot controller and processed in parallel. When the human worker and the robot enter the shared zone at the same time, the robot stops movement until the human worker leaves the zone. This condition check is executed in the safety safety hardware module and safety plug-in software redundantly, and we have confirmed that the function works properly.

D. Evaluation of movement space limitation

The working area of the robot in this production process is always within 50 cm above the workbench as shown in Fig. 2 and within the sharing zone for component exchange. Thus, the maximum movement area of the robot is limited by a rectangular area, as shown in Fig. 5. If the robot attempts to leave this area, the motion is stopped by the safety plug-in software, regardless to the output of the robot control software.

To evaluate this function, an experiment is conducted by applying an incorrect program for robot motion, an order to leave the restricted area, and motion is stopped at the moment the robot actually tries to get over the limitation.

However, the movement area limitation is currently implemented only by the plug-in safety software, which is not compliant with Category 3 safety. In the near future, if higher reliability is required for this area limit function, we will implement an area-limit procedure in the FPGA with lower but adequate precision.

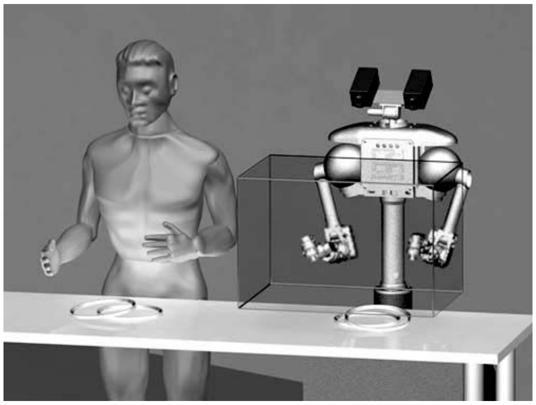

Fig. 5. Movement space limitation (Detail of robot in this figure is modified from its original)

E. Evaluation of mutual observation

The observation function of each hardware module and safety plug-in software checks that proper synchronization is confirmed during the startup, stop, and restart sequence. To check the watchdog signals, we stopped the signal transfer manually and found that the emergency stop was induced within the expected time frame.

F. Evaluating safety of workspace sharing

The features listed above was evaluated for safety and efficiency at an actual factory in which shared workspace production process was implemented. By using a SP-02 with the safety module, no severe accidents, which would result in harm to human workers, has occurred in the four months since the system was installed.

V. Conclusion

To achieve the human-robot interaction during manufacture, we propose a new architecture for a safety module that integrates required safety functions. We also developed an experimental system and implemented it in a real production process to evaluate its safety features.

In future, we will apply the safety module to different types of human workspace sharing robots and increase the functionality and reliability of the safety module by improving the software and inner-FPGA circuitry.

VI. Acknowledgments

This study was supported by Project for Strategic Development of Advanced Robotics Elemental Technologies in FY2006-FY2008 from NEDO of Japan. We would also like to show our gratitude to the professional support of Kawada Industries, Inc. and THK, Co., Ltd.

References

[1] Ordinance on Industrial Safety and Health, Section 9. Industrial Robots, Article 150-4 Prevention of Danger During Operation, Japanese Ministry of Health, Labour and Welfare.

[2] "Safety guidelines for next-generation robots", Japanese Minister of Economy, Trade and Industry, 2007

[3] ISO 10218:2006: Robots for industrial environments – Safety requirements – Part 1: robot

[4] Feng Duan, Masahiro Morioka, Jeffrey Too Chuan Tan, and Tamio Arai, "Multi-Modal Assembly-Support System for Cell Production", International Journal of Automation Technology, Vol.2, No.5 pp. 384-389, 2008

[5] ISO 12100:2003: Safety of machinery – Basic concepts, general principles for design –

[6] Ogorodnikova Olesya, "Human-Robot Interaction Safety problems", 15th International Workshop on Robotics in Alpe-Adria-Danube Region, pp.63–68, Hungary, 2006

[7] ISO 13849-1:1999 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

[8] Bruno Geiger, "New Robot Based Technologies for Industrial & Automotive Market", 1st Robotics & Automation Conference and Robo Expo 2008

[9] Elan Schaltelemente GmbH & Co. KG "ESALAN Safety Controller", *http://www.elan.de*

[10] Noriaki Ando, Takashi Suehiro, Kosei Kitagaki, Tetsuo Kotoku, Woo-Keun Yoon, "Composite Component Framework for RT-Middleware (Robot Technology Middleware)", 2005 IEEE/ASME International Conference on Advanced Intelligent Mechatronics (AIM2005), pp.1330-1335, 2005.07, Monterey, California, U.S.A.