Figure 1. Flexible robotic cell

The design of the robotic cell provides numerous opportunities, although the drawback is the increased number of possible threats, one of those is aforementioned shared workspace. Facing the robots, there are two conveyor belts powered by two asynchronous motors, manufactured by Motovario, which are vastly used in industrial solutions. Their task is to supply the robots with workpieces. The robots can manage to reach both of the conveyor belts and manipulate with oncoming objects. Taking everything into account, flexibility of this robotic cell can provide many different scenarios found in the process industry, may it be simple as maneuvering objects from one conveyor belt with only one robot, or a more complex approach with robot collaboration.

There are several sensors placed around the conveyer belts, which enrich the system and provide easier object detection and manipulation, such as inductive and photo reflective sensors. Inductive sensors detect presence of metal in workpieces, while photo reflective sensors detect if some workpiece are in some position of interest on conveyers.

In order to achieve synchronized control of every component in the system, robotic cell consists of a Programmable logic controller (PLC), which can congregate every information from the peripherals, and act depending on the outcome. The PLC exchanges information over the Ethernet/IP with all vital devices in the robotic cell (robots, conveyer belts, ...)

III. HAZARD IDENTIFICATION

Every component in a system can cause a system failure or a hazard, and manufacturers of those components are aware of that. What if there is a plethora of combined components working in a well-organized system, then a whole new set of possible hazards would emerge. Aside from component failure, a major safety problem occurs when humans interact with machines, this may be collaborative work, maintenance, testing, cleaning or readjustment. Furthermore, there are additional passive health hazards which can cause severe injuries may it be continuous inhalation of harmful fumes, hearing loss caused by environmental noise, high-pressure induced wounds or radiation.

Hardly can safety systems guarantee complete hazard-free environment, while problems occur as a series of unpredictable events, or as intentional security breach. Every system has weaknesses which should be pinpointed while planning how can safety functions be implemented, and step by step decrease possibility of hazards. Safety functions can be derived from additional safety components or from rudimentary approach as in cable management, proper signalization and warning sign posting. When it comes to industrial robotic incidents are grouped into 4 categories [1]:

- impact or collision accidents,
- crushing and trapping accidents,
- mechanical part accidents,
- other accidents.

Impact accidents are commonly associated with unpredicted movements of robot`s arm and unpredicted change of variables in robot`s program, while crushing accidents have similar causes they involve additional peripheral equipment. The breakdown of the robot`s components or equipment fall within mechanical accidents. All of the above-mentioned accidents can occur for numerous reasons which can be divided into several groups [2]:

- human errors,
- control errors,
- unauthorized access,
- mechanical failures
- environmental sources
- power systems
- improper installation.

Taking everything into consideration how can potential hazards be noticed it is of utmost importance to tackle the problems in order to comply with Serbian regulations [3]. Rule book applies to every type of machines, interchangeable equipment, safety components, lifting accessories, partly completed machinery etc. It is stated that safety components are components which are not necessary for the main system to properly work, while the safety system is a standalone system. Risk assessment is of crucial importance as an initial step to establish requirements for occupational health and safety, as it is prerequisite for design and assembly of the safety system. Besides pinpointing potential hazards which machine can create, benefits of opting for risk estimation process for machines are determination of machine limitations, estimation of possible severity of injury and risk reduction for identified peril areas. In accordance to the safety legislation, improper usage should be foreseen and taken into examination when the system is designed, thus providing an insight into what should an operator do and in which manner will he use the machine. Given the fact that robots can work in different modes, the robotic cell needs to have a clearly indicated mode dial which can be blocked in any position. Safety fence presents the first line of safety, on account of this it should be placed to a safe distance, not to allow any collisions. Residual identified potential hazards which cannot be limited, must be depicted in a comprehensible way and placed to be clearly visible, this applies also to every device used for providing information, may it be a HMI panel or light signalization. Every machine made for use in the industry, must yield a manufacturer manual or user manual with technical documentation.

IV. Risk Assessment

In order to implement safety functions, initial safety estimation is required for each component of the safety system. Furthermore, in compliance with safety regulations and standards, there are given safety levels which are defining level of risk-reduction. Two international standards will be taken into discussion, EN ISO 13849 and EN IEC 62061 [4]. While both organizations have the same objectives, and they do work together in the field of standardization, safety levels are defined in different way. Both standards define safety level regarding probability of failure per hour. EN ISO 13849 provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems [5]. International Organization for Standardizations provides Performance levels, or abbreviated PL, which are measured on the scale from letter "a" to "e", where level PL_e stands for most risk reducing level. Alternatively, International Electrotechnical Commission with IEC 62061 make their own recommendations for the design, integration and validation of safety-related electrical, electronic and programmable electronic control systems, or as they call them SRECS [6]. IEC standard introduces Safety Integrity Levels, or abbreviated SIL, with a scale from 1 to 3, where level SIL3 represents most risk reducing level. Methodology of risk assessment according to EN ISO 13849 is based on series of safety questions related to the probability of accidents, breakdowns or similar hazards [7]. Initially, it is necessary to establish severity of injuries which can occur while operating the machine, are they reversible injuries (S1) or irreversible injury or death (S2). Following, defining frequency and/or exposure time to the hazard, seldom to quite often and/or the exposure time is short (F1) or frequent to continuous and/or the exposure time is long (F2). Conclusively, determining probability of avoiding the hazard, as for possible under specific conditions (P1) or scarcely possible (P2). Required safety level estimation for the flexible robotic cell is depicted in figure 2, where it is shown that necessary performance level is PL_d per EN ISO 13849 risk assessment methodology.

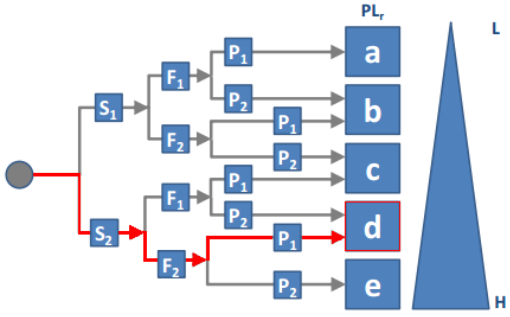

Figure 2. Safety level estimation in accordance with EN ISO 13849 standard for the flexible robotic cell

While there exist discrepancies between EN ISO 13849 and EN IEC 6206, they are correlated in the sense that they both refer to probability of dangerous failure per hour [8]. Relationship between Performance Levels and Safety Integrity Levels is given in Table I, as well as probabilities for every given level.

TABLE I
Safety level correlation between EN ISO 13849 and EN IEC 62061 standards

EN ISO 13849 Performance Level(PL)	Probability of dangerous failure per hour [1/h]	EN IEC 62061 Safety Integrity Level(SIL)
a	$\geq 10^{-5} \ldots < 10^{-4}$	No special safety requirements
b	$\geq 3 \times 10^{-6} \ldots < 10^{-5}$	1
c	$\geq 10^{-6} \ldots < 3 \times 10^{-6}$	1
d	$\geq 10^{-7} \ldots < 10^{-6}$	2
e	$\geq 10^{-8} \ldots < 10^{-7}$	3

TABLE II
Safety level correlation between EN ISO 13849 and EN IEC 62061 standards

Variable name	Probability of (certain event)
P_1	Occurrence of an irreversible human failure that could result in or allow an accident
P_2	Occurrence of a reversible human failure that could result in or permit a mishap
P_3	Robot possessing an adverse characteristic that could result in human error
P_4	Robot experiencing an adverse environmental condition that could result in human error
P_5	Occurrence if the failures that could result in mishaps
P_6	Occurrence of those malfunctions that could result in accidents unless the appropriate actions are taken in a timely manner
P_7	Robot having an adverse characteristic that could result in human error
P_8	Robot experiencing an adverse environmental condition that could result in robot failure
P_9	Robot possessing an adverse characteristic that could result in injury, damage, or loss in the absence of material failure or error
P_{10}	Robot experiencing an adverse environmental condition that could lead to damage or injury in the absence of error or failure
P_{11}	Necessary action taken as required

Although these standards refer to every machine, a more robot specific estimation of probability of an accident occurring related to the operation of a robot can be expressed by (1), where all of the split probabilities are described in Table II [9]. P_{ar} is the probability of an accident occurrence from the operation of a robot.

$$P_{ar} = \sum \{P_1 + P_2(1-P_{11})\}\{1 + P_3 + P_4\} + \sum \{P_5 + P_6(1-P_{11})\}\{1 + P_7 + P_8\} + \sum (P_9 + P_{10})(1-P_{11}) \quad (1)$$

V. SAFETY SYSTEM

To ensure high level of safety while operating the flexible robotic cell, safety components are introduced which are implemented in the safety system. The core processing component is the programmable logic controller (PLC) with fail-safe processor, providing required safety level and serving as acquisition, control and decision-making component. Peripheral components of the safety system are:

- Emergency stop push button,
- Safety interlock switch with separated activator,
- Magnetic proximity sensor,
- Safety light curtain,
- Signalization lights;

Safety interlock devices are used for detecting if doors are properly closed. Proximity sensors serve the same purpose, although they are implemented on sliding windows, they can provide information regarding the position of the windows, whether they are closed or opened, so we can restrict robots of working in automatic mode. In addition to identifying presence in the robot enclosure, light curtains can protect against access into hazardous point and areas, by detecting if an array of light rays is broken by some object. Light curtains are efficient if the operator has to frequently enter the robot work area and if time management is of vital importance. Emergency stop buttons and signalization lights belong to the group of basic safety components when some problem has happened. Implemented safety components are represented in figure 3.

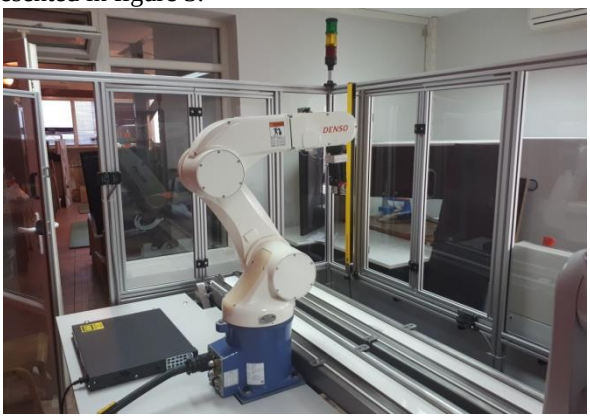

Figure 3. Safety system components implemented in the flexible robotic cell

VI. CONCLUSION

Industrial robots are increasingly becoming a normal sight in industrial facilities. Given the fact that industrial robots can work in dangerous environments, they also contribute to possible hazards for humans. They can move with such a force, or maneuver heavy and sharp objects so which can be harmful for humans. Safety systems can deal with these situations by restricting modes of operations, speed adaptation and managing movement boundaries when humans are in the close proximity to the robot.

Implementation of safety systems provide additional security when operating the machine. Hardly can it be neglected, as it is a prerequisite for proper commissioning of the machine. Although it is a tedious task to identify every potential hazard, it certainly is the main pillar for safety system realization. Industrial robots are usually installed inside a guarded work cell, which is the same case with the flexible robotic cell developed at the University of Belgrade, School of Electrical Engineering, however additional safety components were introduced to reduce probability of dangerous failures. Risk assessment has been conducted to evaluate the safety design of the flexible robotic cell. Given the risk estimation results, which concluded that PL_d safety level should be employed. Each component of safety system has to be at least PL_d rated, or SIL 2, so the whole system would be verified as PL_d. However, it should be stated that in every system there are some residual risks which cannot be predicted, and human awareness should be increased.

Further research in the field of safety technology can provide new approaches to human-robot co-operation and new types of robot applications.

REFERENCES

[1] M. Alvarez, Working Safely Around Industrial Robots in *Gateway for safety and health information resources*, may 2002.

[2] C. Reese, *Material Handling Systems: Designing for Safety and Health*, 2000.

[3] Ministry of Economy and Regional Development of Serbia, Pravilnik o Bezbednosti *in Službeni glasnik RS*, 2016.

[4] S. Robinson, "Functional Safety Standards for Machinery", TÜV SÜD, 2014.

[5] International Organization for Standardization, *Safety of machinery -- Safety-related parts of control systems*, ISO 13849-1, 2015.

[6] International Electrotechnical Commission, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*, IEC 62061, 2005.

[7] D. J. Smith, K. G. L. Simpson, Safety Critical Systems Handbook, third edition 2010.

[8] J. Ridley, D. Pearce, Safety with Machinery, second edition, 2006.

[9] B.S. Dhillon, Robot System Reliability and Safety, 2015