# LIVING WITH THE CHALLENGES TO FUNCTIONAL SAFETY IN THE INDUSTRIAL INTERNET OF THINGS

***Stewart H Robinson MIET MInstMC***

*Principal Engineer and Functional Safety Expert*
*Industry and Energy Products Division*
*TÜV SÜD Ltd*
*Belasis Business Centre*
*Coxwold Way*
*Billingham – TS23 4EA*
*United Kingdom*
*Stewart.Robinson@tuv-sud.co.uk*

**Keywords**: FUNCTIONAL SAFETY, INDUSTRY 4.0, SMART MANUFACTURING, COBOT

## Abstract

This paper addresses the challenges for the realisation of Functional Safety in the implementation of "Smart Manufacturing" (Industry 4.0, also known as the fourth industrial revolution). The use of devices connected to the Industrial Internet of Things (IIoT) is a fundamental part of Smart Manufacturing to help realise the benefits of digitalisation as part of the 4th Industrial Revolution. In this paper traditional approaches to achieve Functional Safety are compared with the emerging technologies that make use of IIoT. The paper includes some examples of industrial equipment used in manufacturing that are typical of the types of machinery that will make use of IIoT, for example Collaborative Robots (Cobots), Autonomous Guided Vehicles (AGVs), and a combination of these Autonomous Mobile Robots (AMRs). As well as discussing the challenges the paper highlights the potential economic benefits of having the factories of the future connected to the Industrial Internet of Things.

## 1. Introduction

This paper deals with some of the obstacles (challenges) and advantages that exist when applying the Internet of Things in industrial processes. The specific focus is on how the challenges relate to "Functional Safety", particularly to machinery used in manufacturing industries.

## 2. Functional Safety

Functional Safety can be defined as part of the safety of machinery and the machine control system that depends on the correct functioning of a Safety-Related Control System. For machinery it is a statutory requirement that hazards (something with the potential to cause harm) are identified and that the risks associated with the hazards are assessed, in this context risk is defined as the combination of the severity of possible harm and the likelihood of the occurrence of that harm. Any unacceptable levels of risk associated with the identified hazards must be reduced to a level that is as low as reasonably practicable (ALARP). Safety functions implemented by safety-related control systems make a contribution to the reduction of the risk, usually by reducing the possibility of occurrence.

### *2.1. Machinery Safety Functions*

Safety functions on machinery are often provided by using devices that detect the presence of a person in a danger zone and then having an automatic reaction that places the hazard in a safe state. For example, at the entrance door to a robot cell there may be an interlock switch as shown below, the outputs of the switch would typically be connected to a safety monitor of some kind (e.g. a 'safety relay' or a 'safety PLC') and the outputs of this device would be connected to the safety circuits of the robot controller.

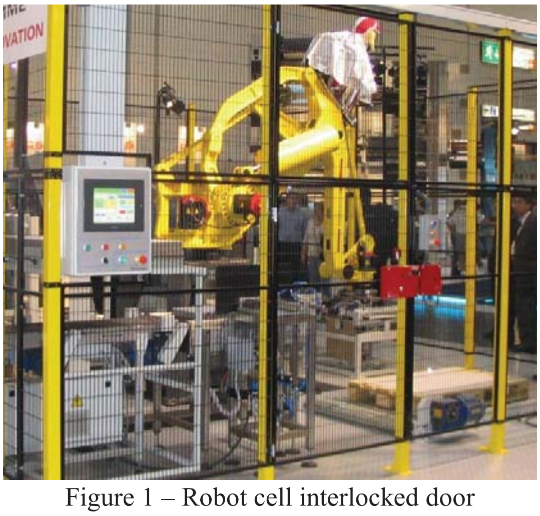


Figure 1 – Robot cell interlocked door

An arrangement like this would provide the safety function at a suitable level of risk reduction (SIL or PL, see next section) and also satisfy other requirements for example a safety reaction time.

The functions should be 'de-composed' into subsystems as a logical representation, so in the example for the robot cell the function may be represented as:

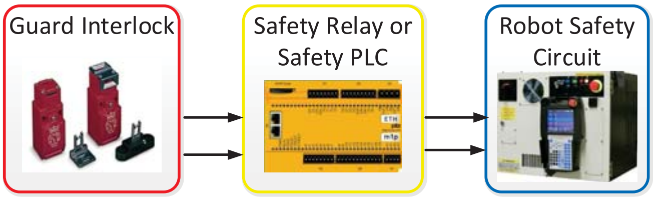


Figure 2 – Functional block decomposition

### 2.2. *Safety Integrity Level (SIL)*

The level of risk reduction required from a safety function is quantified as an average frequency of dangerous failure per hour (normally represented as a $PFH_D$) or occasionally as an average probability of failure on demand (PFD). There are two international standards that describe the requirements of safety systems for machines these are IEC 62061 [1] and ISO 13849 [2].

IEC 62061 uses SIL and describes 3 levels where SIL1 is the lowest level and SIL3 is the highest (most reliable) level. SIL1 requires functions to achieve a $PFH_D$ of less than $1x10^{-5}$ per hour, SIL2 $<1x10^{-6}$ per hour and SIL 3 $<1x10^{-7}$ per hour. ISO 13849 [1] also has targets for $PFH_D$ of functions but describes them as 'Performance Levels' (PL), there are 5 Performance Levels from PLa to PLe where the $PFH_D$ for PLd is directly equivalent to SIL2 and the $PFH_D$ for PLe is directly equivalent to SIL3.

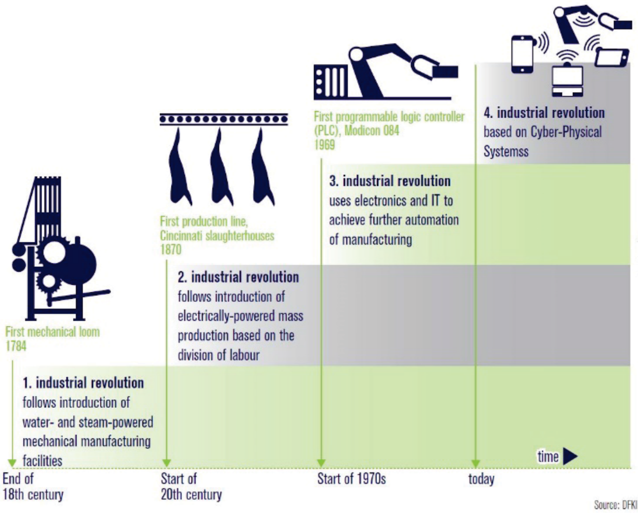
In the example of the robot cell interlock the $PFH_D$ of the function would be the sum of the $PFH_D$s of the individual subsystems.

In a system where the subsystems are physically connected to each other by 'hard wiring' the statistical reliability of the interconnecting means is often discounted (fault excluded), in cases where the interconnection is by a communication network it would normally be a dedicated and certified safety network that is used where safety is assured by the use of safety protocols that are embedded in the systems, examples include PROFIsafe; EtherNet/IP, SafetyNET p etc. These networks have a very low $PFH_D$ and deterministic reaction times.

**Note: In addition to the quantified aspects of functional safety it is important to also consider the non-quantified 'systematic' requirements.**

## 3. Industry 4.0 (Smart manufacturing)

"Industry 4.0 is a name given to the current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of things, cloud computing and cognitive computing. Industry 4.0 is commonly referred to as the fourth industrial revolution." [3]


First mechanical loom 1784
1. industrial revolution follows introduction of water- and steam-powered mechanical manufacturing facilities
First production line, Cincinnati slaughterhouses 1870
2. industrial revolution follows introduction of electrically-powered mass production based on the division of labour
First programmable logic controller (PLC), Modicon 084 1969
3. industrial revolution uses electronics and IT to achieve further automation of manufacturing
4. industrial revolution based on Cyber-Physical Systemss
complexity
time
End of 18th century
Start of 20th century
Start of 1970s
today

Source: DFKI 2011

Figure 3 – The Industrial Revolutions

It is also sometimes referred to as smart manufacturing.

"Industrie 4.0" is a concept endorsed and promoted by the German government.

### 3.1. *Cyber Physical Systems*

Components, tools and machines are becoming Industry 4.0 Components as Cyber-Physical Systems (CPS). This can be defined as a system of collaborating computational elements including mechanical and electrical elements connected in a smart cloud able to communicate in real time. The combination of technologies (cloud, AI, 5G wireless, etc.) enables new capabilities (software defined networking, machines, platform, etc.).

### 3.2. *Digital Twin*

The concept of smart manufacturing includes the use of digital twins to represent physical assets (e.g. machines). The digital twins are part of the Industrial Internet of Things.

## 4. Industrial Internet of Things (IIoT)

It is sometimes said that the IIot is ahead of the IoT, this may be, at least in part, due to the greater incentives for adoption of IIoT. For example in industry the IIot is used to connect critical sensors and machines where a failure might result in serious consequences, whereas IoT tends to be used in consumer level devices (e.g. smart home devices, wearable fitness trackers, etc.) where failures are inconvenient but not normally critical.

### 4.1. *IIoT Innovations*

There have been many innovations in the last few years that have presented significant opportunities for industries. Hardware innovation has resulted in devices like sensors becoming more powerful whilst costs have decreased. Power consumption improvements and battery technology has resulted longer run times. Connectivity has also improved meaning that cloud communications is now simpler and cheaper. The analytics that can be applied to the data gives a greater insight into industrial processes and can help optimise processes, reduce downtime and predict the need for maintenance intervention.

### 4.2. *IIoT Advantages*

The adoption of smart manufacturing which includes the use of IIoT and Cyber Physical Systems brings many advantages. A study about the IIoT commissioned by the World Economic Forum [4] summarised the opportunities and benefits as:

"Our research reveals that disruption will come from new value creation made possible by massive volumes of data from connected products, and the increased ability to make automated decisions and take actions in real time. The key business opportunities will be found in four major areas:

- "Vastly improved operational efficiency (e.g., improved uptime, asset utilization) through predictive maintenance and remote management
- "The emergence of an outcome economy, fuelled by software-driven services; innovations in hardware; and the increased visibility into products, processes, customers and partners
- "New connected ecosystems, coalescing around software platforms that blur traditional industry boundaries
- "Collaboration between humans and machines, which will result in unprecedented levels of productivity and more engaging work experiences" [4]

However there are also challenges to be overcome.

## 5. Challenges of IIoT for Functional Safety

According to the World Economic Forum survey the second greatest barrier inhibiting the adoption of IIoT was "Security concerns" (the greatest barrier by a small margin was "Lack of interoperability of standards"). [4]

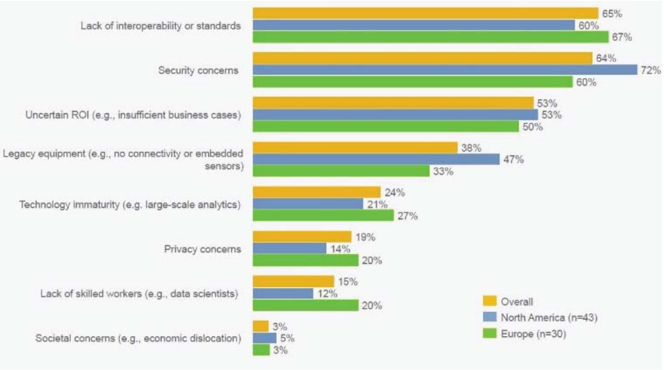


Figure 4 – Barriers to adoption of IIoT

There are various challenges to overcome when using IIoT, and they include the risks associated with security and data privacy of course, but these are outside of the scope of this paper.

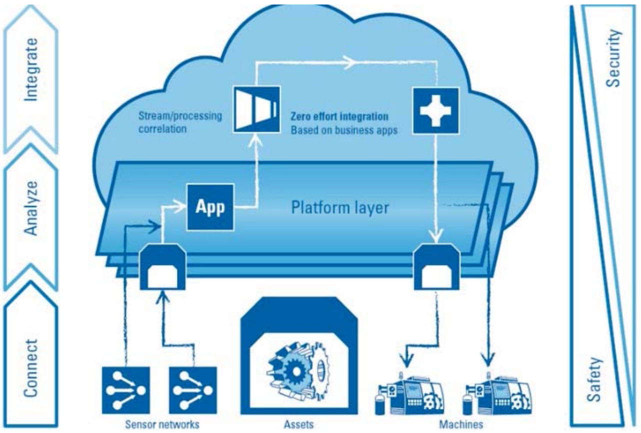


Figure 5 - Safety and Security lifecycle

The challenges when using IIoT for functional safety are primarily to do with data integrity and reaction times. In the example of the robot cell interlock the consequence of the interlock device failing to report to the cloud it's correct state, or the failure of the safety PLC to receive the status of the interlock, or the failure of the robot controller to receive a shut-down command, etc. etc. could all result in a dangerous failure and the loss of the function. Quantifying the reliability of cloud-based communication as a $PFH_D$ is a significant challenge.

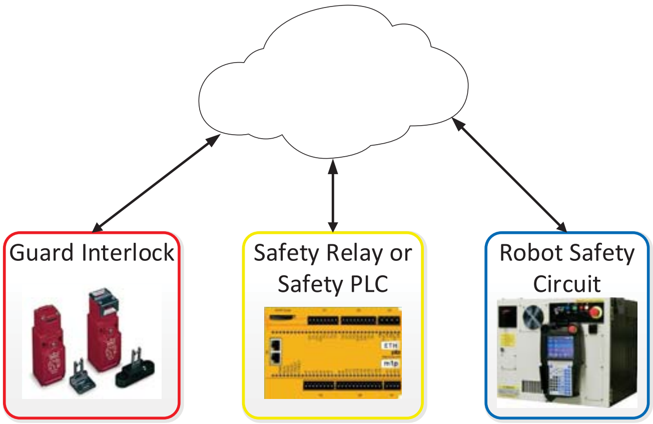


Figure 6 – Devices exchanging data through the cloud

It might also be the case that one or more of the components are in the cloud. The challenge of having an acceptable and justifiable $PFH_D$ then becomes even greater.

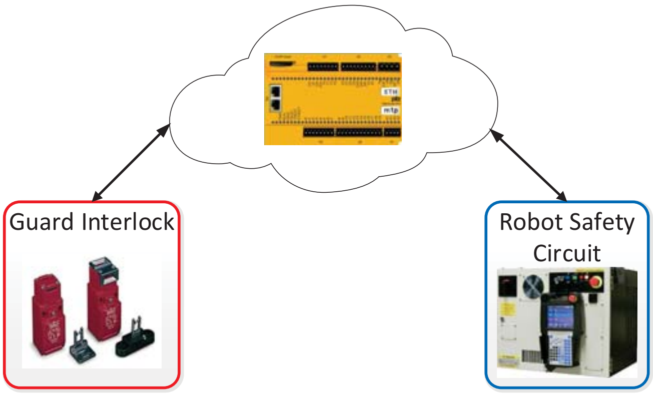


Figure 7 – Systems embedded in the cloud

### 5.1. *Reaction times*

Reaction times of safety functions are also critical, using an example of a presence sensing device to stop hazardous movement it is important to position the devices or the detection zones at a suitable distance from the hazard to ensure that movement will have stopped before anyone could come into contact with the hazard

The following illustration shows an 'area scanner' monitoring the approach areas of a robot. An area scanner, sometimes called a laser scanner, is a two dimensional "Active Opto-Electronic Protection Device using Diffuse Reflection" (AOPDDR). These devices can be programmed with warning zones (yellow in the diagram), and trip zones (red in the diagram). In this example if anyone is detected the red zone the robot must be stopped and not allowed to move whilst the area is occupied.

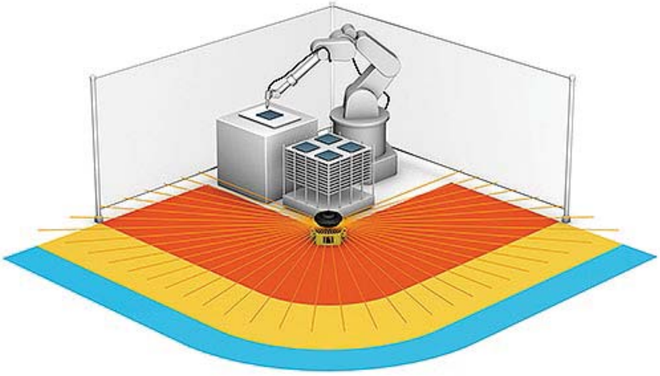


Figure 8 – Area scanner monitoring approach zones

The separation distance between the edge of the red zone and the working 'envelope' of the robot is established by applying the measures and formulæ given in the international standard ISO 13855 [5]. The basic formula is S = (KxT)+C where:

S = Minimum separation distance (mm);
K = Approach speed (mm/s);
T = overall system stopping performance (s)
C = Intrusion distance (mm)

The value for K for whole body approach (walking) is 1600mm/s, the value for C is 850mm (unless the detection device has high resolution).

Devices like an area scanner would usually have a reaction time in hundreds of milliseconds (e.g. 100ms) and the time for hazardous movement to stop after a stop command is received might be a second or so giving an overall stopping time (T) of 1.1s. Using those values if the devices were directly connected to each other would give a separation distance (S) of:

S = (1600 x 1.1) + 850;
S = 1760 + 850 = <u>2610mm</u>

If the devices are connected using IIoT through the cloud the reaction time of the system would be increased, and the time might not be deterministic. This could result in applications like this requiring separation distances that become impractical.

## 6. Types of machines using IIoT

There are very many types of machines that will ultimately be connected to the IIoT. A "Smart Factory" may have all machines configured as modules which will feature 'Plug & Play' intelligent configuration, this will also of course include the checking and certification of the functional safety aspects.

The "Technologie-Initiative SmartFactory KL e.V" [6] was founded in 2005 by: BASF; the German Research Center for Artificial Intelligence (DFKI); KSB; Pepperl+Fuchs; ProMinent; the TU Kaiserslautern and Siemens. With the aim of being a "Pioneer of Industrie 4.0". It has now grown to include approximately 50 members and they have jointly developed an “innovative demonstrator platform capable of presenting many technical solutions”.

As part of this concept a dynamic modular safety system has been developed giving an automated certification procedure for functional safety.

Some of the newer or emerging types of machine that will make use of the IIoT are Collaborative Robots (Cobots), Automatic Guided Vehicles (AGVs) and a combination of these Autonomous Mobile Robots (AMRs)

### *6.1. Collaborative Robots (Cobots)*

Collaborative Robots, sometimes referred to as cobots, are designed to work alongside humans in a “collaborative workspace”, an area where the robot and the human can perform tasks simultaneously

Unlike more traditional machines, which are ‘caged’ by a guarding mechanism, collaborative robots often operate in the human-occupied workspace without safety fencing. However, not all collaborative robots are guard-free, depending on their function and related safety requirements.
In order to ensure that humans are not exposed to unacceptable risks when working collaboratively the current standards describe four separate measures that can be used to provide risk reduction. It is required that at least one of these requirements needs to be fulfilled, in addition to having visual indication that the robot is in collaborative operation.

The standards are ISO 10218 part 1 [7] and ISO 10218 part 2 [8] and the four measures are:

1. Safety-rated monitored stop
This measure requires that when it is detected that a human has entered the collaborative workspace, the robot should be stopped. The stop condition should then be maintained until the human leaves the workspace.

2. Hand guiding
In this mode the human can guide the robot at the end effector by hand. Additional requirements for safety include safe-limited speed monitoring, a local emergency stop, and the use of an enabling device, which is a three position device that has to be held in the centre position.

3. Speed and separation monitoring
In this mode, the robot must maintain a specified separation distance from the human and operate at a predetermined speed. This measure requires careful risk assessment and needs to take account of safety distances, which should include the consideration of approach speeds of parts of the human body as described in EN ISO 13855 [5].

4. Power and force limiting by inherent design or control. In this mode the power and force of the robot actuators need to be monitored by safety related control systems to ensure that they are within limits established by a risk assessment.

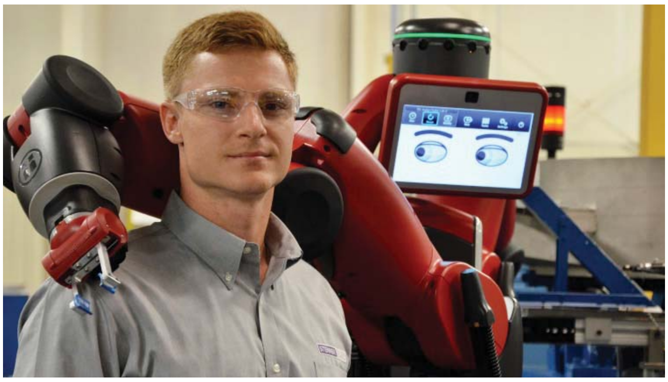


Figure 9 - Picture courtesy of Rethink Robotics

### *6.2. Automatic guided vehicles (AGVs)*

“Automatic guided vehicles (AGVs) are autonomous vehicles used to transport materials or accomplish specific tasks in many different industrial settings. They feature batteries or electric powered motors and computer technology that has been programmed to drive to and from specific points. Sometimes, since they are controlled by a computer rather than a human, AGVs are referred to as self guided vehicles, self-propelled vehicles or autonomous guided vehicles.

“An automatic guided vehicle is directed by a pre-programmed guidance system that varies in complexity based on the function being performed. Some AGVs are guided by lasers, but fixed path and free-range systems are more common. Other less common AGV systems include: camera guided AGVs, optical guided AGVs, forked AGVS, unit load AGVs, inertial guided AGVs, automated guided carts, towing vehicles and outrigger AGVs.” [7] www.automaticguidedvehicles.com

### *6.3. Autonomous Mobile Robots (AMRs)*

Autonomous mobile robots are, unsurprisingly, a combination of a Cobot and an AGV

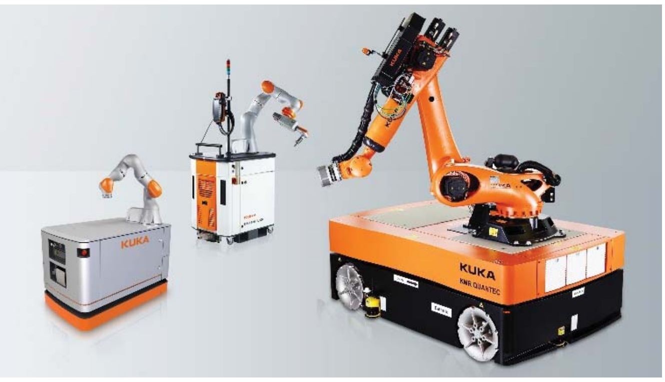


Figure 10 - Picture courtesy of KUKA Robots

The robot manipulator can be transported to any number of working positions to carry out it’s tasks.

## 7. Conclusion

In conclusion – Whilst the implementation of IIoT in industrial manufacturing facilities presents some challenges, particularly for Functional Safety, these challenges can be, and are being, overcome. There are already a significant number of industrial devices and systems that are connected to the IIoT in some way, and this includes safety-related systems. Although today this is mainly through connections based on cabled Ethernet based safety networks of some kind there are some exceptions where safety-related information is communicated wirelessly, but usually this is in a one to one configuration. A lot of work is being done on systems to make use of a cloud-based approach and this could include safety logic systems being 'in the cloud'. The development of Industry 4.0 concepts in real world applications is an example of this and checks and balances are being developed and implemented to ensure that data integrity and reaction times can be relied upon.

This development is being driven by industry because there are real socio-economic benefits, for example:

Increased efficiency of production could restore manufacturing to developed countries instead of the use of manufacturing in countries based on low labour costs. Whilst this results in a loss of unskilled or semi-skilled jobs it would also create new jobs for highly skilled people to design and support these high-tech systems.

Increased efficiency and agile production will also mean that manufacturing cost per unit will reduce and companies will be able to respond quickly to changing requirements from their customers

## 8. References

[3] Marr, Bernard. "Why Everyone Must Get Ready For The 4th Industrial Revolution". www.forbes.com/ accessed 17/02/2019

[4] "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services". World Economic Forum.

[6] "SmartFactory$^{KL}$ Pioneer of Industrie 4.0" Technologie-Initiative SmartFactory KL e.V. www.smartfactory.de accessed 18/02/2019

[9] www.automaticguidedvehicles.com accessed 18/02/2019

Standards

[1] IEC 62061:2015 "Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems

[2] ISO 13849-1:2015 "Safety of machinery — Safety related parts of control systems Part 1: General principles for design

[5] ISO 13855:2010 "Safety of machinery — Positioning of safeguards with respect to the approach speeds of parts of the human body"

[7] ISO 10218-1:2011 "Robots and robotic devices — Safety requirements for industrial robots Part 1: Robots"

[8] ISO 10218-2:2011 "Robots and robotic devices — Safety requirements for industrial robots Part 2: Robot systems and integration"