Safety as Bad Cop of Physical Assistance Systems?

Michael Rathmair, Mathias Brandstötter

Safety as Bad Cop of Physical Assistance Systems?

Michael Rathmair and Mathias Brandstötter

ROBOTICS, Institute for Robotics and Mechatronics,
JOANNEUM RESEARCH Forschungsgesellschaft mbH,
9020 Klagenfurt am Wörthersee, Austria
Michael.Rathmair@joanneum.at, Mathias.Brandstoetter@joanneum.at

Abstract. Constantly increasing variety of products and customer-specific requirements lead to more complex assembly lines in the shop floors. These new demands require novel systems and technologies such as flexible assembly lines, track and trace systems or assistive systems. In this paper, supporting systems on the physical level are analyzed and in particular robot assistance systems with respect to their safety aspects are discussed. Moreover, the current standards and guidelines in the field of robot safety and their development focus are presented. It is intended to provide a comprehensive overview of what role safety actually plays with assistance systems and how ongoing research may affect it in future.

Keywords: Safety · Collaborative robots · Human-robot interaction

1 Introduction and Motivation

Physical assistive systems in the context of this paper have the goal to support humans in a highly flexible and volatile industrial production environment. Besides already implemented fully automatic workplaces (e.g. for welding) there are still many semi-automatic assembly stations within a modern production line. Especially due to Industry 4.0 requirements as the increased need for flexible machines that can be adapted to fulfill smaller lot sizes under changing production conditions quickly and efficiently. For this reason, the number of assembly stations using advances of collaborative robotic systems as production assistance equipment even rises. A common vision is to develop an enhanced individual robotic asssistive system replacing the today's cordless electric screwdriver. However, in this paper we identify and discuss several challenges with a special focus on robotics safety that explain why this replacement is not as simple as it may seem at first glance.

Collaborative robotic assistance systems on the first side support workers in complex assembly tasks but on the other side they also provide valuable services in the automated manipulation of workpieces or perform intralogistic tasks (e.g. machine tending). However, the collaborative robots (mobile robots and serial manipulators) in a production facility, are not operated behind any physically

separating protective devices but act in a workspace which is largely shared between humans and machines. This has the consequence, that collisions between robotic equipment and human body parts are no longer avoidable. On the contrary, physical interaction/contact between the robot and the human can be used to further increase the performance of the assistive function and enhance easy operation features.

As already reported within this paper we illustrate current challenges, approaches to manage them and give an overview to future research trends in the field of industrial assisitive systems. Our focus is robot safety which has an increased significance in fanceless robot operation. In industrial manufacturing, there is an increasing need for flexible machines that are able to work autonomously and can be adapted to changing production conditions quickly and efficiently.

2 State of the Art Safety Standards and Guidelines for Industrial Assistive Systems

Assistive systems in the context of this work are permanently used in an industrial environment and require properties as robustness, reliability, precision and availability similar to classical industrial robots. Thus, industrial assisitive systems face different safety requirements in contrast to service robot applications. In addition to the EC Machinery Directive 2006/42/EC [1], specific standards and regulations for robot safety, in particular for serial manipulators the EN ISO 10218 (Robots And Robotic Devices - Safety Requirements For Industrial Robots) [2, 3], define the regulatory framework for safe cooperation between humans and robots in an industrial application context. For human-robot collaboration the since 2011 the ISO 10218 defines four clearly defined scenarios:

- **Safety-rated monitored stop:** The movements of a robot is stopped during human-machine interactions within the shared space. Such a state is safety-rated monitored with the consequence that the robot's drives can remain energized.
- **Hand guiding:** The safety is given by manual physical guiding of the robot under appropriately reduced speed.
- **Speed and separation monitoring:** Movements and speed parameters are adjusted in a way to keep a safeguard space between the operator and any part of the robot.
- **Power and force limiting by design or control:** Power and force control parameters are set in a way that in case of an occurring contact between a human and the robot given limits are not exceeded.

Taking into account the rapid development of collaborative robotics in 2016, the technical specification ISO/TS 15066 [4] as an extension to the ISO 10218 was published. On the first side, the specification includes more technical and organisational details especially about the power and force limiting operation mode.

On the other side, ISO/TS 15066 holds a table specifying limits for acceptable force and pressure values in the case of a human-robot contact situation. The given bio-mechanical load limits are derived from in-depth studies carried out with human volunteers under a strictly defined experimental set-up. At the time of writing (Nov. 2019) the ISO 10218-1/2 (part 1 and part 2) standards are under revision by the ISO/TC 299/WG 3 committee. The official release of both parts is scheduled by end of 2021. A major improvement in the perspective of collaborative robots is that two informative annexes based on the ISO/TS 15066 will be integrated. These Sections, Annex N: Limits for quasi-static and transient contact and Annex O: Power and force limited robot applications – Pressure and force measurements, are already integrated and released for comments in the ISO/CDrev3 10218 (committee draft revision 3) document developed at the 11th committee meeting in Waldkirch. Besides that, substantial changes e.g. in safety functions performance requirements are planned for the 2021 versions of the new ISO 10218-1/2.

Assistive systems based on mobile robots so called AGVs (automated guided vehicles) are also clearly regulated by the European machinery directive. Additionally, a national and an international standards are in place. First, the EN 1525:1997 (Safety of industrial trucks - Driverless trucks and their systems) [6] which is due to its release date of 1997 not longer representing state of the art technology. Second, the ISO/FDIS 3691-4 [5] which is currently in FDIS (Final Draft International Standard) state (Nov. 2019) will replace EN 1525:1997. As long as the standard is not officially published, manufacturers are obliged to directly fulfill the requirements given by the machinery directive without having a corresponding state of the art Type C standard [23].

Mobile manipulators are assistive systems where a robotic arm is mounted on a mobile platform. Depending on the purpose of the arm standards for mobile robots and/or stationary industrial robots have to be applied. There are no fully-compliant standards, guidelines or design proposals for this type of robot. However, in the US RIA (Robotic Industries Association) in cooperation with ANSI (American National Standards Institute) are working on the national standard ANSI/RIA R15.08 (Draft) which has the goal to bridge any gaps between regulations for AGVs, robot arms and mobile manipulators [24]. The R15.08 is in draft state since 2017 and consists of three parts. Part 1 will specify safety requirements for the manufacturer, part 2 will describe requirements for designers and integrators and part 3 will define safety requirements for the end-user of industrial mobile robots. Part 1 was scheduled for being published in 2019, followed by part 2 and 3 in 2020 as soon as the committee completed all revision and balloting processes.

In Austria, the national standardisation authority Austrian Standards is reacting to the described trends in modern assistive production systems by setting up a new committee for "Smart Manufacturing" [12]. The group will support the international technical committees ISO/TC 184 - Automation systems and integration [14] and IEC/JWG 21 - Smart Manufacturing Reference Model(s) [15]. A large number of well-known Austrian companies and research centres

have already expressed their interest in participating. The official launch of the smart manufacturing committee is planed in early 2020 [13].

3 Safety Measures Implemented in Industrial Assisitive Systems

Assistive systems have already been successfully installed in numerous modern industrial production sites. This has the consequence, that they can be sufficiently secured by arbitrary technical and/or organisational measures even to get them CE certified. Basis of any safety measure implemented within a collaborative robotic assisitve system is a comprehensive risk analysis which is nevertheless required according to the ISO 10218-2:2011 [3] standard. A risk analysis in general should accompany a project in every phase of life and provide appropriate measures in order to reduce the probability of dangerous situations to an acceptable residual level of risk [25].

In the perspective of technical measures, inherent safety can be achieved by the design of the robot, its manipulation tool, external support equipment, the workpiece or other machine parts that are moved within the collaboration area. Besides that a wide product palette of auxiliary equipment as light barriers, laser scanners, safety matts, etc. offered by different vendors are available to solve almost any safety issue. The goal is to avoid/reduce identified risks occurring at potential contacts between a human and a robot, by an emergency stop triggered by complementary functional safety hardware [25]. The challenge for designers and safety engineers is to find a requirements fulfilling solution at a good balance between efficiency, cost and installation complexity.

If no technical solution is applicable under reasonable effort the according standard ISO 12100:2010 [7] provides organisational measures for risk reduction (see Figure 1). For example these are pictograms and written warning signs on machines, comprehensive training for competence acquisition, working procedures, supervision, the use of personal protective equipment, etc.

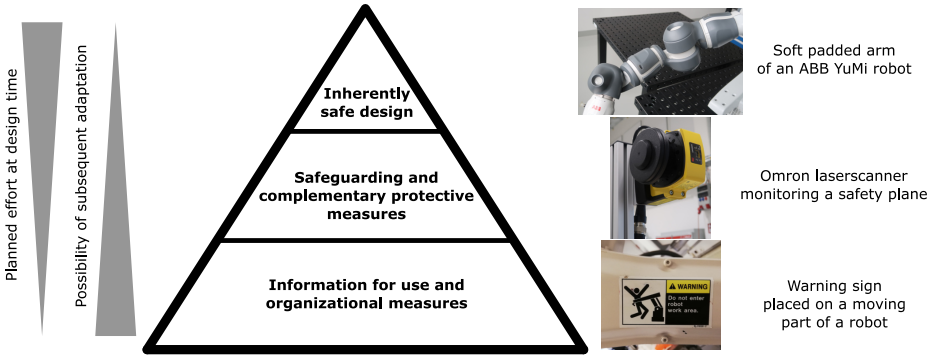


Fig. 1. Measures to reduce risk according to ISO 12100 and a selected example

A particular scenario which is very interesting for risk analysis and the associated measures for reduction is placing a robotic assistive system in a public open space as exhibitions, art projects, makerspaces, etc. Within such an environment systems impose higher risks of unintended human-robot contacts compared to well-studied shop floor applications. Moreover, collaborative assistive robots in public spaces are difficult to validate, as relevant standards and directives (e.g. EC Machinery Directive 2006/42/EC) are not sufficiently applicable. This open space context is investigated in detail in the research project CoMeMak[1]. New approaches for risk assessment and corresponding reduction are developed through novel combinations and structured methodologies of measures.

4 Safety - State of the Art Challenges, best Practices and Future Tends

Companies and users partially perceive the safety awareness in the field of collaborative robotics as exaggerated. This impression is often not misleading, as the safety assessment in the end can be the decisive factor in not being able to put a plant into operation in the desired form. In the following section we try to look at this circumstance one step deeper, to point out the causes and to sketch out solution attempts.

4.1 Possibility of modifications

Every modification of a plant or process has an impact on safety and can affect the operational risk. According to the current state of the art, an automation system must be recertified after any modification. However, this process is time-consuming and always associated with additional costs. Hence, there is a lack of practicable flexibility for collaborative robot systems in case a modification is demanded.

The research project DR.KORS[2] is focused on defining safe modification limits for a known robot application. By the approach developed a user is able to make modifications to the robot system or process and still operate in a well-defined safe system configuration. Numerous essential modification dimensions can be identified for a plant or a physical assistance system, whereby their relevance always depends on the application. Examples for such modification dimensions are the workpiece dimensions, the distance of a safety sensor to the robot base and the robot speed. This means that a generous safety evaluation is accomplished during the design time and statistical and dynamic models are used to evaluate any variation along a modification dimension during runtime. [26]

[1] CoMeMak – Cobot Meets Makerspace is funded by the FFG (grant agreement No 871459)

[2] DR.KORS – Dynamic reconfigurability of collaborative robot systems is funded by the FFG (grant agreement No 864892)

4.2 Applications are slow and bulky

At physically interacting robot assistants where the operation modes separation monitoring or power and force limiting (see Section 2) are used, movements of robot parts and humans might be completely dynamic, uncertain and thus in some cases also unforseeable. As a result, an accurately performed risk analysis prescribes extremely low speed and acceleration values for robot movements. Collaborative applications thus become increasingly inefficient in terms of production cycle times and the resulting effectiveness. Strictly speaking, the challenge is to avoid unforeseeable risky contact situations resulting in requested slow robot movements with the consequence of low production efficiency.

Classically, organisational and technical solutions for (subsequent) securing assistive systems as discussed in Section 3 are applied. Alliteratively, enhanced effort can be shifted to application-analysis processes during the design time. Comprehensive safety-goal oriented optimizations, design reviews, semi-automatic tuning algorithms, etc. may beneficially influence safety behavior even under decreasing production cycle times. Such processes will be generally conducted with a detailed analysis of existing workflows, possible dimensions of flexibility as well as customized guidance though production steps. Therefore illustrative software packages as described in the next Subsection offer great possibilities of production visualization and demonstration of collaborative workflows including humans and machines.

The Horizon2020 project RobMoSys[3] has the goal of an model-driven design methodology for robotic applications as well as assistive systems by using compositions of hard- and software elements with managed, assured and maintained system-level properties. Such properties may range from production characteristics concerning cycle time, human machine interactions and optimized integration of assistive applications into a workflow, to safety properties derived from normative requirements. However, the vision of such model-driven approach is that an application designer has the ability to optimize and adapt a robotic assistive system and the associated workflows at a very early development stage in a way that the safest handling of the robot trends to be the most efficient.

4.3 Complex risk analysis

Risk analysis for the safety of any type of machinery and the general principles for design are basically regulated in the type A standard ISO 12100:2010 [7] and its applicable practical guide ISO/TR 14121:2012 [8]. However, caused by increased dynamic behavior and application flexibility the principles given in the guidance document become harder and harder to follow in a practical way. The effort for assessing and documenting risks in spreadsheets will be significantly increasing. Research projects and the associated developed tools trend to semi-automize risk assessment processes to overcome this challenge.

[3] RobMoSys is an European Horizon2020 project (grant agreement No 732410) - *https://robmosys.eu/*

The research project eITUS[4] [29] develops methodologies for a more intuitive risk assessment based on a model-based system design approach. The core concept is to apply fault injection simulations using high level models specified in the Papyrus for robotics Modeling Framework [27] which is fully compliant with the model-based RobMoSys design methodology (see previous subsection) [28]. Software developed in eITUS configures, executes and analyses simulation results for automatic generation of commonly used risk analysis documents as Hazard and Operability Analysis (HZOP), Failure Modes and Effects Analysis (FEMA) and Fault Tree Analysis. Model-based design of assistive systems in combination with fault injection simulation embedded in a virtual environment poses an applicable approach for risk assessment which is a salable solution even under sequentially increasing system complexity.

Model based design methods are a promising approach to develop modern high performance assistance systems. Abstract models, however, are difficult to handle and potentially unsuitable for domain experts or lead to a lack of clarity in their symbolic/mathematical abstraction. Engineers attempt to make models more illustrate via virtual reality or virtual digital twins. Plant simulation software packages like *Siemens Tecnomatix*[5], *Arena*[6], and *ema Work Designer*[7] represent useful tools. In addition to the mechanical and human process flow, handling tasks of robot systems can be simulated.

For collaborative workplaces, some of these tools can also provide force estimation in critical contact situations. Fig. 2 shows an example of a report result from ema Work Designer. It returns unacceptable contact scenarios if the permissible force limit according to ISO/TS 15066:2016 [4] for a contact is exceeded.

4.4 Safety test and verification processes are not that accurate, reliable and high performance

In agile systems and software development processes, testing as well as verification and validation are significant accompanying activities during the whole design phase. However, testing safety related properties in highly complex systems is becoming more and more challenging and exhaustive testing covering all possible scenarios is not possible. This means, that test cases have to be carefully selected and designed to ensure an appropriate functional safety coverage.

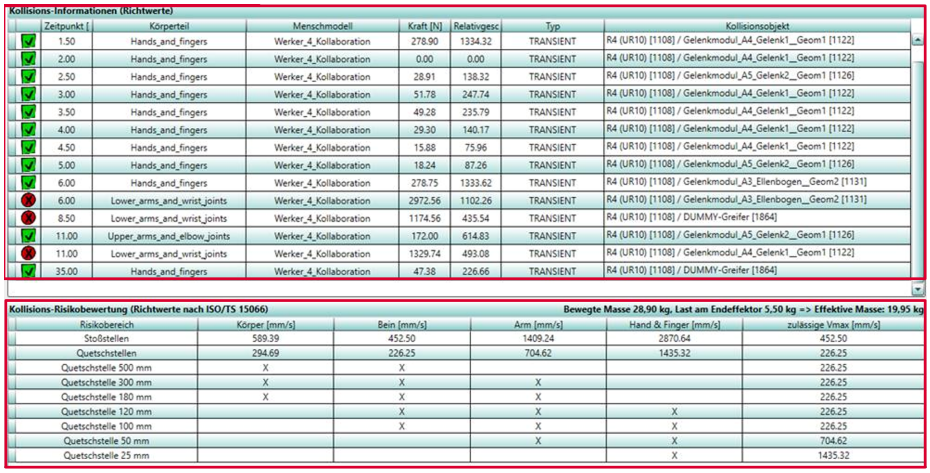
A further critical issue in the perspective of test and verification processes of any modern technical application is the focus of an appropriate level of abstraction the system under test is described, modeled and inspected. A layer model applicable for assistive systems is illustrated in Figure 3. The given layers define a generalized behavioral description implemented as a composition of application dependent as well as commercial hard- and software elements (examples

[4] eITUS – Experimental Infrastructure Towards Ubiquitously Safe Robotics Systems is cascaded funded by European Horizon2020 project RobMoSys (grant agreement No 732410)

[5] *https://www.plm.automation.siemens.com/global/de/products/tecnomatix/*

[6] *https://www.arenasimulation.com/*

[7] *https://imk-ema.com/workdesigner.html*



Kollisions-Informationen (Richtwerte)

	Zeitpunkt [	Körperteil	Menschmodell	Kraft [N]	Relativgesc	Typ	Kollisionsobjekt
✓	1.50	Hands_and_fingers	Werker_4_Kollaboration	278.90	1334.32	TRANSIENT	R4 (UR10) [1108] / Gelenkmodul_A4_Gelenk1__Geom1 [1122]
✓	2.00	Hands_and_fingers	Werker_4_Kollaboration	0.00	0.00	TRANSIENT	R4 (UR10) [1108] / Gelenkmodul_A4_Gelenk1__Geom1 [1122]
✓	2.50	Hands_and_fingers	Werker_4_Kollaboration	28.91	138.32	TRANSIENT	R4 (UR10) [1108] / Gelenkmodul_A5_Gelenk2__Geom1 [1126]
✓	3.00	Hands_and_fingers	Werker_4_Kollaboration	51.78	247.74	TRANSIENT	R4 (UR10) [1108] / Gelenkmodul_A4_Gelenk1__Geom1 [1122]
✓	3.50	Hands_and_fingers	Werker_4_Kollaboration	49.28	235.79	TRANSIENT	R4 (UR10) [1108] / Gelenkmodul_A4_Gelenk1__Geom1 [1122]
✓	4.00	Hands_and_fingers	Werker_4_Kollaboration	29.30	140.17	TRANSIENT	R4 (UR10) [1108] / Gelenkmodul_A4_Gelenk1__Geom1 [1122]
✓	4.50	Hands_and_fingers	Werker_4_Kollaboration	15.88	75.96	TRANSIENT	R4 (UR10) [1108] / Gelenkmodul_A4_Gelenk1__Geom1 [1122]
✓	5.00	Hands_and_fingers	Werker_4_Kollaboration	18.24	87.26	TRANSIENT	R4 (UR10) [1108] / Gelenkmodul_A5_Gelenk2__Geom1 [1126]
✓	6.00	Hands_and_fingers	Werker_4_Kollaboration	278.75	1333.62	TRANSIENT	R4 (UR10) [1108] / Gelenkmodul_A3_Ellenbogen__Geom2 [1131]
✗	6.00	Lower_arms_and_wrist_joints	Werker_4_Kollaboration	2972.56	1102.26	TRANSIENT	R4 (UR10) [1108] / Gelenkmodul_A3_Ellenbogen__Geom2 [1131]
✗	8.50	Lower_arms_and_wrist_joints	Werker_4_Kollaboration	1174.56	435.54	TRANSIENT	R4 (UR10) [1108] / DUMMY-Greifer [1864]
✓	11.00	Upper_arms_and_elbow_joints	Werker_4_Kollaboration	172.00	614.83	TRANSIENT	R4 (UR10) [1108] / Gelenkmodul_A5_Gelenk2__Geom1 [1126]
✗	11.00	Lower_arms_and_wrist_joints	Werker_4_Kollaboration	1329.74	493.08	TRANSIENT	R4 (UR10) [1108] / Gelenkmodul_A4_Gelenk1__Geom1 [1122]
✓	35.00	Hands_and_fingers	Werker_4_Kollaboration	47.38	226.66	TRANSIENT	R4 (UR10) [1108] / DUMMY-Greifer [1864]

Kollisions-Risikobewertung (Richtwerte nach ISO/TS 15066) — Bewegte Masse 28,90 kg, Last am Endeffektor 5,50 kg => Effektive Masse: 19,95 kg

Risikobereich	Körper [mm/s]	Bein [mm/s]	Arm [mm/s]	Hand & Finger [mm/s]	zulässige Vmax [mm/s]
Stoßstellen	589.39	452.50	1409.24	2870.64	452.50
Quetschstellen	294.69	226.25	704.62	1435.32	226.25
Quetschstelle 500 mm	X	X			226.25
Quetschstelle 300 mm	X	X	X		226.25
Quetschstelle 180 mm	X	X	X		226.25
Quetschstelle 120 mm		X	X	X	226.25
Quetschstelle 100 mm		X	X	X	226.25
Quetschstelle 50 mm			X	X	704.62
Quetschstelle 25 mm				X	1435.32

Fig. 2. Exemplary report on the virtual collision evaluation in ema Work Designer.

of a description are given on the right side in the figure). A coarse description at a high level of abstraction hides specific details with the consequence that verification runs fast but may suffer under low expressiveness. Vice versa, a low level of abstraction requires highly detailed, complex and large models which allows very detailed and expressive specification of tests. However, the challenge is to abstract systems in a clever way so that verification and testing is affordable and safety critical situations are detected in an early project phase. This ensures a clear top-down (in reality, meet in the middle) design approach, even with the advantage that errors, bugs as well as safety critical system properties can be detected and corrected cheaply. For verifying the safety property defined in the red box we aim a model of the skill "pick up screws" refined by a more specific refined model of the implemented robot arm in order to estimate contact forces at collisions between human body parts and a part of the robot. Further refinements to individual joint dive models or specific more controller hardware properties in this case would make the model unnecessarily complex and thus the verification slow. However, if a verification engineer is in particular interested in an highly accurate contact force model we recommend using the methodology objective-drive system analysis methodologies as discussed in [11]. Here a specific focus is set on a verification goal when switching to a lower level of abstraction in order to obtain a statement for a system (safety) property that is as precise as requested.

An innovative approach for verification developed in the ForSAMARA[8] project is the utilization of formal methods for safety verification of robotic assistive systems. Such methods, in particular symbolic model checking, result in a mathematical verification proof, while conventional verification approaches are based

[8] ForSAMARA – Formal safety analysis in modular robotic applications is cascaded funded by European Horizon2020 project RobMoSys (grant agreement No 732410)

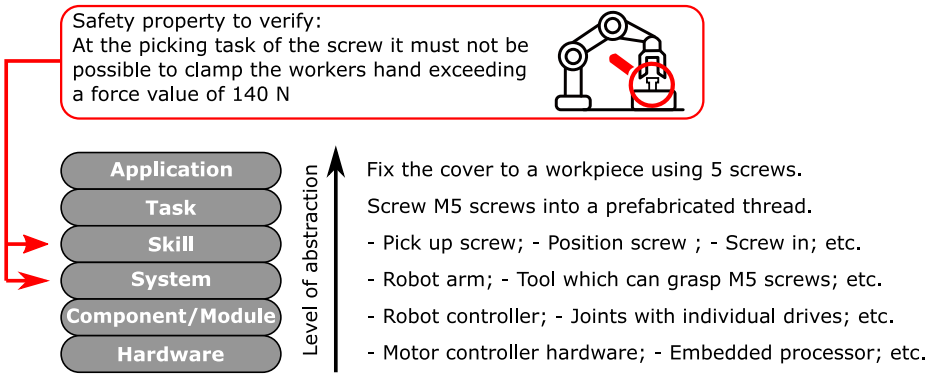


Fig. 3. Levels of abstraction to classify behavioral descriptions, models and verification approaches of an assistive system.

on test scenarios (informal methods) just selectively increase the confidence of the system [19–22]. As illustrated in Figure 4, informal verification runs depend on specifically defined test cases, which target single selected issues. In the figure test cases tc1 to tc3 verify features f4, f6 and f3 which may represent for example specific skill definitions at a certain level of abstraction (see Figure 3). Model checking is able to act more comprehensively by verifying if a formulated property (as the safety property specified in natural language in Figure 3) is fulfilled on a composition of features. However, a natural language specification has to be formalized in a unambiguous machine-readable presentation (e.g. represented as p1 in the Figure). The formalized property p1 it then verified on a composition of system features f4, f5, f7 and f8 using a model checking tool such as NuSMV [16], Spin [17] or UPPAAL [18].

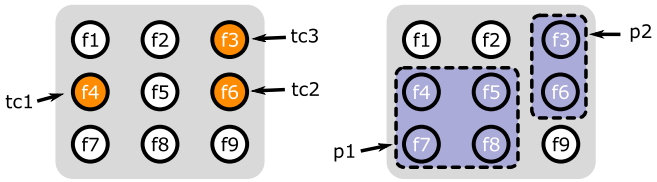


Fig. 4. Comparison between a test-based (left) and model checking-based (right) verification approach.

4.5 Safety verification in highly dynamic, AI and deep learning Robotic Applications

Of course, assistive systems also benefit from forefront technological innovations. They already rely on machine learning (ML), artificial intelligence (AI), and

context-aware (context aware assistive systems - CAAS [30]) components. A major advantage is that these systems react very quickly and flexibly to changes in their environment and application conditions by learning and optimizing new behavioral patterns online during the operation of the system. Thus, testing and verification against safety properties in a classical way before deployment is increasingly challenging. Strictly speaking, it must be proven that safe operation can be guaranteed even under any possible learning evolution of the system [31].

An approach to overcome that challenge might be runtime verification where formally defined properties as explained in the latter subsection are compiled to monitors (hardware or software) executed during the system operation. The creation as well as the integration of monitor structures can be highly automated, offering a well scalable verification methodology. The verification of a safety property can be executed independently of the implemented functional behavior. A property violation is reported and the system can be potentially steered back to a save operation state [32, 33].

4.6 Physical measurement is more tricky than it seems to be

Placing an industrial assistive application using the power and force limitation mode into the market, requires compliance with the force and pressure limits specified by ISO/TS 15066. However, the technical specification defines only the limits that must not be exceeded but holds no information about an associated measurement method. The most important (and only) guideline, implementing a so called biofidel measurement method for the evaluation of human-robot contact situations, has been published by the Deutschen Gesetzlichen Unfallversicherung (DGUV) in 2017. Biofidel in this context means that the affected human body part is imitated by a specific combination of a metal spring and damping material placed on the force sensor element.

Measuring instruments to evaluate the described contact situations are becoming highly affordable and commercial. As a result of this continuing trend, system inegrators and operators of assistive systems will increasingly switch over to buying their own devices and performing measurements. However, many then discover that executing measurements, in particular under high quality assurance measures such as those required for a test laboratory according to ISO 17025, entails significant challenges:

- As already reported the procedure defined by the DGUV have an informational and not a normative character. As long as this DGUV document is under revision for being integrated into the new ISO 10218-2 standard a SOP (standard operating procedure) has to be defined as a basis for the biofidelic measurement process, Nevertheless a clear measurement instruction document is strictly required for being certified by an accreditation body.
- A significant challenge during the design and execution of measurements is to place and configure a measurement device as well as the robot system accurately. This includes among others the selection of a contact situation according a provided risk analysis, localization and biofidel configuration of

the measurement device, ensure repeatable accuracy of robot movements and the associated reproducible measured values, documentation of measurement results as well as a comprehensive description of the robot system for which the performed evaluation is unambiguously valid, etc.

An example is shown in Figure 5 where a Franka Emika Panda robot performs a pick task of a cylindrical workpiece. Both illustrated poses of the robot enables to lower the gripper at the same constant speed to pick up the object. However, the kinematic configuration has a significant impact on the the sensitivity of the robot [10]. Identical movements of the gripper leads in the ellbow-up configuration (left) to a transient contact force of 318 N, whereas the ellbow-down configuration (right) only 133 N have been evaluated. Also humans use this property, rising the ellbow to a horizontal position if we want to press an object powerfully. The limit according to ISO/TS 15066:2016 for such a transient clamping situation of the hand (280 N) is thus fulfilled only at the ellbow-down configuration. As a consequence, on the first side this example shows the possibility of inherent risk reduction by design modifications as described in Section 3. On the other side the tight dependency between the configuration of the robot system and the evaluated biofidel force measurement results are highlighted.

- Having an accredidated calibration certificate for a measurement device and considering the associated uncertainty is good, but only an extremely limited way of considering uncertainty. A significantly higher impact to the total uncertainty budget is given by the integration of the measurement device into the fully specified evaluation process. Several other impact factors as environmental parameters, placement of the device, repeatability of contacts, etc. suddenly become highly relevant. Moreover, their evaluation of measurement uncertainty has to be divided into a static and dynamic load characteristic representing clamping situations and free space contacts respectively.
- Since there is no structured comparison between inspection bodies offering biofidel measurements at the moment, it is hard to validate human skills of a measurement engineer as well as the properties of a specifically used measurement device. The research project *CoHoMe*, which got a cascaded funding award by the EU project *COVR*, focuses on closing this gap. Within the project several evaluation rounds including inter-laboratory comparison experiments at an increasing complexity, are defined. The participants of this study get immediate feedback as well as pass and fail assessment of the executed tests.

This is just a list of the selective challenges that the authors had to overcome during the accreditation process of their inspection facility REL - Robotics Evaluation Lab[9]. Within this test center JOANNEUM RESEARCH offers robot safety evaluation through applied biofidel measurements according to the ISO 17025 quality standard [9].

[9] https://rel.joanneum.at/

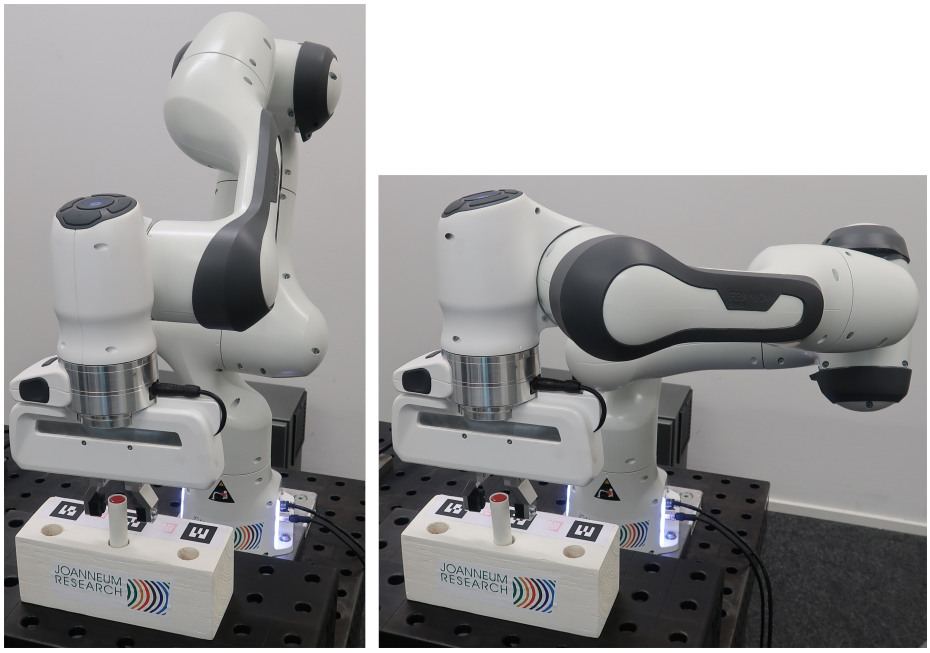


Fig. 5. Due to the redundant geometry of the Panda robot (7 degrees of freedom) the position to pick up the cylindrical workpiece can be reached under various positions of the elbow joint.

5 Conclusion

The working environment and task for an employee should be as appropriate, structured and, above all, safe as possible. Obviously, this also applies to collaborative workplaces where the feeling of overprotection of the employee sometimes arises. An essential reason to be careful with freely acting cobots is based on the forces that occur application-specifically. In particular, the gripping technology used as well as the manipulated workpieces are the greatest uncertainty factor for classifying a priori collaborative robot applications as safe. Quite apart from these obvious influencing factors, some other aspects may have an influence as discussed in this work.

In order to tackle safe operation of modern industrial physical assistive systems, a large number of not directly technical challenges must also be solved. On the one hand, the conformity with current standards and as the highest directive valid laws have to be fulfilled. On the other hand, the aim is to not reduce the effectiveness of production by placing requirements on the operational safety of assistance systems. If these requirements are not met, safety issues can quickly develop into a serious bad cop.

6 Acknowledgements

This work is part of the funded project MMAssist II (Assistance Systems in Production in the Context of Man – Machine Cooperation) supported by the Austrian Research Promotion Agency (FFG) and the Austrian Ministry for Transport, Innovation and Technology (bmvit) under grant agreement number 858623.

References

1. Directive 2006/42/EC of the European Parliament and of the Council of the European Union, 17 May 2006 - Machinery Directive
2. ISO 10218-1:2011 - Robots And Robotic Devices - Safety Requirements For Industrial Robots - Part 1: Robots
3. ISO 10218-2:2011 - Robots And Robotic Devices - Safety Requirements For Industrial Robots - Part 2: Robot systems and integration
4. ISO/TS 15066:2016 - Robots and robotic devices — Collaborative robots
5. ISO/FDIS 3691-4 - Industrial trucks — Safety requirements and verification — Part 4: Driverless industrial trucks and their systems
6. DIN EN 1525:1997-12 - Safety of industrial trucks - Driverless trucks and their systems
7. ISO 12100:2010 - Safety of machinery — General principles for design — Risk assessment and risk reduction
8. ISO/TR 14121-2:2012 - Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods
9. DIN ISO 17025-1:2003-05, General requirements for the competence of testing and calibration laboratories (ISO/IEC 17025:2017)
10. Wahrburg, A., Robertsson, A., Matthias, B., Dai, F., Ding, H.: Improving contact force estimation accuracy by optimal redundancy resolution. In IEEE/RSJ international conference on intelligent robots and systems (IROS), 2016, pp. 3735–3741.
11. Rathmair, M.: Insight in analog systems: a semi-symbolic approach using enhanced deviation traceability. PhD thesis,TU-Wien, Institute for computer Technology, 2018
12. Standards sind entscheidend, damit Industrie 4.0 funktioniert - *https://www.austrian-standards.at/infopedia-themencenter/specials/2-fachkongress-industrie-40/standards-sind-entscheidend-damit-industrie-40-funktioniert/*, [Online; accessed November-2019]
13. Internal Austrian Standards committee document - N0467, 2019-03-08
14. Technical committee ISO/TC 184 - Automation systems and integration, *https://www.iso.org/committee/54110.html*, [Online; accessed November-2019]
15. IEC/TC 65 - Industrial-process measurement, control and automation, *https://tinyurl.com/r3psfg4*, [Online; accessed November-2019]
16. NuSMV: a new symbolic model checker, *http://nusmv.fbk.eu/*, [Online; accessed March-2019].
17. SPIN Verifying Multi-threaded Software with Spin, *http://spinroot.com/spin/whatispin.html*, [Online; accessed March-2019].
18. UPPAAL - an integrated tool environment for modeling, validation and verification of real-time systems, *http://www.uppaal.org/*, [Online; accessed March-2019].
19. Brinkmann R., Kelf D. (2018) Formal Verification—The Industrial Perspective. In: Drechsler R. (eds) Formal System Verification. Springer, Cham

20. Baier C., Katoen and J.P.: Principles of Model Checking. MIT Press, 2008
21. Webster M, et al.: Toward Reliable Autonomous Robotic Assistants Through Formal Verification: A Case Study. In IEEE Transactions on Human-Machine Systems, vol. 46, no. 2, pp. 186-196, April 2016.
22. Rathmair M., Luckeneder C., Kaindl H.: Minimalist Qualitative Models for Model Checking Cyber-Physical Feature Coordination, 2016 23rd Asia-Pacific Software Engineering Conference (APSEC'16), pp. 233-240.
23. Markis A., Papa M., Kaselautzke D., Rathmair M., Sattinger V., and Brandstötter M.: Safety of Mobile Robot Systems in Industrial Applications, 2019 Proceedings of ARW & OAGM Workshop, DOI: 10.3217/978-3-85125-663-5-04
24. RIA - Robotics Industries Association, Industrial mobile robot safety standards on the forefront, *https://www.robotics.org/content-detail.cfm?content_id=6710*, [Online; accessed November-2019].
25. Platbrood F., Görnemann O.: Safe Robotics - Safety in collaborative robot systems, White Paper 2018-06, *https://tinyurl.com/yayepzxt*, [Online; accessed November-2019].
26. Brandstötter M., Komenda T., Ranz F., Wedenig P., Gattringer H., Kaiser L., Breitenhuber B., Schlotzhauer A., Müller A., Hofbaur M.: Versatile Collaborative Robot Applications Through Safety-Rated Modification Limits. In: Berns K., Görges D. (eds) Advances in Service and Industrial Robotics. RAAD 2019. Advances in Intelligent Systems and Computing, vol 980, 2019. Springer, Cham., DOI: 10.1007/978-3-030-19648-6
27. Papyrus for Robotics - *https://www.eclipse.org/papyrus/components/robotics/*, [Online; accessed November-2019].
28. Composable models and software for robotic systems - *https://robmosys.eu/*, [Online; accessed November-2019].
29. Experimental Infrastructure Towards Ubiquitously Safe Robotic Systems using RobMoSys - *https://robmosys.eu/e-itus/*, [Online; accessed November-2019].
30. Korn O., Funk M., Abele S., Hörz T., Schmidt A.. 2014. Context-aware assistive systems at the workplace: analyzing the effects of projection and gamification. In Proceedings of the 7th International Conference on PErvasive Technologies Related to Assistive Environments (PETRA '14). ACM, New York, NY, USA
31. Huang, X., Kwiatkowska, M., Wang, S. and Wu, M., 2017, July. Safety verification of deep neural networks. In International Conference on Computer Aided Verification (pp. 3-29). Springer, Cham.
32. Huang, J., Erdogan, C., Zhang, Y., Moore, B., Luo, Q., Sundaresan, A. and Rosu, G., 2014, September. ROSRV: Runtime verification for robots. In International Conference on Runtime Verification (pp. 247-254). Springer, Cham.
33. Dong, Zhijiang et al., Runtime Verification on Robotics Systems IJRAT 3 (2015): 23-40.