Safety 4.0 for Collaborative Robotics in the Factories of the Future

Luca Caruana
Department of Industrial Manufacturing Engineering
Faculty of Engineering
University of Malta
Malta

Emmanuel Francalanza
Department of Industrial Manufacturing Engineering
Faculty of Engineering
University of Malta
Malta

Technology changes present a constant drive for evolvement in the manufacturing industry. This development has brought about a complete change in the way the industry implements technologies. The complexity of state-of-the-art technologies is on the increase as new and unforeseen perils continue to emerge. One of the main challenges being faced is the adaptation of manufacturing systems to the latest safety and security considerations. The research hypothesis being investigated is that a logically structured procedure incorporating safety and security would be able to assist in designing an ergonomic and collaborative manufacturing system while identifying and analysing risks, eventually establishing feasible solutions for these specific burdens. This paper therefore contributes a methodology which was developed to address issues of safety and security in the design and implementation of cyber-physical production systems in collaborative environments.

Keywords: *Safety, Security, Ergonomics, Industry 4.0, CPPS, Risk Analysis*

1. INTRODUCTION

Industrial control systems (ICS) are traditionally designed to conform with the latest safety and security advances at that time. This implies that the environment in which the standalone system is running would not compromise on the health and safety of the personal operating it. Security was traditionally directed towards off-line protection and limited access of data of each system individually. With the continuous evolvement of digital control, new advances in roboticsas well as networked strategies being introduced in the industrial scene, this ‘traditional’ approach to design for safety has now become obsolete [1].

Advances in robotics have led to the introduction of collaborative environments. Human-Robot Collaboration (HRC) involves the direct contact between the human and the robot sharing the same workspace while also sharing various tasks together. Therefore, collaborative robots represent a natural progression that can solve existing challenges in the manufacturing industry as they help in achieving anincreased productivity while decreasing the production costs. This is made possible by combining the human ability to judge and react with the repeatability and strength of a robot [2,3].

The market demand is endlessly changing triggering shifts within the manufacturing industry. The needs of people strongly dictate the market demand, hence the changes implied should suite these needs. Besides ever-evolving customer demands, another key factor for change is the emergence of new key enabling technologies. These technologies make up what is called the fourth industrial revolution [1].

Industry 4.0 has led to numerous advancements in the manufacturing industries, causing an everchanging competitive scenario. These advances bring about the sharing of both cyber and physical resources between various entities within the same system, or moreover, between a number of systems. This change drives the need for new safety and security approaches which are often neglected and only addressed once systems are designed and technologies are determined. The evolution of manufacturing process technologies as well as safety and security components and procedures should work seamlessly together to progress in parallel, leaving no gaps to be filled at a later stage [1],[4]. This work therefore aims at contributing a methodology which addresses issues of safety and security in the design and implementation of CPPS in collaborative environments.

2. SAFETY & SECURITY APPROACHES IN THE FACTORIES OF THE FUTURE

Protecting collaborative environments against safety and cyber threats is a priority for the thorough implementation of these latest technologies in a system. Traditional means of managing incidents and failures mostly rely on human involvement in industrial practices. These systems do not provide suitable protection in this novel scenario, due to real-time technologies and high availability of most components. Refined devices need be employed to effectively protect the system in a timely manner against any of these threats [5].

2.1 Safety & Security in Cyber-Physical Production Systems (CPPS)

The manufacturing industry is experiencing a huge hype around CPPS and Industry 4.0. These innovative areas lead to investments from different manufacturers to keep up with the latest trends and acquire the state-of-the-art connectivity technologies on the market. However, Sharpe et al. [6] argues that the majority of manufacturers are still far from experiencing the benefits of CPS and that there is a lack of research within this field to

Received: January 2021, Accepted: September 2021
Correspondence to: Dr Emmanuel Francalanza
Department of Industrial Manufacturing Engineering
University of Malta, Malta
E-mail: emmanuel.francalanza@um.edu.mt
doi:10.5937/fme2104842C

adequately demonstrate these improvements. Security is displayed as the main obstacle within this regard and might be the greatest hurdle to overcome in order to start experiencing the aforementioned benefits of this progress in technologies. Further strengthening Sharpe's [6] arguments, Hemilä et al. [7] states that the current challenge revolves around the proposal of novel architectures, methodologies and technologies which optimise the level of efficiency while respecting a decent level of security. Hemilä et al. [7] points out that an increase in cyber-attacks on industrial and manufacturing systems are being reported and this exhibits the problem of cyber threats in these systems, while the repercussions of such attacks can be severe. This imposes the need for operations where cyber risks are managed, but operations are optimised [6-8].

Challenges and cyber security risks are mostly related to humans and IT implementations which exist practically in all aspects of the organization. This is especially relevant to instances where cyber-physical collaboration processes take place. As the complexity in supply chains increases, the amount of information and integration is also increased. Communications between some object (human or machine) requires the exchange and sharing of data, which in turn produces a risk of a cyber-attack. Hemilä et al. [7] indicates that the majority of manufacturing organisations around the world have not yet fully secured themselves from such threats related to cyber security. Schneider et al. [9] points out that the literature existing so far is short of a holistic outline and framework to define the risks existing in the factories of the future [7, 9].

Collaboration processes also bring about safety threats. The proximity of humans working directly with machines in the same workspace makes it susceptible for collisions or injuries in turn. This leads to the development of different safety concepts including inherent safety designs, safety devices and safety strategies. Komenda et al. [10]points out that machines nowadays do not include safety fences but rather incorporate an interface for communication and therefore can be a risk, both in terms of safety as well as security. Komenda et al. [10] remarks that a complete safety design means a constructive design so that there are no pinch points [10,11].

These new technologies and requirements of the factories of the future create a new demand for stan–dardisation, which plays a vital role in refining security, safety and legal aspects. In the past years, a number of standard organizations have published various standards in different areas and topics. Cybersecurity Coordi–nation Group (CSCG), EU Network and Information Security (ENISA), The European Telecommunications Standards Institute (ETSI), International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are some of the most popular standardisation bodies [12].

2.2 Safety & Security challenges in Human-Robot Collaboration

The combination of robots with humans in the manufacturing industry can improve on both efficiency and precision while reducing overall costs. However, the dangers associated with robotics merged with the risks imposed by introducing the human collaboration needs to be addressed to experience a thorough interaction. Moreover, despite the implementation of security measures, accidents still do occur[13].

The majority of accidents experienced are evident and their repercussions are felt immediately. Cases such as the latter are given the most attention, especially since the problems caused are tangible. However, Pogliani et al [14]explains that challenges can vary significantly, and are not limited to these types of accidents. Having a production outcome altered might go unnoticed as micro defects within the production can be introduced by an attacker, yet the consequences of such an attack can be severe. Pogliani et al. [14] explains that defects within products could cause financial loss or tarnish the company's reputation in the long run. Depending on the goods in question, defects could also themselves cause fatalities [14].

Pogliani et al. [14] provides another simple example of a challenge faced with generally any system containing a cyber element, i.e. unauthorised access. Eventhough a manufacturing system contains basic control elements, these control elements include sensitive program codes and machining source codes. These codes can be reverse engineered and reproduced to reveal engineering secrets from one company to another or modified to impose injury on a machine operator. Pogliani et al. [14] makes use of such examples to defend the argument of no tolerance to any type of safety or security threat[14].

Contrarly, Kuts et al. [15] focuses on other aspects and states that the two main challenges in HRC are related to the down time once the safety system is activated, and the human monitoring control within the collaborative environment. Kuts et al. [15] explains that eventhough the collaboration is required, the safety system still differentiates between the robot environment and the collaborative environment, as per the ISO 15066 standard. The fact that a collaborative robot is not separated with a physical fence, as this goes against the purpose of the system, leaves no other choice but to abide to relevant standards which need to be taken into consideration at specific instances. One of the standard procedures is the decreasing of the speed or even stopping the robot once the human interrupts its work environment. This in turn increases the downtime of a collaborative system drastically[15], [16].

2.3 State of the art Safety & Security Standard Approaches

HRC is a relatively novel area for which a number of standards are already set up. Specific HRC standards revolve around the adherence to safety and security protocols without introducing a physical separation. There exist three main categories of standards relevant to robotic systems. Type-A, B and C as can be seen in Figure 1. The ISO 12100 type-A standard defines the basic principles and methodology for achieving safety in the design of the machinery. The principles defined are based on risk assessments and risk reduction together with knowledge and experience of design in this field. ISO 12100 is intended to be used as a preparation of type-B and type-C standards to follow [2,11,14].

Type-B standards are once again generic safety standards that cover the safety aspects or one type of safeguard that can be used with a number of different machineries. There exist two types of type-B standards; B1 standards for specific safety aspects and B2 standards for safeguards. An example of a type-B1 standard is ISO 13849, dealing with the safety requirements for design and integration of safety related control systems. ISO 13850 is a type-B2 standard which deals with the emergency stop function of machinery.

Type-C standards prioritise over type-A and B standards. These standards are safety countermeasures for specific machinery also called product standards, in this case for robotic systems. An example is the ISO 10218 family of standards related to the safety requirements of industrial robots. Upon the introduction of HRC, this standard was updated to address new working scenarios. The updated version of this standard specifies four collaborative operative modes as summarised in Figure 2[2].

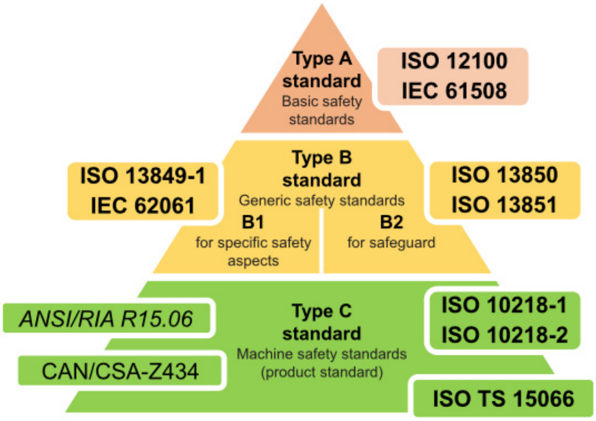


Figure 1. Robotic safety standards categories [2]

Approaches for Safety and Cyber Security

Bicaku et al. [12] proposes a framework for monitoring and mapping of CPPS and IoT in terms of safety and security compliance. There exist several similar approaches and prototypes, however there is no general method which is accepted worldwide. The framework proposed, as Bicaku et al. [12]explains, advances the state of the art by taking safety, security and organisational related legal aspects into consideration without compromising the cyber-physical foundations [12].

The framework consists of four main modules; Monitoring Agents (MA), Evidence Gathering Mechanism (EGM), Compliance and the Target System (TS). The target system is basically the system or component that is monitored. The monitoring agents are used to gather data from the target system. This data is then sent to the EGM, where it is analysed and compared to the related legal evidence, together with the relevant safety and security evidence stored. The EGM decides when and what data to send to the compliance module by utilising a writing buffer. The last module is the compliance module which is responsible in assuring that the system is operating in a secure and standard compliant manner[12].

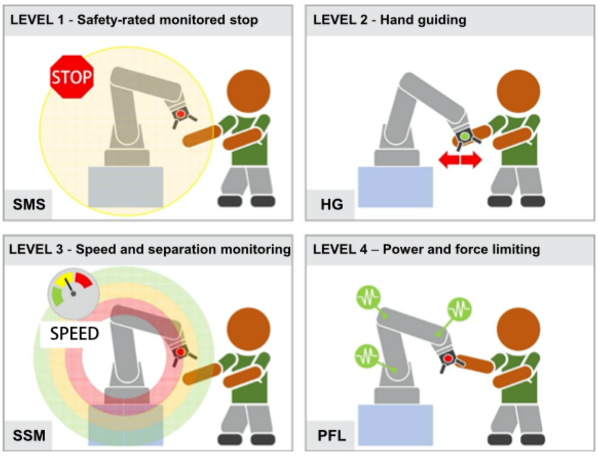

LEVEL 1 - Safety-rated monitored stop
STOP
SMS
LEVEL 2 - Hand guiding
HG
LEVEL 3 - Speed and separation monitoring
SPEED
SSM
LEVEL 4 – Power and force limiting
PFL

Figure 2. Robot collaborative modes (ISO 10218)[2]

Hemilä et al. [7] proposes a framework for cyber security threat management, composed over three organisational dimensions; Technical, Economical and Human. This first of which relates to the human-machine transaction management, for which a digital twin is created. A digital twin brings about a number of advantages apart from real-time tracking of the production line. From the cyber risk management point of view, the management can easily identify the cyber security tools required for detecting and preventing cyber-attacks within the production line. The economical dimension deals with the supply chain and the ecosystem modelling. The previously mentioned digital twin can be easily integrated with the supply chain models, in such way, the whole system can be defined digitally. This enables transaction flow control which is required or the detection, investigations and responses in order to prevent cyber risks in human-machine interactions. The third and last dimension revolves around human-machine interaction modelling.

Optimising this feature enables for cyber risk management of human-machine interaction. Human-machine interaction cyber risk management is used to prevent risks and maintain cyber risk control as much as possible [7].

2.4 Research Gap

When designing a system, collaborative environment designers must make reference to the relevant standards in order to be in conformity with the latest guidelines.

As previously described, there exist a number of standards relevant for robotic systems and HRC, yet these standards cannot exist in a vacuum. There is a need to integrate these standards within a complete methodology relevant for a variety of systems in any phase of implementation. Such integration aids the designer by having a structured approach to follow rather than a list of guidelines without reference. This review has aided in establishing the standard safety and security approaches utilised, together with any procedures and frameworks which may be useful towards this study.

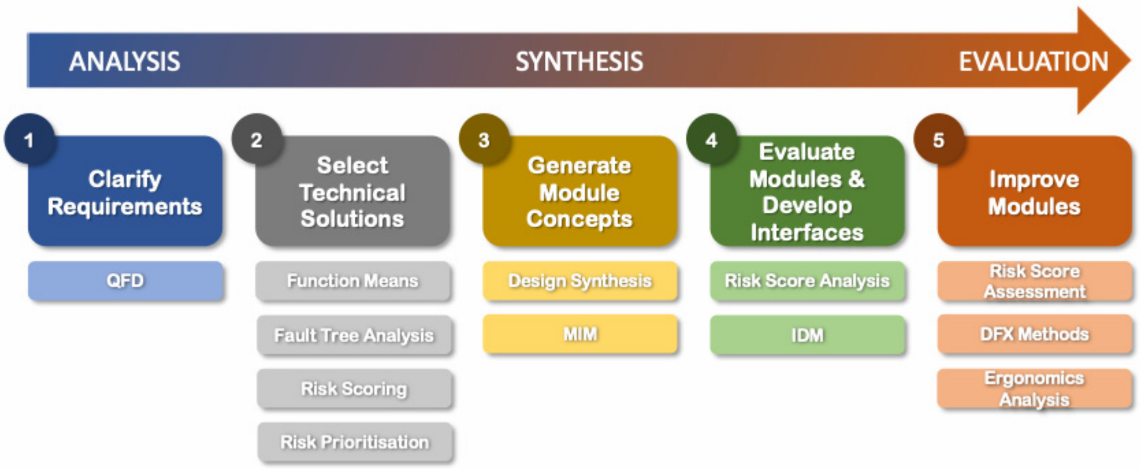


Figure 3. Safety embedded MFD 4.0

Therefore, whilst there exist several frameworks which address either the safety or the security aspects in the design of HRC, yet there is very little effort to adopt a combined safety and security framework as a whole. Tackling safety and security separately, especially when dealing with CPPS and HRC, can be troublesome as the solutions generated for both should be integrated collectively and should also work simultaneously. This research therefore aims to integrate these separate approaches and to structure them in one complete design methodology.

3. SAFETY EMBEDDED MFD 4.0

3.1 Introduction

The methodology developed in this can study, whichcan be seen in Figure 3, has been named Safety Embedded Modular Function Deployment (MFD) 4.0, a portmanteau of Safety 4.0 and Modular Function Deployment 4.0. This method is in fact based upon two previously well-established methodologies. The first, which was developed by Francalanza et al. [17],is used for the design of modular reconfigurable CPPS, and is titled; Modular Function Deployment 4.0 (MFD 4.0). The MFD approach was originally developed by Erixon et al. [18]and intended for the development of modular products. In this case, the MFD is being adapted for the development of modular cyber-physical manufacturing systems, more specifically CPPS in Industry 4.0.

The second methodology integrated within this work is the Safety 4.0 methodology by Caruana and Fran–calanza [19]. This method deals with the implementation of safety and security characteristics of an up and running CPPS. The aim of the Safety 4.0 methodology was to implement safety as part of a brown field project, where the design of the system was already previously determined and the CPPS was already implemented and operational.

The aim of this research is to shift from the upgrading of a brown field system to a green field project. This offers numerous opportunities to set up a system with integrated safety and security while dealing with the design aspects conjunctly. To do so affectively, the conjunction of the Safety 4.0 methodology with the MFD 4.0 is essential in order to concurrently implement both the safety and modular design aspects.

3.2 Safety embedded MFD 4.0

As can be seen in Figure 3, the Safety embedded MFD 4.0 approach comprises of five steps. Within each step various tools (such as Quality Function Deployment (QFD) and the Modular Indication Matrix (MIM)) are utilised. These tools help to achieve the ultimate goal, that of developing a CPPS system with modular principles and embedded safety.

Apart from the tools dealing with the general development of modules, the Safety embedded MFD 4.0 makes use of additional tools such as Hazard and Risk Assessments, Morphological Charts and Risk Score Analysis. These tools deal with the safety aspects within this same approach while the general tools utilised in the MFD 4.0 are still in place. This is done to exploit the benefits of both the MFD 4.0 and the Safety 4.0 methodology when developing a new system.

It is important to note that, as pointed out by Erixon et al. [18], although the steps of the MFD are produced in a certain sequential order, these never follow suit in a linear fashion, from the first to the final step. The starting point might vary, together with the need for iterations in some steps, before achieving the final result [18].

Step 1: Clarify Requirements

The first step of this approach, as with every design method, is the clarification of requirements. This starts off with the identification and analyses of the problem at hand, which aids in the clarification of what is required to address that problem. By utilising this method for the design of a CPPS, the typical physical system requirements and the specific CPPS requirements are combined. The requirements must be defined in enough detail in order to attain an in-depth specification of the system to be developed. Based on the systems, the key enabling technologies involved, and the level of collaboration, one has to also determine the safety requirements. To derive such requirements, a QFD exercise has proven to be a suitable tool while ensuring that enough information is derived for this task [18].

Step 2: Select Technical Solutions

This step focuses on the translation of the specifications into feasible technical solutions. This is achieved by identifying the different functional elements of the system required to achieve a modular architecture, while in turn defining how these functional elements can be implemented. The requirements identified previously in the QFD are decomposed into functions and sub-func–tions, using tools such as the function-means tree. Brea–king down the system into basic functions together with their respective technical solution does not only make it clearer which technical solutions satisfy each function but also aids in the ultimate goal of the approach, that of attaining a comprehensive modular design.

The Safety embedded MFD 4.0 requires that safety and security play a vital role throughout all the steps, hence this should be evident in the function means tree. A dedicated branch for both safety and security within the function-means is essential in order to evaluate thoroughly the solutions required to achieve both safety and security through specialised modules.

Choley et al. [20] states that when dealing with safety and security risks, a means of hazard analysis is required. A Failure Mode and Effects Analysis (FMEA) or a Fault Tree Analysis (FTA) are two suitable tools to formulate a comprehensive hazard analysis. Friedberg et al. [21] also suggests that a qualitative analysis tool such as the Hazard and Operability Analysis (HAZOP) could be sufficient to analyse the hazards in a system. On the other hand Friedberg [21] notes that a problem exists when using HAZOP. Friedberg [21] argues that it is difficult to achieve quantifiable results and all the efforts to quantify the qualitative results of this exercise have led back to the use of an FTA. In light of Friedberg's [21] argument and to avoid overlap with other analyses tools, the FTA was chosen to be used within this methodology.

Once the hazards are identified, it is essential to score each of the hazards to quantify their risk. The risk scoring exercise is a simple yet crucial step in a hazard and risk analysis which quantifies the probability and severity of a certain hazard happening. Poot et al. [22] suggests that this quantification is done in line with predetermined standard classifications, hence the values of each risk are relative to each other. Following the risk quantification, these risks are prioritised using tools such as the Pareto Analysis. This step aids in determining where the main focus and work is required within the system being dealt with.

Step 3: Generate Module Concepts

The third step involves the translation of all the sub-functions identified in the previous step into technical solutions, in order to create modules for the system. To start off, a design synthesis addressed specifically for safety and security takes place where a number of solutions to satisfy the safety requirements imposed earlier are generated. Design Synthesis is a brainstorming step which makes use of a morphological chart to generate as many solutions as possible based on the Risk Prioritisation conducted. Babar et al. [23] highlights the importance of generating solutions according to the risk level attained, while in this case, keeping in mind that the solutions need to work as a module together within the system.

Once a number of safety solution ideas are generated, the MIM can take place. The MIM is a QFD like approach used to quantitively evaluate the relationship of each technical solution and module driver of both the general and safety design solutions. By using the MIM, the functional elements are portrayed and these can be grouped together in one single module as much as possible. Additionally, a scoring exercise is carried out according to the relevance of each relationship towards the ultimate goal, that of achieving modularity [18].

Step 4: Evaluate Modules and Develop Interfaces

This step analyses the previous concepts generated and further develops them. In terms of safety design, the risk scores need to be re-evaluated to make sure that the safety module concept developed previously is adequate and reduces the original risk score to the satisfactory level. This step can be considered as an additional step yet is required before conducting the general approach, which shall be discussed next. The main reason for this additional step is to make sure that the safety related module is up to standard and is scrutinised more than once to avoid any missing details which could lead to catastrophe.

When dealing with the design aspect of modularity, this depends on the quality of each module interface, therefore each module is evaluated before the interfaces are developed. The design of interfaces is based on the Interface Design Methodology (IDM) as authored by Scalice et al. [24] and can be seen in Figure 4.

Step 5: Improve Modules

The final step deals with improvements to the newly designed system in order to meet the requirements imposed at the beginning. To start off, the safety related modules need to hold a risk score below the pre-determined threshold value. If this value is not satisfied, the safety module undergoes the same procedure described in the previous steps until the value reaches a satisfactory level.

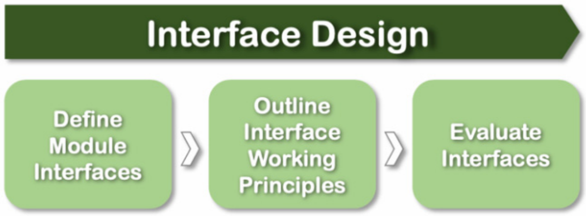


Figure 4. Interface Design Methodology (IDM) [24]

The rest of the modules can still be improved on the part level, where each module is developed to its necessities. Were needed, each module is optimised using Design for 'X' (DFX) methods, for which the priorities can be obtained from the MIM conducted in Step 4. Therefore, the aspects of importance of each module are easily defined using the MIM, while the DFX can be utilised to improve on these characteristics when possible. Special attention is given to the physical safety of the operators, hence ergonomics analysis based on the detailed design of the system is essential to make sure that the human is not subject to access fatigue while working on the system [17].

4. METHOD IMPLEMENTATION AND EVALUATION

To evaluate the Safety Embedded MFD4.0 methodology it was decided to apply the approach to a case-study. This method of evaluation allows for the implementation of the methodology and to assess its effectiveness in deriving a safe and secure CPPS. The case-study was centred on the assembly and customisa–tion of the sample product which is illustrated in Figure 5. This product is a picture frame made up of a number of components. The CPPS to produce this pro–duct is to be composed of two stations. The first station is a collaborative station where a human and robot will work together to assemble the product. The second station is an automated fabrication station which will eng–rave a customised text message on the top of the frame.

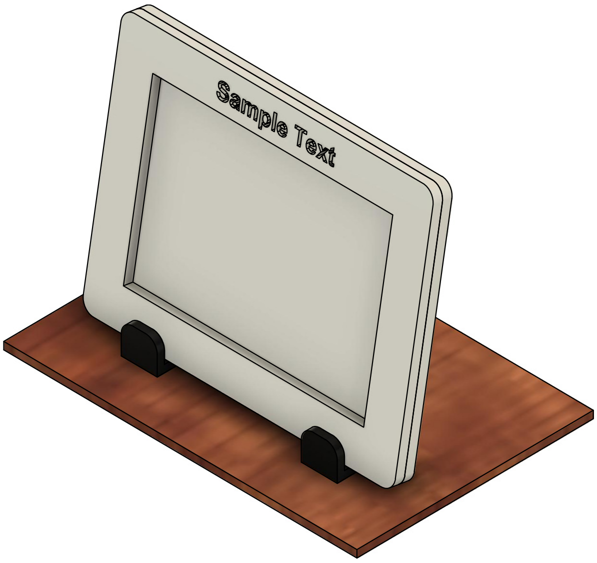


Figure 5. Objective of the Case Study

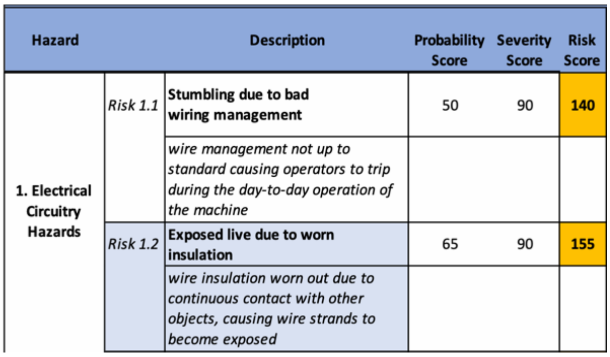
Step 1: Clarify Requirements

The first step of the methodology involves the clari–fication of requirements. For this step a QFD was utilised in order to determine the relationships between the system requirements, and the design parameters. As is illustrated in Figure 8 the design parameters show both the cyber and physical aspects of the system. It is important to note that at this stage important relationships are highlighted between system requirements such as connectivity and for example security. If a connection to the internet is required this exposes the system to greater security threats, and the possibility of increased safety risks.

Step 2: Select Technical Solutions

The selection of technical solutions is a key step in this methodology, and plays a critical role with respect to safety and security. This begins with the selection of possible technical solutions which map to the design parameters and system requirements previously established. In order to carry out this task a FMA tree was utilised. Whilst separate FMAs were utilised for both the cyber and physical systems, an excerpt of which is being shown in Figure 9,dedicated safety and security branches were developed for both aspects.

Furthermore, in parallel with FMA a Fault Tree Analysis (Figure 10) was carried out in order to identify the possible hazards in the system. The means being identified in the FMA were therefore analysed to relate any possible security and safety hazards. Once these hazards have been identified with respect to the cyber and physical functions of the system, these were scored with respect to their probability and severity. This results in the respective risk score for each potential hazard. All the hazards were then ranked according to their respective risk score and using a Pareto analysis the top-ranking hazards were identified. In the following steps these were tackled using specific solutions accordingly. An excerpt of the risk scoring is shown in Figure 6.



Hazard		Description	Probability Score	Severity Score	Risk Score
1. Electrical Circuitry Hazards	*Risk 1.1*	**Stumbling due to bad wiring management**	50	90	**140**
		wire management not up to standard causing operators to trip during the day-to-day operation of the machine			
	Risk 1.2	**Exposed live due to worn insulation**	65	90	**155**
		wire insulation worn out due to continuous contact with other objects, causing wire strands to become exposed			

Figure 6. Risk Scoring

Step 3: Generate Module Concepts

Once all the technical, safety and security solutions have been identified, the next step of the methodology is to generate the module concepts. These modules merge together a number of solutions depending on their interrelationships with a set of module drivers. This exercise is carried out using the MIM [25].The aim is to develop a set of modular and reusable solutions which can then be interfaced with each other to generate the overall collaborative CPPS. Therefore, as shown in Figure 11, solution elements such as the Light Curtains, Interlocks, E-Stop and Electrical Components can be grouped into a module which can be re-used for both the assembly as well as the fabrication stations.

Step 4: Evaluate Modules and Develop Interfaces

Once all the modules have been identified, and based on the Interface Design Methodology (IDM),the approp–riate interfaces between them had to be developed. For the physical modules these included physical interfaces such as attachment brackets, and for the cyber modules these included the industrial communication protocols to be utilised.

Following this exercise all the modules and interfaces were once again evaluated with respect to their risk-score to ensure that the recommended solutions were adequately implemented. An example of which is given in Figure 12.

STEP 5: IMPROVE MODULES

The final step of the methodology is the detailed design of the solution and improvement of the modules. A CAD model of the system was developed based on the modular structure developed. Detailed design was carried out, including the detailed design of the physical interfaces. Furthermore, in order to further improve the modules from a physical safety perspective, an ergonomic analysis was carried out using Dassault 3D Experience. As illustrated in Figure 7 this allowed for the detailed design and improvement of the modules to ensure that the human would not be subject to fatigue.

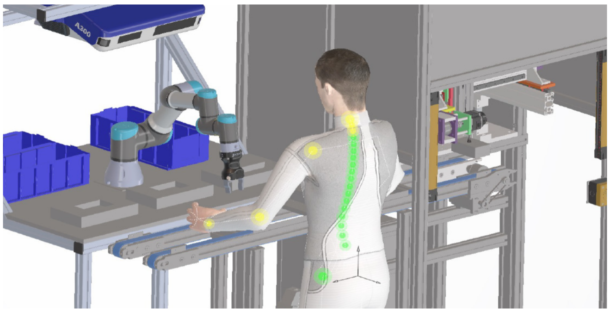
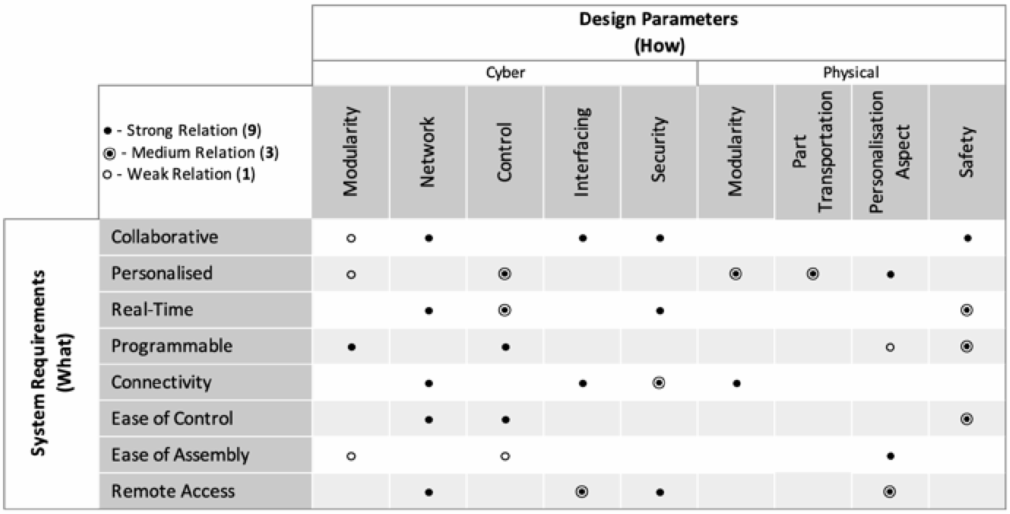


Figure 7. Ergonomics Analysis



● - Strong Relation (9)
◉ - Medium Relation (3)
○ - Weak Relation (1)

		Design Parameters (How)								
		Cyber					Physical			
		Modularity	Network	Control	Interfacing	Security	Modularity	Part Transportation	Personalisation Aspect	Safety
System Requirements (What)	Collaborative	○	●		●	●				●
	Personalised	○		◉			◉	◉	●	
	Real-Time		●	◉		●				◉
	Programmable	●		●					○	◉
	Connectivity		●		●	◉	●			
	Ease of Control		●	●						◉
	Ease of Assembly	○		○					●	
	Remote Access		●		◉	●			◉	

Figure 8. Quality Function Deployment (QFD)

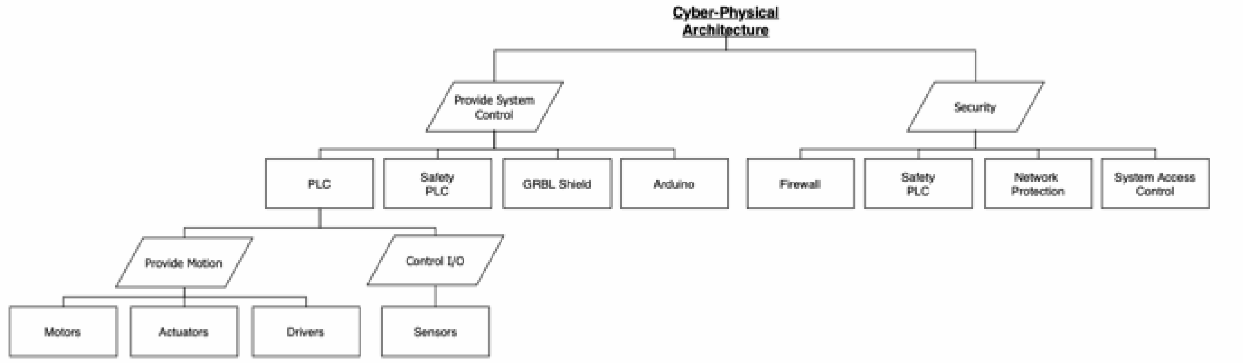


Figure 9. Function Means Analysis (Cyber Physical)

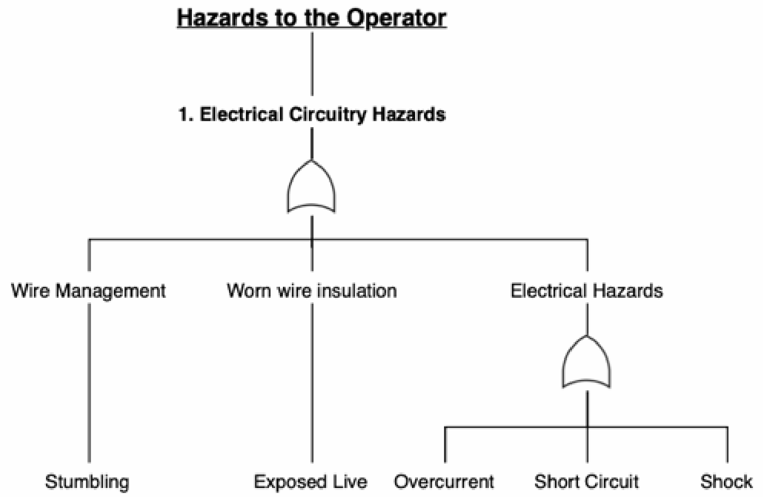
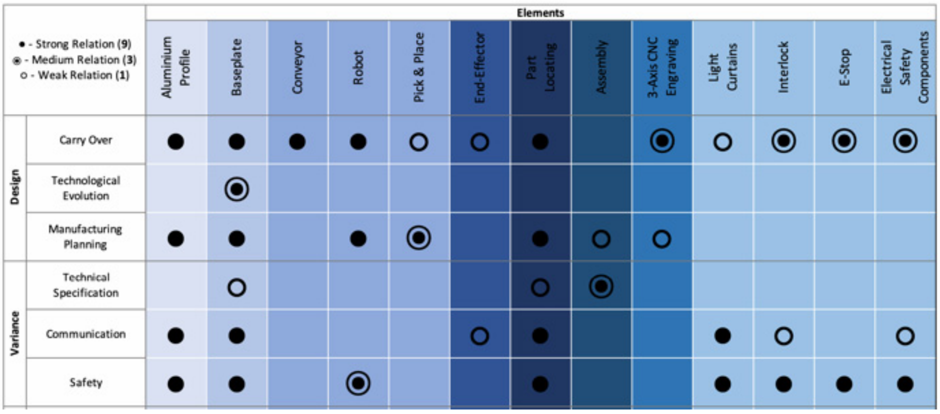
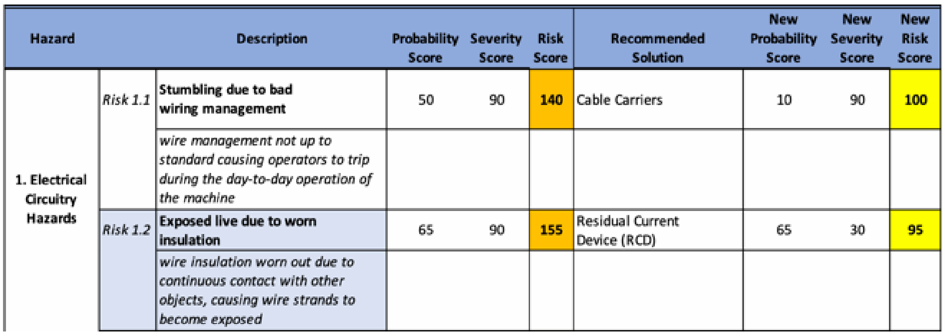


Figure 10. Fault Tree Analysis



● - Strong Relation (9) ◉ - Medium Relation (3) ○ - Weak Relation (1)		Elements												
		Aluminium Profile	Baseplate	Conveyor	Robot	Pick & Place	End-Effector	Part Locating	Assembly	3-Axis CNC Engraving	Light Curtains	Interlock	E-Stop	Electrical Safety Components
Design	Carry Over	●	●	●	●	○	○	●		◉	○	◉	◉	◉
	Technological Evolution		◉											
	Manufacturing Planning	●	●		●	◉		●	○	○				
Variance	Technical Specification		○					○	◉					
	Communication	●	●				○	●			●	○		○
	Safety	●	●		◉			●			●	●	●	●

Figure 11. Modular Indication Matrix



Hazard		Description	Probability Score	Severity Score	Risk Score	Recommended Solution	New Probability Score	New Severity Score	New Risk Score
1. Electrical Circuitry Hazards	*Risk 1.1*	**Stumbling due to bad wiring management**	50	90	140	Cable Carriers	10	90	100
		wire management not up to standard causing operators to trip during the day-to-day operation of the machine							
	Risk 1.2	**Exposed live due to worn insulation**	65	90	155	Residual Current Device (RCD)	65	30	95
		wire insulation worn out due to continuous contact with other objects, causing wire strands to become exposed							

Figure 12. Updated Risk Scoring

5. CONCLUSIONS & FUTURE WORK

The rapid development towards CPPSs which integrate within them collaborative workspace necessitates the implementation of safety and security procedures. Based on a detailed review of existing literature there is no methodology which integrates these aspects within a CPPS design methodology. This research has therefore contributed a methodology for safety and security embedded modular design of CPPS.

When compared to existing methods and app–roaches in the state of the art this work contributes a methodology which jointly considers the safety and security implications on cyber and physical aspects. This may have implications on safety aspects on elements, such as coots, which combine both the cyber and physical aspects concurrently.

Future work will therefore look at how possible solutions may simultaneously affect both cyber as well physical aspects. Furthermore, the system designed during this research will be implemented within a laboratory condition such as to further evaluate the safety and security capabilities of the CPPS.

ACKNOWLEDGEMENT

The main author would like to acknowledge the funding received through the ENDEAVOUR Scholarships Scheme to carry out the research reported in this paper.

REFERENCES

[1] P. Gupta, M. Asjad, Reconfigurable Manufacturing System (RMS): Accelerate Towards Industries 4.0, SSRN Electron. J., Jan. 2019.

[2] V. Villani, F. Pini, F. Leali, and C. Secchi, Survey on human–robot collaboration in industrial settings: Safety, intuitive interfaces and applications, Mechatronics, vol. 55, pp. 248–266, Nov. 2018.

[3] E. Matheson, R. Minto, E. G. Zampieri, M. Faccio, and G. Rosati, Human–Robot Collaboration in Manufacturing Applications: A Review, Robotics, vol. 8, no. 4, p. 100, 2019.

[4] P. Pinheiro, G. D. Putnik, A. Castro, H. Castro, B. F. R. Dal, and F. Romero, Industry 4.0 and industrial revolutions: An assessment based on complexity,FME Trans., vol. 47, no. 4, pp. 831–840, 2019.

[5] G. Settanni, F. Skopik, A. Karaj, M. Wurzenberger, and R. Fiedler, Protecting cyber physical production systems using anomaly detection to enable self-adaptation, in 2018 IEEE Industrial Cyber-Physical Systems (ICPS), May 2018, pp. 173–180.

[6] R. Sharpe, K. van Lopik, A. Neal, P. Goodall, P. P. Conway, and A. A. West, An industrial evaluation of an Industry 4.0 reference architecture demon–strating the need for the inclusion of security and human components, Comput. Ind., vol. 108, pp. 37–44, Jun. 2019.

[7] J. Hemilä, M. Mikkola, and J. Salonen, Mana–gement of Cyber Security Threats in the Factories of the Future Supply Chains, 2019.

[8] G. Putnik, L. Ferreira, N. Lopes, and Z. Putnik, What is a Cyber-Physical System: Definitions and models spectrum, FME Trans., vol. 47, pp. 663–674, Jan. 2019.

[9] P. Schneider, Managerial challenges of Industry 4.0: an empirically backed research agenda for a nascent field’, Rev. Manag. Sci., vol. 12, no. 3, pp. 803–848, Jul. 2018.

[10] T. Komenda, G. Reisinger, and and Wilfried Sihn, A Practical Approach of Teaching Digitalization and Safety Strategies in Cyber-Physical Production Systems, Res. Exp. Educ. 9th Conf. Learn. Factories 2019 CLF 2019 Braunschw. Ger., vol. 31, pp. 296–301, Jan. 2019.

[11] J. Huang et al., A strategy for human-robot colla–boration in taking products apart for remanufacture, Fme Trans., vol. 47, no. 4, pp. 731–738, 2019.

[12] A. Bicaku, M. Tauber, J. Delsing, C. Schmittner, Monitoring Industry 4.0 Applications for Security and Safety Standard Compliance. 2018.

[13] P. Long, C. Christine, D. Chablat, and A. Girin, An industrial security system for human-robot coexistence, Ind. Robot Int. J., vol. 45, Dec. 2017.

[14] M. Pogliani, D. Quarta, M. Polino, M. Vittone, F. Maggi, and S. Zanero, Security of controlled manufacturing systems in the connected factory: the case of industrial robots, J. Comput. Virol. Hacking Tech., vol. 15, no. 3, pp. 161–175, Sep. 2019.

[15] V. Kuts, M. Šarkans, T. Otto, and T. Tahemaa, Collaborative Work Between Human And Indus–trial Robot In Manufacturing By Advanced Safety Monitoring System, 2017, pp. 0996–1001.

[16] D. Antonelli and G. Bruno, Dynamic distribution of assembly tasks in a collaborative workcell of humans and robots, FME Trans., vol. 47, pp. 723–730, 2019.

[17] E. Francalanza, M. Mercieca, and A. Fenech, Modular System Design Approach for Cyber Physical Production Systems, Procedia CIRP, vol. 72, pp. 486–491, Jan. 2018.

[18] G. Erixon and T. högskolan, Modular Function Deployment: A Method for Product Modula–risation. Royal Inst. of Technology, Department of Manufacturing Systems, Assembly Systems Division, 1998.

[19] L. Caruana, E. Francalanza, Design for Safety and Security in Cyber Physical Production Systems, presented at the 2100 Projects Association, Dec. 2020.

[20] [20] J.-Y. Choley, F. Mhenni, N. Nguyen, and A. Baklouti, Topology-based Safety Analysis for Safety Critical CPS, Procedia Comput. Sci., vol. 95, pp. 32–39, Dec. 2016.

[21] [21] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, STPA-SafeSec: Safety and security analysis for cyber-physical systems, J. Inf. Secur. Appl., vol. 34, pp. 183–196, Jun. 2017.

[22] [22] L. Poot, K. Johansen, and V. Gopinath, Supporting risk assessment of human-robot collaborative production layouts: a proposed design automation framework, Procedia Manuf., vol. 25, pp. 543–548, Jan. 2018.

[23] [23] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad,Proposed Embedded Security Framework for Internet of Things (IoT). 2011..

[24] [24] R. Scalice, L. Andrade, and F. Forcellini, A Design Methodology for Module Interfaces', 2008, pp. 297–304..

[25] [25] G. Erixon, Design for Modularity, in Design for X: Concurrent engineering imperatives, G. Q. Huang, Ed. Dordrecht: Springer Netherlands, 1996, pp. 356–379.

СИГУРНОСТ 4.0 ЗА КОЛАБОРАТИВНУ РОБОТИКУ У ФАБРИКАМА БУДУЋНОСТИ

Л. Каруана, Е. Франкаланза

Технолошке промене представљају стални покретач за развој у прерађивачкој индустрији. Овај развој довео је до потпуне промене у начину на који индустрија примењује технологије. Комплексност најсавременијих технологија расте како се нове и непредвиђене опасности и даље појављују. Један од главних изазова са којима се суочава је прилагођавање производних система најновијим питањима безбедности и заштите. Хипотеза истраживања која се испитује је да би логички структурирана процедура која укључује сигурност и заштиту била у могућности да помогне у пројек–товању ергономског и колаборативног производног система кроз идентификацију и анализу ризика, на крају успостављајући изводљива решења за ова спе–цифичне отежавајуће факторе. Овај рад стога доп–риноси методологију која је развијена за решавање питања безбедности и заштите при пројектовању и имплементацији сајбер-физичких производних сис–тема у колаборативним окружењима.