DOI: 10.2507/29th.daaam.proceedings.022

INTEGRATED METHOD FOR THE DESIGN AND EVALUATION OF SAFETY & SECURE MANUFACTURING SYSTEMS

Kemajl Stuja, Günther Poszvek, Walter Wölfel & Erich Markl

This Publication has to be referred as: Stuja, K[emajl]; Poszvek, G[unther]; Wolfel, W[alter] & Markl, E[rich] (2018). Integrated Method for the Design and Evaluation of Safety & Secure Manufacturing Systems, Proceedings of the 29th DAAAM International Symposium, pp.0157-0163, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-20-4, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/29th.daaam.proceedings.022

Abstract

Modern manufacturing systems are increasingly characterized by using of complex machines, tools and electronics components. Especially a proportion of electronics and software has increased steadily in recent years. Challenge of this progression is the complexity of manufacturing systems during designing, integrating and operating. Based on a product lifecycle -PL- this article introduces an integrated method for system design, which supports engineering and management of safety/security for digital manufacturing systems. This method was practically established during a planning and implementation of digital manufacturing system at the university of applied sciences "Technikum Wien". The outcomes of this method – integrated safety and security (ISS) - ought to help the factory designers, integrators and users for (re)designing, operating and maintaining of machines, robots as far work-cells. The future work is to build simple software tool to support small and medium-sized enterprises (SMEs) for decision making during evaluation of risk assessment and management.

Keywords: functional safety; industrial security; production systems; product lifecycle management

1. Introduction

The great idea "Internet of Things (IoT)" for real time connection of system components to the worldwide network enables not only advanced manufacturing features of production system but completely new business models too. New entrepreneurial concepts enables to open market much better competitiveness for medium-sized or small-scale production facilities. On the other hand, this worldwide connection of production system turns themselves into complex system structure and highlights the problem of information security. Therefore industry sets very high and new requirements for the machines and production systems [1] as follows:

1. to be able to produce customized, complex but cost-effectively products in small batches,
2. to be (re)designed or adapted in ever shorter planning times and
3. to interact autonomously and self-organizing.

To fulfil the first requirement, the smart production system must have among other hard-/software compatible interfaces, capable for the connectivity with other manufacturing segments. The new domain will be articulated through design of cyber-physical systems. This terminology is (in Europe) often associated with Industry 4.0, where the physical representation is enhanced, by using of a virtual technology to ultimately simulate and plan the products in altered batches. In order to fulfil the second requirement, computer aided methodical approaches, are mandatory. This part is the subject of this work and will be shortly explained above. The last requirement would be reached by establishing a secure communication between the components of the systems. For decision making an artificial intelligence must be established.

While for the company owner, the technological progress and rentability of production systems are important foundations, for policy maker is the safety of employees very important. Furthermore, the information security has a rocky relationship with safety machinery [2]. A quantitative relationship between these two important issues was shown in [3]. In Figure 1 you can see the integral method for the risk analysis. This method explains the integrated method for machine safety and security for one concept solution. That means usability of a given method limits only for the machines (closed systems) - and for system- integrators and -users, but not for system-designer, who among other must to take a decision by choosing/evaluating the best suitable solution from a possible concept.

This work extends and elaborates “building blocks” as conceived in [3] for the lifecycle phases of (machines/ manufacturing) system. This uses the classic method of system design and adds the newly safety and security requirements as an integral part of system design.

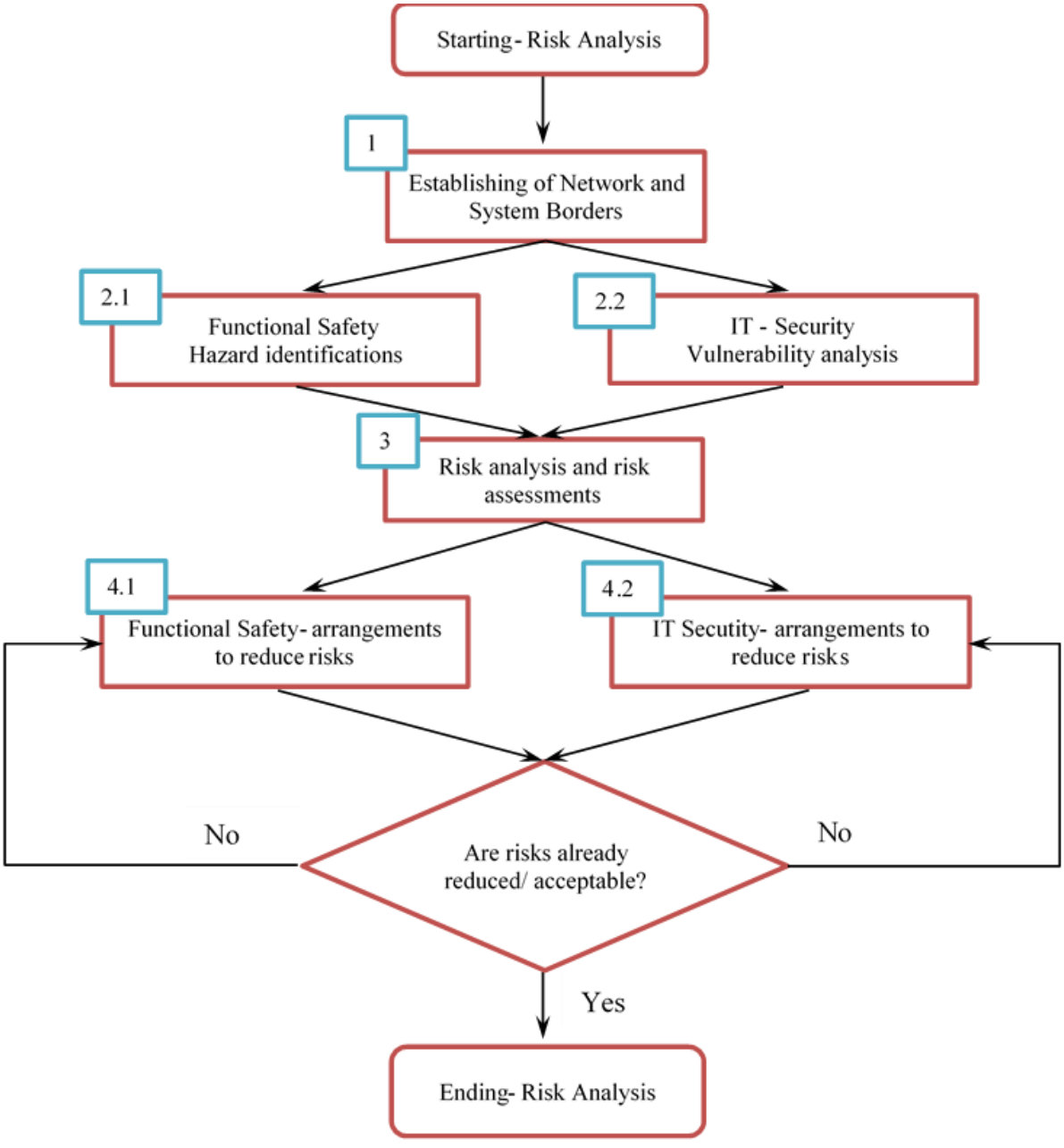

Fig. 1. Workflow of integrated safety and security [3]

2. Problem Statements

In order to use/operate/sold a machinery on the European Union, the requirements of European Machinery Directive must to be fulfilled. The machines and systems in the European Union, who already fulfils this requirement are certified and signed with 'CE' letters. Among others the letters 'CE' signify two safety aspects: that products meets high safety and health protection requirements for employees and for environment.

Technically means that the manufacturer of products (machines or workcells) have to ensure that a risk assessment and all technical documents are available for the system integrators or system operators. While for the design of the machine exists legal standards, for robot cells ore manufacturing cells/systems, due to large variety of manufacturing processes, there are either explicitly standardized solution nor principally design method.

A robotic workcell is a technical system that includes the stationary industrial robot(s), controller(s) and peripherals (such as a moving track, part positioner etc.) and safety components (reported at [4] and [5]). The classical method for design of the technical system stabled by the academia is shown in the Figure 2. There are four relevant phases of design using this method:

1. Clarifying "Design Requirements" sometimes termed as problem definition, is one of the most central element in the design process. When clarifying the task, the first step in the problem definition is given by specifying the product and creating the requirement list. The design requirements control the design of the product being developed, during the engineering design phases.
2. A conceptualization is a phase of product lifecycle that includes generating ideas about product being developed. These include basic elements of system definition like the function-items, relationships, and attributes determined after assessing user needs.
3. Preliminary design includes often bridges a gap between concept and detailed design, in cases where the level of concept attained during conceptualization is not sufficient for full assessment.
4. Detailed design is the lifecycle phase, which elaborates each aspect of the product by complete description through solid modelling, drawings, handbooks as well as specifications.

As shown in the Figure 2 the safety and security aspect is often neglected during the evaluation of concepts. Usually only the best chosen concept, which technically and economically criteria fulfils, will be taken into account by adding of safety/security components. Furthermore the safety/security is treated there as a technical feature. This problem will be solved by extending the safety and security evaluation for all candidate-concepts. This work explain the important of this way of thinking.

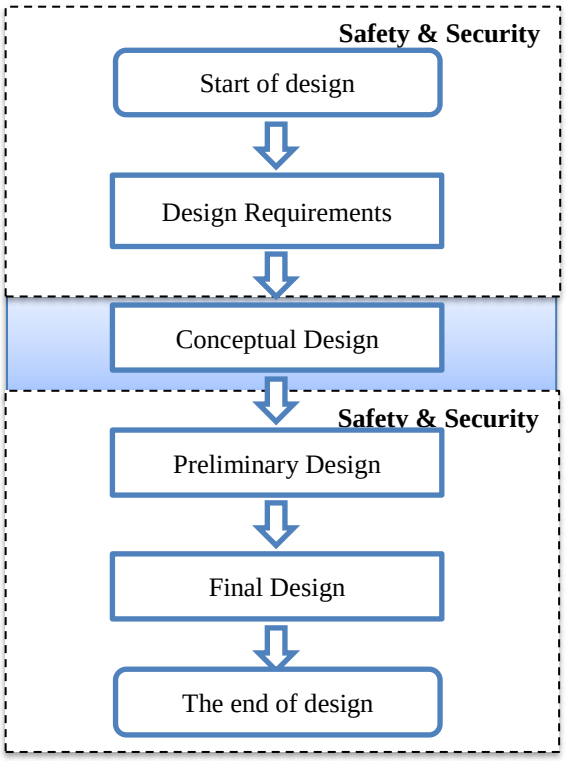

Fig. 2. Classical design workflow diagram

3. Solution and method

In Figure 1 and 2 are shown the "integrated safety and security workflow" which is mandatory for product approval and the "classical design workflow diagram" essential method for product design. This paper shows the integration (parallel executions) of this two product life cycle phases, extend the usability to all candidate-concepts and list the advantages of used methodology by system design.

3.1. Design Requirements

The first phase of design method is clarifying the task and defining of requirements of the system being designed. When accomplishing this task the limits of the system will be clarify. At this point, the first data which can be obtained from the design process by using well-prepared questionnaire are setting up the physical-, energy- and network limits (scope) of the system. On the another hand by establishing the system limits the necessary standards and guidelines for the design process will be well-defined. That is the first very important step for "risk analyses" (see Fig. 3.), which can be done to this early design phase.

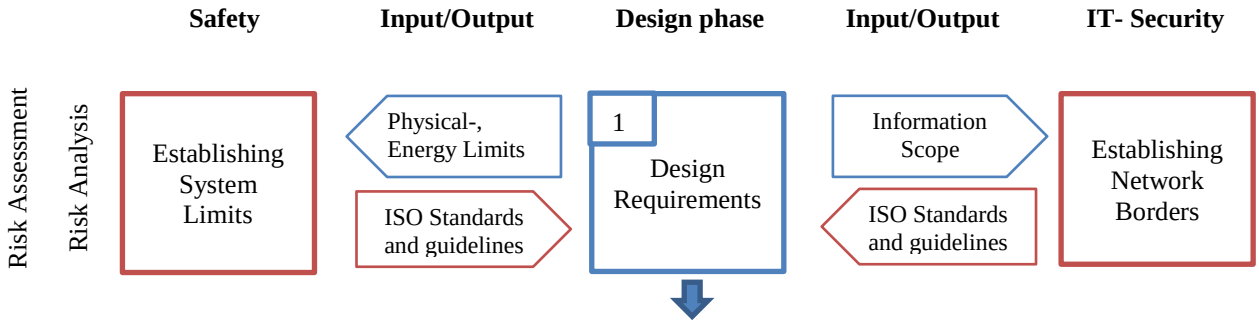

Fig. 3. Design Requirements and relationship with the safety and security

3.2. Conceptual design

The conceptual design phase involves the rational process of producing ideas into a realistic research design. During this phase according to the list requirements the system being designed will be represented as "black box" with main function/purpose as well as with inputs/outputs. The complex main function of the system will be analysed and divided into many solvable sub-functions. This sections of the design is well known as system-analysis. By dividing the main function the relationship between the sub-functions must remain. Relationship between the sub-functions can be mechanically, energetically, information or combined nature. In this way, the functional structure of the system being designed is given. The next stage is searching for solution(s) [6]. Sometimes Designer deals with only one possible solution, but in most cases there are many imaginable solutions. Imaginable solutions can be placed to the known "morphological box" (see Table 1). The next step is system-synthesis. Within the "morphological box" combining the possible solution and generating of possible concept candidate from active structure. For the first time hazards can be derived from the active structure.

			Sub-Solution			
		Sub-Function SF	**Sub-Solution 1**	**Sub-Solution 2**	**….**	**Sub- Solution n**
Conceptual design for a robotic work-cell	Hardware	Robots (R)	**R1**	**R2**	**….**	**Rn**
		End- Effectors (EE)	**EE1**	**EE2**	**….**	**EEn**
		Actuators (A)	**A1**	**A2**	**….**	**An**
		Sensors (S)	**S1**	**S2**	**….**	**Sn**
		Safety components (SC)	**SC1**	**SC2**	**….**	**SCn**
		……	**……**	**……**	**…..**	**……**
	Software	Software for Robot (SR)	**SR1**	**SR2**	**….**	**SRn**
		Software for X	**X1**	**X2**	**….**	**Xn**
		Software for Safety Components (SSC)	**SSC1**	**SSC2**	**….**	**SSCn**
		Solution Candidate	SC1	SC2		SCn

Table 1. Design Requirements and relationship with the safety and security

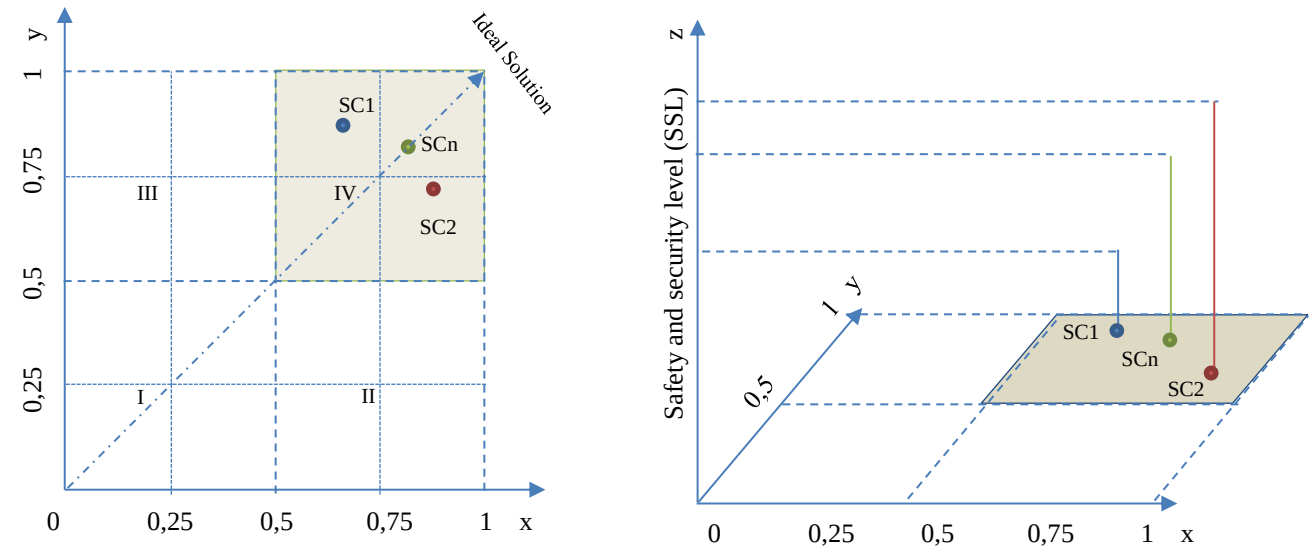

Fig. 4. Design Requirements and relationship with the safety and security

To choose the best solution for the preliminary design, all candidates will be evaluated for technical valence, economy and safety/security level. When evaluating the candidates, it is convenient to carry out with point evaluation and weighting of the evaluation criteria [6]. That will be useful to put the values in coordinate system as x-technical valence and y-economic valence. This parameters can take a values between 0 (worst solution) and 1 (ideal solution) (see Fig.4.). This is called "strength" diagram and shows the chosen solution for evaluation. According to that, acceptable solutions would be placed at fourth quadrant. All other solutions outside the fourth quadrants are not taken to evaluation, since they are either expensive or have technical weak points. And here is the tricky part of the method being introduced: simultaneously (beside evaluation of technical/economic performance) evaluating the safety/security level. Important is here to choose the solution with acceptable safety/security level. Too much safety/security means maybe to high costs. If the solution SCn fulfils the safety/security standards, then can be chosen as final concept, rather than SC2, ignoring hers higher safety/security level. In other words, the system with minimal equipment's, which satisfy safety/security level given by actual "CE"- standards will be the preferred concept for the new system being designed.

Summary at this stage of lifecycle design using active structure of the concepts candidate is possible to derive the possible hazards (see Fig. 5). Conceptual design phase inputs the physical principles to safety and at the same time gives the possible network topology for the network being designed. As shown in figure, after the hazard identifications at safety column and identifications of vulnerabilities at the security column was done, conceptual design phase benefits to important constraints besides the technical/economical aspects. Evaluation /selection of suitable combinations of the active structure for the subsequent concretization may consequently lead to a different design process and thus also to entirely different risk qualification procedures with potentially saving costs as well simultaneously increasing the level of safety/security. Hence this method prolongs various "gears" to compare and contrast the relative strengths and weakness of possible alternatives for getting the right decision.

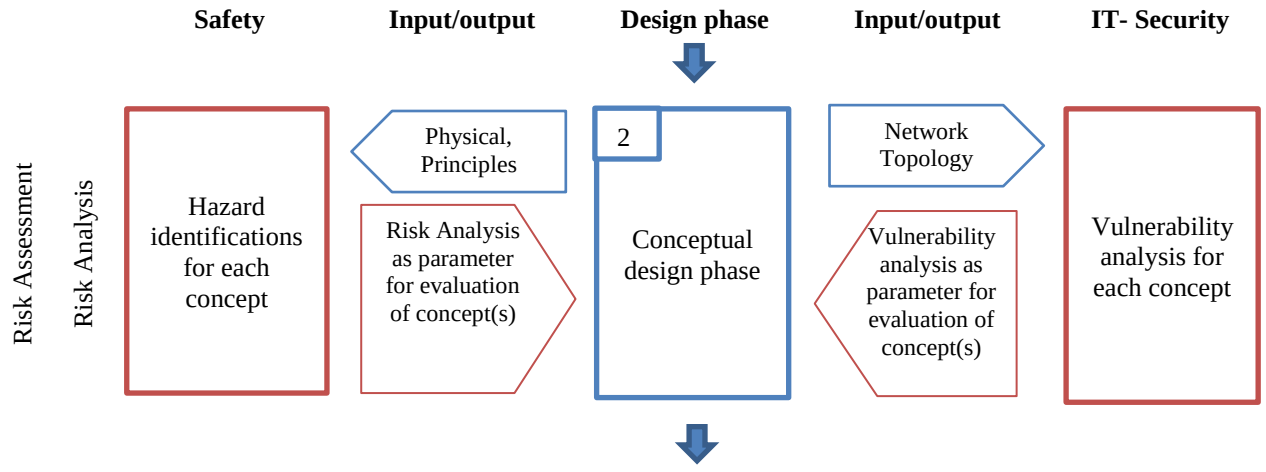

Fig. 5. Conceptual design phase including safety and security inputs/outputs

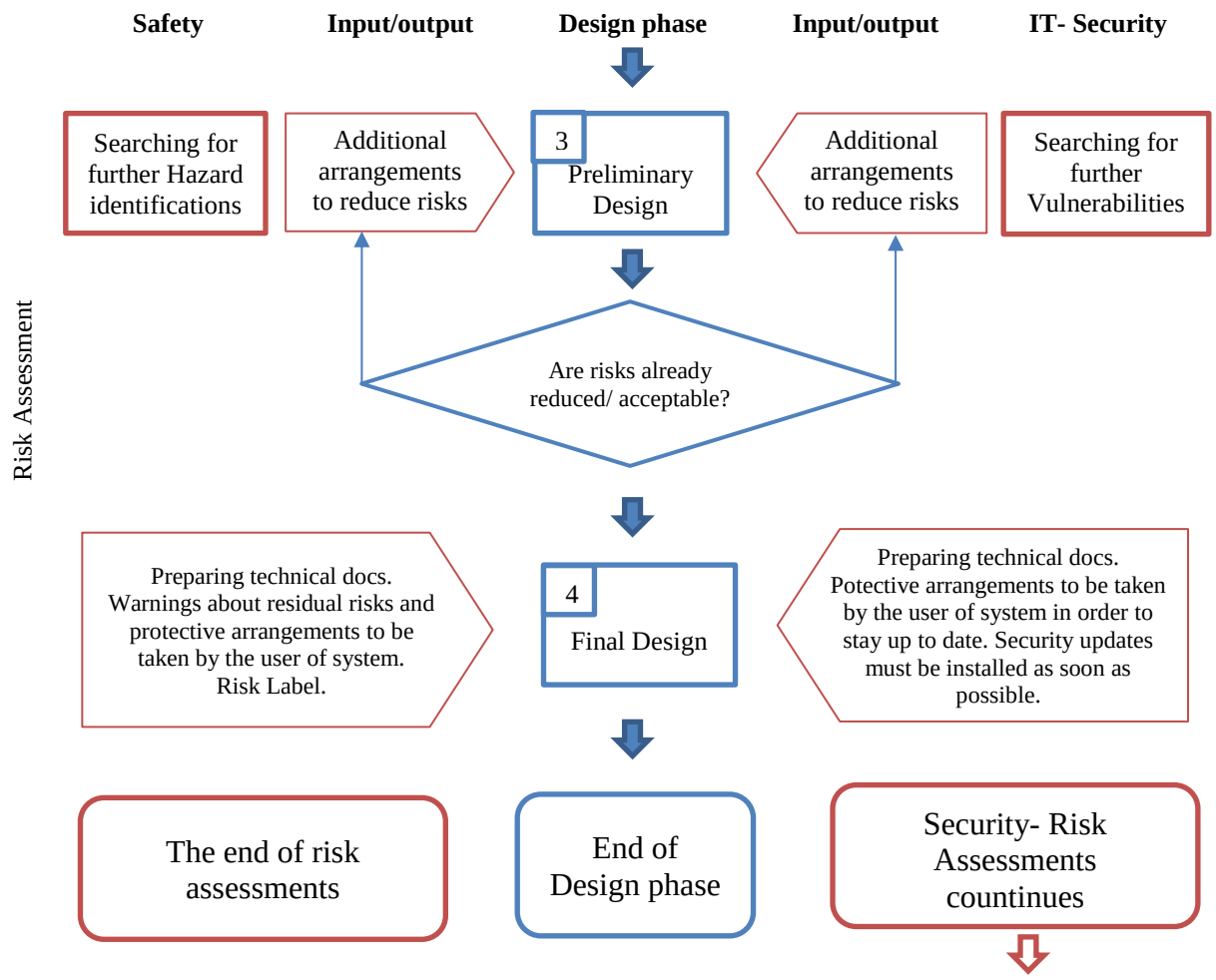

Fig. 6. Preliminary and final design phase as well as safety and security inputs/outputs

3.3. Preliminary design

After the evaluations of different concepts the chosen candidate represents the preliminary design. The preliminary design focuses on creating the general framework. The preliminary design is a key step in the early stages of hardware/software development as well as risk/vulnerability analysis, where customer requirements support the creation of the system architecture [7]. Hard-/software interfaces and established relationship between the components and system architecture should be included in the preliminary design. With these inputs of the preliminary design should improve hard/software development by giving floor plan, identifying further risks/ vulnerability and supporting additional optimisation of the solution. During these analysis of the preliminary design may be taken additional arrangements in order to reduce the risk to the tolerable level. The best example is given by [3]. In order to use the industrial robot in collaboration mode (with human) must any arrangements to be taken, for example: to reduce the power and force of the robot with corresponding file-module. At the security side of risk analysis the additional arrangements can be thought as actions for minimizing of "attack area". If the residual risk is acceptable the next stage of design phase can be started.

3.4. Final design

In this task the overall system configuration is defined. Specifically, this phase includes the optimal design of the CAD parts, assemblies as well as drafting of all parts, with detailed manufacturing parameters and tolerances. Layouts, schematics, diagrams, handbooks of the hardware/software must be prepared for the system integrator and user for safety operating. All the documents and information's concerning security updates and upgrades must to be accessible for the system owner. As shown in the figure 6, the safety part helps the final design by preparing of technical documentation, labelling the residuals risks and ends with system integration respectively with functional test. Labels of system components, which are potential risk for the safety operation, must to be visible and perceptible. Against the safety, security continuous his activities during pending phases of system life cycle. Important are periodic threat analysis, proactive information about security vulnerabilities, providing and installing updates [8]. In case of the hardware upgrade the functional safety must to be rechecked.

4. Conclusion

For realization of innovative manufacturing concepts and business models in the industry is the connection of machines and safety controllers to the industry network unavoidable. Paradigm called "Industry 4.0", in the production process designates not only opportunities for the future business models, but also risks that should not be undervalued. Challenges of this progress are difficulties by designing, integrating and operating of machines and work-cells in the networked factory. Difficulties are technical, organizational and straight legal nature. Therefore, from recent designer are required interdisciplinary knowledge in technical as well as in products certification fields. The rocky relationship between safety and security was explained in this work, when (if) the security of the system fails and the vital files responsible for the system safety are corrupted, the machines, work-cells and equipment's are not more safety for humans, operation and environment. Only safety/secure equipment's legitimates usage and operation of production systems. Concurrent treatment of this both issues (- integrated safety and security) during the design and lifecycle management would guarantee the company`s success.

This relationship between this two issues guided the researcher team to find the method and tools for performance evaluation of system. The outcomes of this method – integrated safety and security- would help designer, integrators and operators for designing, modifying, integrating, operating as well as maintaining of manufacturing resources. This method was practically established during a planning and implementation of several robot work-cells within digital manufacturing system at the university of applied sciences "Technikum Wien" in Vienna, Austria.

The main advantages of this method are:

- Saving costs during design process,
- Extensive analysis for hazard and vulnerabilities of design leads to minimizing of residual risks.
- Reducing time for the integration into the production systems
- Transparency between contractor and customer
- Stimulating teamwork of system designers

The most disadvantages of this method is the complexity and "big data" calculations. In order to diminish that, the future work was started to build software tool. This tool shows the mandatory standards, guidelines and all necessary information for designer/integrator of technical systems. The starting point of this safety-oriented software tool will be the analysis of the hazards in all phase's product life cycle as well as realistic prognosis of all risks associated with these hazards.

5. Acknowledgments

We would like to express our special thanks of gratitude to our sponsor MA23 Vienna, Austria. On this way, we want to express our special thanks to researcher group from "TÜV –Austria Gruppe". Without this support it would be not possible to realise this research.

6. References

[1] Dietrich, U. (2017), Modellbasiertes Systems Engineering – methodische Unterstützung zur Entwicklung Cyber-physischer Produktionssysteme – Sicherheitsanforderungen und praktische Grenzen, In: Industrie 4.0 – Safety und Security – Mit Sicherheit gut vernetzt, pp. 28-39. ISBN 978-3-410-26406-4, Berlin: DIN Deutsches Institut für Normung e. V., Beuth Verlag

[2] https://library.e.abb.com/public/3e234b767729aaa0c1257aa60064b129/3BUS095673_en_Whitepaper_-_The__Rocky_Relationship_between_Safety_and_Security.pdf, (2018). ABB AG. Accessed on: 2018-09-05

[3] Sicherheit in der Mensch-Roboter-Kollaboration, (2018). TÜV Austria Gruppe; Fraunhofer Austria Research GmbH, pp. 23-25, White Paper, No.3, March 2018

[4] Stuja K., Bruqi, M., Markl E. & Aburaia, M. (2016). Lightweight 4 -Axis Scara Robot for Education and Research, Proceedings of the 27th DAAAM International Symposium,pp. 0102-0108, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-08-2, ISSN 1726-9679, Vienna, Austria

[5] Radinger, T,; Stuja, K.; Wolfel, W. & Markl, E. (2017). Functional Safety Concept for a Handling Robot Built on Optical Systems, Proceedings of the 28th DAAAM International Symposium, pp.0168-0172, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-11-2, ISSN 1726-9679, Vienna, Austria

[6] Wittel H.; Muhs D.; Jannasch D. & Voßiek J. (2017). Roloff/Matek Maschinenelemente, pp. 9-17, SBN 978-3-8348-0689-5, Vieweg+Teubner GWV Fachverlage GmbH, Wiesbaden 2009

[7] https://www.seguetech.com/preliminary-design-improve-development, (2018). Segue Technologies Inc. ISO 9001: 2015 certified company, Accessed on: 2018-09-05

[8] Thomasius, R. (2017), Steuerung in der Cloud – Sicherheitsanforderungen und praktische Grenzen, In: Industrie 4.0 – Safety und Security – Mit Sicherheit gut vernetzt, pp. (195-208). ISBN 978-3-410-26406-4, Berlin: DIN Deutsches Institut für Normung e. V., Beuth Verlag