PESARO 2021

The Eleventh International Conference on Performance, Safety and Robustness in Complex Systems and Applications

ISBN: 978-1-61208-840-2

April 18 - 22, 2021

PESARO 2021 Editors

Mohammad Rajabali Nejad, University of Twente, the Netherlands

PESARO 2021

Forward

The Eleventh International Conference on Performance, Safety and Robustness in Complex Systems and Applications (PESARO 2021) continued a series of events dedicated to fundamentals, techniques and experiments to specify, design, and deploy systems and applications under given constraints on performance, safety and robustness.

There is a relation between organizational, design and operational complexity of organization and systems and the degree of robustness and safety under given performance metrics. More complex systems and applications might not be necessarily more profitable, but are less robust. There are trade-offs involved in designing and deploying distributed systems. Some designing technologies have a positive influence on safety and robustness, even operational performance is not optimized. Under constantly changing system infrastructure and user behaviors and needs, there is a challenge in designing complex systems and applications with a required level of performance, safety and robustness.

We take here the opportunity to warmly thank all the members of the PESARO 2021 technical program committee, as well as all the reviewers. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and effort to contribute to PESARO 2021. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions. We also thank the members of the PESARO 2021 organizing committee for their help in handling the logistics of this event.

PESARO 2021 Chairs

PESARO 2021 Steering Committee
Mohammad Rajabali Nejad, University of Twente, the Netherlands
Rémy Houssin, Université de Strasbourg - ICube Laboratory, France

PESARO 2021 Advisory Committee
Wolfgang Leister, Norsk Regnesentral (Norwegian Computing Center), Norway

PESARO 2021 Industry/Research Advisory Committee
Jean-Pierre Seifert, TU Berlin & FhG SIT Darmstadt, Germany

PESARO 2021 Publicity Chairs
Lorena Parra, Universitat Politecnica de Valencia, Spain
Jose Luis García, Universitat Politecnica de Valencia, Spain

PESARO 2021

Committee

PESARO 2021 Steering Committee

Rémy Houssin, Université de Strasbourg - ICube Laboratory, France
Mohammad Rajabali Nejad, University of Twente, the Netherlands

PESARO 2021 Advisory Committee

Wolfgang Leister, Norsk Regnesentral (Norwegian Computing Center), Norway

PESARO 2021 Industry/Research Advisory Committee

Jean-Pierre Seifert, TU Berlin & FhG SIT Darmstadt, Germany

PESARO 2021 Publicity Chairs

Lorena Parra, Universitat Politecnica de Valencia, Spain
Jose Luis García, Universitat Politecnica de Valencia, Spain

PESARO 2021 Technical Program Committee

H. B. Acharya, Rochester Institute of Technology, USA
Kaustav Basu, Arizona State University, USA
Morteza Biglari-Abhari, University of Auckland, New Zealand
Lelio Campanile, University of Campania Luigi Vanvitelli, Italy
Pasquale Cantiello, University of Campania Luigi Vanvitelli, Italy
Dieter Claeys, Ghent University, Belgium
Frank Coolen, Durham University, UK
Simon Eismann, University of Würzburg, Germany
Faten Fakhfakh, National School of Engineering of Sfax, Tunisia
Victor Flores, Universidad Católica del Norte, Chile
Rita Girao-Silva, University of Coimbra &INESC-Coimbra, Portugal
Teresa Gomes, University of Coimbra | INESC Coimbra, Portugal
Marco Gribaudo, Politecnico di Milano, Italy
Manu K. Gupta, Institut de Recherche en Informatique de Toulouse (IRIT), France
Mohamed-Faouzi Harkat, Badji Mokhtar - Annaba University, Algeria
Christoph-Alexander Holst, inIT - Institute Industrial IT, Germany
Rémy Houssin, Université de Strasbourg - ICube Laboratory, France
Sokratis K. Katsikas, Norwegian University of Science and Technology, Norway
Christos Kalloniatis, University of the Aegean, Greece
Atsushi Kanai, Hosei University, Japan
Georgios Keramidas, Think Silicon S.A., Greece

Copyright Information

Table of Contents

Personal Factors in Dealing with Safety Risks for Design and Use of Products and Systems

Mohammad Rajabali Nejad
Department of Design, Production, and Management
Faculty of Engineering Technology, University of Twente
Enschede, Netherlands
email: m.rajabalinejad@utwente.nl

Abstract—**This paper presents our study's result on the influence of personal factors on the design or use of products and systems in dealing with safety risks. It explores the impact of individual preferences on professional choices. The conducted interview results and collected responses show that personal preferences influence professional decisions for managing safety through design or operation.**

Keywords-safety; leadership; human factors; design; engineering

I. INTRODUCTION

Safety is the state of freedom from harm for humans, properties, and the environment, according to [1]. Safety overlaps with security. Safety and security are mainly about people, and humans have the most considerable influence on them. Humans, or people, have different values and interests. They sometimes share their interests and sometimes compete with each other. Also, people may use products in unintended ways or even misuse products. The human factors and safety culture are well-established in design, integration, and technical systems operation; see for example [2][3]. Although human factors for the users have been well-studied through literature [4], human factors may also influence designers themselves. In other words, the personality of designers (or their characteristics) may affect their design. That is a topic that requires attention because it can influence the use. This paper focuses on personal styles and their influences on both design and service.

Dealing with personal factors has been discussed in the literature. Among others, Katcher et al. define four different orientations that influence a person's value, interest, and behaviour [5]. This study adopts Katcher et al. because they focus on humans' strength to determine their behavioural styles. They define four main orientations to describe an individual style. They assume that each person has elements of all four directions in his or her behaviour. Those four orientations or categories are Supporting-Giving (SG), Controlling-Taking (CT), Conserving-Holding (CH), and Adapting-Dealing (AD) [5].

Studies show that human behaviour is also under the influence of the context. Katcher et al. describe two particular contexts stated as favourable and unfavourable [5]. They argue that personal behaviour – or the so-called personal style – is the combination of the four orientations and the context's influence.

II. HUMANS SYSTEM INTERACTIONS

For studying the role of humans in connection with a product or system, we first look into the product/system life cycle. The entire product life cycle includes three different phases: functional, technical and operational, according to [6], as shown in Figure 1.

The role of humans in each one of those phases is explained next.

A. *Humans in dealing with functional aspects*

Functional aspects refer to the life cycle stage which results in functions and specifications for a system or product [6]. Safety is a market must and dictated through regulations. However, pushing safety through a prescriptive approach is most of the time giving its place to reaching goals and motivations. In addition to the safety-related requirements, personal, social, or political interests may compete or conflict. Those needs – which might be unspoken – may substantially influence a specific design's success or failure.

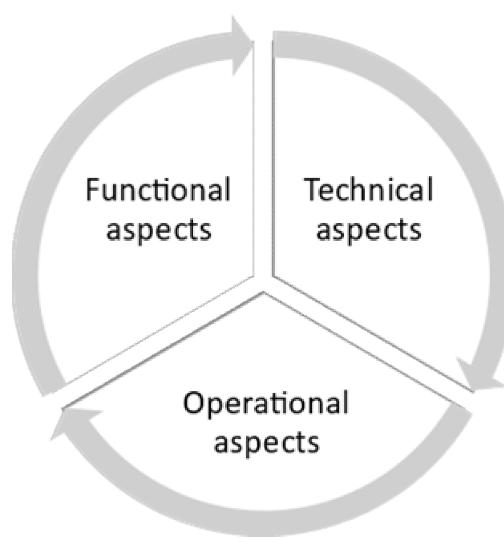

Figure 1. A system/ product life cycle has functional, technical, and operational phases, adapted from [6].

 ISBN: 978-1-61208-840-2

B. Humans in dealing with technical aspects

Technical aspects refer to the life cycle stage which results in technical design, production, and installation for a system or product [6]. This phase is under the direct influence of designers. Designers are also humans and have their values, styles, and interest which may influence their design practices.

C. Humans in dealing with operational aspects

Operational aspects refer to the life cycle stage which results in operation, maintenance, and retirement for a system or product [6].

Managing risks and opportunities for occupational health and safety is a significant task for the safe operation of products and systems. The commitment of top management, sound policies and communication, consultation and participation of workers, and effective processes are critical success factors [7]. Therefore, proper commitment, communication, and culture are indispensable elements of safe and successful operation.

III. PROBLEM STATEMENT

Designers and users are the two stakeholders who influence product safety at most, according to [6, 8]. Designers are dominantly present in the functional and technical phases, and users (or operators) directly affect the operational phase. This study's primary question is: "do the personal factors influence the design or use style?". In this context, the personal, design, and use styles have been defined as follows:

- Personal style refers to the combination of the orientations that characterises a persons' behaviour
- Design style refers to the combination of the orientations that characterise a designer's choices in the course of design
- Use style refers to the combination of the orientations that characterise a user's choices in the course of the use

In other words, the hypothesis is that the design or use styles are under the influence of personal orientations. This assumption leads to two important conclusions. It implies that design style may be under the influence of the designer's personality. It also means that the use style may be under the influence of individual users.

IV. RESEARCH METHODS

A. Literature domains

This study assumes that people have different styles and uses four categories of personality types based on the method developed by Katcher et al. [5]. Those four categories are SG, CT, CH, and AD. The literature for this research mainly covers the domains of human behaviour [5][7], safety engineering [1][9], and design [6][8].

B. Interviews

In addition to the literature review, this research's primary hypothesis was reviewed by different experts in human psychology, system safety, and professional designers. Interviews were conducted through an unstructured approach. Based on the literature review and the collected feedback, a questionnaire was designed to find the possible correlation between personal and professional styles.

C. Questionnaire

A questionnaire was designed to cover multiple topics and to identify personal styles, design style, and the responders' use style. The questions were multiple choice and had no right or wrong answers. In other words, all the answers were correct and of an equal level of importance. They were designed to force the responder to prioritise the given choices. In this way, the responder is likely to prioritise those answers that resonate with his/her personal preferences. A summary of the questions is provided in Table 1.

TABLE 1. THE SETTING OF THE QUESTIONNAIRE

	Subject of questions	***Main questions***	***Sub-questions***
1	personal style recognition	6	24
2	design style recognition	3	12
3	use style recognition	3	12

D. Workshop

The responders were asked to participate in a workshop. The responders were assigned to different groups. The same use scenario was given to all the groups, and they were asked to sketch the response of the users/ designers based on various personal orientations. Based on the author's review, the outcomes showed that the reactions were converging to specific patterns.

V. RESULTS AND DISCUSSION

In total, ten professional designers completed the questionnaire successfully. In general, the responders found the questions relevant and exciting. However, they also often experienced a dilemma to choose the most favourable answer. The results are presented in Figure 2. In this figure, the axes show relevant scores per each orientation, and each colour represents a response. There are two types of markers in the graph. The circles present the design orientations, and the triangles present the use orientations. In general, the figure shows a Pearson correlation between personal, design, and use orientations.

Table 2 shows the Pearson correlation coefficients between personal style and design style and between personal style and use style. In both cases, more than 50% of answers represented a correlation above 50%.

The results present a correlation between personal preferences and design or use choices. The results confirm that a designer with the supporting orientation intends to help and support others in the best possible way considering that all human lives are of equal worth. For the conserving direction, the designer wants to focus on quick solutions and the users' responsibility. A designer with a conserving orientation is likely to focus on details, follow instructions, and use logical arguments for managing risks. A designer with an adaptive orientation is likely to focus mainly on the reactions of users, stakeholders, or other team members aiming to avoid conflicts.

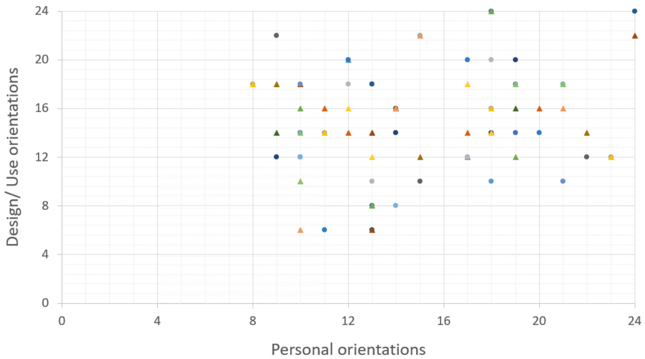

Figure 2. Collected responses

TABLE 2. CORRELATION COEFFICIENTS

		Correlation coefficient (%)			
Number of responses	**Style**	0-25	25-50	50-77	75-100
	personal vs design style	1	3	1	5
	personal vs use	1	3	5	1

VI. CONCLUSIONS

This paper's main conclusion is that personal factors (preferences, values, and styles) influence professional choices for designers, operators, and users. It seems necessary to point designers' attention to their unique styles and make them aware of their strengths and points for extra attention. Moreover, this awareness can help to design products and system in a way that will satisfy a variety of users with different styles. In other words, designers need to aim to design products and systems in such a way that the operation in both normal and extreme modes of operation covers a wide range of personal styles.

The next step for this study will be reviewing and comparing the final products delivered by different designers.

ACKNOWLEDGEMENT

The author kindly acknowledges the support of designers, safety engineers, certified trainers, and the responders who participated in this study. Special thanks to peer reviewers for their feedback and to Y.V.D. Leeuwen for her contribution in making the questionnaire.

REFERENCES

[1] DoD, "MIL-STD-882E: 2012 Department of Defense Standard Practice System Safety," *MIL-STD-882E,* 2012.

[2] G. G. Porto, "Safety By Design: Ten Lessons From Human Factors Research," *Journal of Healthcare Risk Management,* no. 3, 2001.

[3] L. Cullen, "Human factors integration - Bridging the gap between system designers and end-users: A case study," (in English), *Safety Sci,* vol. 45, no. 5, pp. 621-629, Jun 2007, doi: DOI 10.1016/j.ssci.2007.01.002.

[4] X. Sun, R. Houssin, J. Renaud, and M. Gardoni, "A review of methodologies for integrating human factors and ergonomics in engineering design," *Int J Prod Res,* vol. 57, no. 15-16, pp. 4961-4976, 2018, doi: 10.1080/00207543.2018.1492161.

[5] A. Katcher, G. Knodt, and B. Forbis, *Effective Consultation with the Lifo(r) Method*. Createspace, 2015.

[6] M. R. Nejad, *Safety by Design Engineering Products and Systems*, First ed. Hengelo, Netherlands, 2020, p. 164.

[7] ISO, *ISO 45001 Occupational health and safety management systems — Requirements with guidance for use*. Switzerland: International Organization for Standardization, 2018.

[8] ISO, *EN-ISO 12100:2010 Safety Of Machinery - General Principles For Design - Risk Assessment And Risk Reduction*. Brussels: European Committee For Standardization, 2010.

[9] N. J. Bahr, *System Safety Engineering and risk assessment*. CRC Press, 2014.

Safety Case Generation by Model-based Engineering: State of the Art and a Proposal

Fang Yan, Simon Foster, Ibrahim Habli
Department of Computer Science
University of York
York, UK
email: firstname.lastname@york.ac.uk

***Abstract*—The paper is a review to evaluate the current techniques for safety case generation using Model-based Engineering. Safety cases provide an explicit and structured means for assessing and assuring the safety of complex systems. For systems developed with Model-based Engineering, safety cases can be constructed with system models as input and should evolve hand-in-hand with system models when the system updates. Model-based Engineering can provide automatic means for the generation to improve efficiency. But there is not a full automation solution to cover the entire generation process. This paper investigates state-of-the-art of Model-based Engineering applications to safety case generation, explores the challenges and gaps, and proposes a solution framework to address the gaps through the model transformation within the Eclipse Modeling Framework.**

Keywords-safety case; assurance case; model-based engineering; generation; model.

I. Introduction

Safety Cases (SC) are defined as compelling arguments, supported by evidence, that systems operate as intended for defined applications in defined environments [1]. They provide a systematic way to argue the safety properties. SCs are important to the operation of safety-critical systems and recommended in some safety standards, such as ISO 26262 [2].

Many robotics and autonomous systems are safety-critical, such as autonomous cars, unmanned aerial vehicles, and medical robots. Their operational environments are relatively open and not sufficiently predictable during design. This may necessitate the system evolution, i.e., the redesign or replacement of system functions/components, during runtime at a higher frequency than traditional safety-critical systems.

SCs are constructed alongside the system development process. One of the issues for SC generation is the repeated workload from SC evolution due to system development iteration. Therefore, an automatic way for SC generation and co-evolution with system design is desired. SCs need to evolve when the systems are subjected to updates. This evolution is really an instance of the more general problem of generation, and so if we tackle the latter, we can more easily tackle the former. Therefore, We discuss the generation process in the paper.

In terms of the technical solution for generation automation, we explore Model-based Engineering (MBE). MBE has been well-adopted for system development thanks to its efficient tool support, and its applications have expanded into the surrounding aspects including SC generation. MBE techniques bring the capabilities of validation, model checking, simulation, model to model transformations, etc. From the published work, we can tell that the MBE applications on SC generation vary in terms of the techniques exploited, the generation phases applied to, and the extent of automation, etc. However, there is not an MBE solution to guide the whole engineering process of SC generation. The purpose of this paper is to understand the state-of-the-art of MBE applications on SC generation, to evaluate the automation degree of the solutions, and to point out the research gaps and the possible research directions. A new technical solution is proposed at the end to provide a framework to address the gaps. We only focus on the work that treats SCs as models, i.e., the whole set of SCs can be manipulated with MBE techniques.

Section II introduces the main background of the paper. Section III investigates the state-of-the-art of MBE based SC generation methods. Section IV evaluates these MBE solutions, identifies the open gaps, and proposes a new MBE solution. We conclude in Section V.

II. Background

A. Safety Case Notations

The widely used SC notations are the structured graphical forms, including Goal Structuring Notation (GSN) [1] and Claims-Arguments-Evidence (CAE) [3]. Many tools for SC generation and management are compliant with GSN. But most of them are not suitable for MBE applications due to the lack of a model-based foundation.

Structured Assurance Case Meta-Model (SACM) [4] is a standard for SC development and exchange released by Object Management Group (OMG). It specifies a metamodel composed of three concepts: argumentation, artifact, and terminology. SACM can support a variety of notations including GSN and CAE. SACM version 2.1 was published in 2020. As a new standard, SACM has little application in industry yet. However, it enables MBE techniques to be applied to SCs. We envisage future applications of SACM with possible toolchain support.

B. Model-based Engineering

To generate and manipulate SCs as models, metamodels of SC are indispensable. The most prominent modelling frameworks are the Eclipse Modeling Framework (EMF) [5], offering the metamodelling language Ecore, and the Meta Object Facility (MOF) [6], a standard metamodelling language defined by OMG.

 ISBN: 978-1-61208-840-2

III. Model-based SC Generation

A. A common SC generation practice

From a practical point of view, a common SC process is threefold, as shown in Fig. 1, including SC pattern design, instantiable data management, and pattern instantiation.

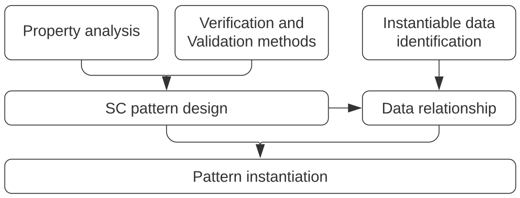

Fig. 1. A common process for SC generation

The concept of SC pattern is introduced by Kelly in [7]. It is an abstract structure containing placeholders that can be instantiated by concrete argument elements. For example, hazards with placeholders {Hazard} in patterns need to be replaced by the specific hazard content. It is a good practice for reusing SC structures.

To implement the instantiation, we need to manage the instantiable data. That is to identify the data required for SCs, and the relationships between the data elements and also between the data and SC elements. For example, a regulatory requirement may require that all hazards are mitigated. Thus, this requirement and all the hazards are instantiable data and the traceability between them shall be built. Further, the regulatory requirements may fit into the top claim of SCs, the hazards shall be used for lower claims to support the top claim.

The SC process progresses along with system development, and takes the system data as input, such as regulations, hazards, safety requirements, architecture, specification and design, validation and verification plan and results. To feed the system data into the pattern is the process of instantiation. This can be either manual or automatic depending on the data form and the tool support. If the intention is an automatic instantiation by tool, machine-readable instantiation data is required. Similar to the instantiation process, the data processing can be either manual or automatic through MBE as well. Based on the process above, different possibilities to use MBE for SC generation automation are discussed in the rest of this section.

B. SC generation by pattern instantiation

In this section, we discuss a common way to exploit MBE in SC generations following the process in Section III-A. The idea is to generate SC pattern models compliant with a metamodel, manually build the mapping between instantiable data and SC pattern nodes, then to instantiate the pattern automatically through MBE. The method includes following steps.

Step 1, to build a SC metamodel. This is usually done by building a GSN-based metamodel, or extending the SACM metamodel to be compliant with GSN.

Step 2, to design the SC pattern according to the system nature and create the pattern models using the SC metamodel.

Step 3, to identify and organize the instantiable data as a data table. The data may include hazards, causes, safety requirements, system requirements, tests, etc. The data types and the inter-relationships among data are defined in the table. The data can be either in a structured or unstructured manner.

Step 4, to manually establish the mapping between the nodes of SC pattern and the elements of the data tables.

Step 5, to instantiate the pattern models according to the mapping table of Step 4 and to output the SC models. The way to instantiate is first to identify the node in the pattern to be instantiated and the corresponding data for the node from the mapping table, then to fill the data into the pattern nodes.

The SC pattern is represented as models which allows the generation of SC models by automatic instantiation, and the subsequent model management capabilities, e.g., model validation, model query, and model comparison. However, since the data mapping table is generated manually, every time the source data in Step 3 is changed, e.g., a hazard is added or a safety requirement is deleted, the mapping needs a manual upgrade. This will bring high workload due to the frequent system design modifications.

Denney and Pai [8] have developed an automatic tool AdvoCATE based on this process for SC generation, management, and evaluation with the Eclipse EMF. The AC metamodel is created based GSN with a formal syntax. However, this is not a fully automated process as the logical mapping between SC nodes and system data are identified manually in the instantiable data processing phase.

The approach of Hawkins et al. [9] follows the same Step 1 and Step 2 as in [8], but exploits model weaving [10] to establish the mapping between instantiable data models and SC pattern models at the metamodel level. Model weaving is used to build relationships between elements of different metamodels, and can be realized manually or automatically by model transformation. The process differs from the method above in Step 3 to 5 as follows.

Step 3, to identify the instantiable models, such as system models, system error models.

Step 4, to establish the relationship between the elements of SC pattern and the elements of the instantiable models at their metamodel level within a weaving model.

Step 5, to instantiate through the weaving model execution and to output the SC models. The way to instantiate is first to identify the elements to be instantiated in the pattern, then to find the corresponding system model element through weaving model. For example, the “component goal” in SC pattern is the “process” element in Architecture Analysis and Design Language (AADL) models. So, the “process” models are extracted from the package of the whole system models and filled into the “component goal” in SCs.

Compared with [8], one of the advantages of the model weaving method is that the instantiable data can be extracted from the system models automatically. Secondly, the automatic co-evolution is enabled because the links between SC elements and system models are built between the metamodels instead

 ISBN: 978-1-61208-840-2

of specific system data therefore can be updated automatically when the system design changes.

However, the method is limited to the systems developed with MBE because the data that has no metamodel supports cannot be processed by model weaving. We refer to this kind of data as ”unstructured” in the paper. Also, with the claims instantiated only by system models, the SC generated is incomplete. A SC structure usually starts from abstract property goal, goes down to the hazards and safety requirements, and then is related to system models representing functional requirements and design. Since the first three of data above are usually unstructured and cannot be processed by MBE directly, the corresponding claims are not covered by this method.

C. Integrated SC generation by system model query

This method is to generate SC models by system model query. The query language and the environment are both integrated with the system development environment. The query codes for SC generation are generated manually, but the codes can be reused as a library, thus the co-evolution of the SC models and system models can be automated. The method includes the following steps.

Step 1, to design a Domain Specific Language (DSL) specific to a certain system modelling language for SC claim generation in a formal manner and for system model query.

Step 2, to formally define the top-level claim using DSL within the system development environment.

Step 3, to design model query rules for the top-level claim using DSL, and return the query results as the SC evidence.

The claim formalization and the system query are implemented in the same environment of system modelling. This allows the tight coupling of SCs with system models and ensures the automatic consistency of the two when design changes. Resolute [11] is a DSL designed for creating SCs for AADL models following the steps above. The limitation is that the DSL is specific to AADL and not applicable to other modelling languages. Also, since SCs are highly integrated with system models, the claims do not involve the unstructured data including such as hazard and hazard causes, etc. Thus, the SCs generated are incomplete.

D. SC generation by claim formalization and refinement

In this method, SC claims are formalized as a series of mathematical assertions about a system model equipped with a formal semantics. While the system models are refined, the concrete low level claims are inferred from top level assertion in parallel. The main benefit of the method is that the inference from top level to lower level claims can be verified by rigorous mathematical refinement checking. The method includes three steps.

Step 1, to formalize the top claim as an assertion “$M \models G$ under A”, where M is the system model, A is an assumption on environment, G is the guarantee on system model. This assertion denotes that the system models satisfy the guarantee if the assumption is valid.

Step 2, to decompose the top claim by model refinement, i.e., by refining the system model through system development, weakening the assumptions, and decomposing or adding guarantees. Thus, the lower level claims are inferred as a set of “$M^* \models G^*$ under A^*” where * means “refined”.

Step 3, to verify the correctness and completeness of the refinement by Formal Method (FM) verification. This activity assures the completeness of the SC structure generated through model refinement in a rigorously mathematical way.

Besides the benefit of the rigorous verification, the integration of the system models with SC claims supports the automatic co-evolution of SC whenever system design changes. However, since the top level claims are usually abstract, engineering review is a more appropriate way for decomposition validation, and the formalization and refinement checking would add no extra value. Additionally, the tight coupling of SCs with system models requires that both the SC and system be modelled in a formal way, and this requires the expertise of formal methods.

Gleirscher et al. [12] proposes this solution and formalize the claims using differential dynamic logic. The refinement checking is demonstrated in Isabelle/HOL [13]. Diskin et al. [14] applied the similar concepts for SC construction using data refinement. To reduce the need for FM expertise, Block Diagrams (BD) are used to guide the system model refinement from the perspective of the system architecture. However, for the further detailed system implementation, FM expertise is still unavoidable.

IV. Evaluation and proposal

From Section III, we can see that the SC generation by automatic pattern instantiation [8] provides a solution for construction of a complete SC. But the instantiable data process is not automated. This will bring a high workload of SC update when system data change. Also, the system model is not well integrated with SCs. On the other hand, the integration of the system models into SCs [9] [11] [12] [14] brings the benefit of automatic co-evolution of the SCs and system models. However, these system model-based solutions only create the lower structure of SCs because the upper structure of SC does not involve the concrete system design but the unstructured hazard analysis data. Moreover, the model query [11] provides an automatic traceability from system model to SCs, but the application is constrained to a certain system modelling language. The method of claim formalization and refinement [12] [14] requires FM expertise which may block the way of the engineering practical application.

To summarize, there is not an automatic solution fully covering the SC generation process with a wide application scope. The gaps lie mainly in: (1) a lack of an automatic way to process the unstructured instantiable data for MBE manipulation; (2) the missing of integration of upper SC structure derived from hazard analysis and the lower SC structure from system models; (3) a narrowed scope of applicability to the system development techniques.

To close the gaps, we propose an SACM compliant framework for SC generation combining the pattern instantiation based method and system model query based method. The

 ISBN: 978-1-61208-840-2

method is to be applied within the Eclipse EMF framework. The instantiable data, the system design, and SCs are all handled as EMF models. For a use case study, RoboChart [15] is chosen as the system modelling language which is designed in Eclipse and can be exported as EMF models. The framework includes following steps as shown in Fig. 2.

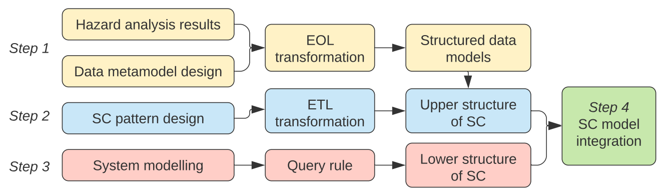

Fig. 2. A common process for SC generation

Step 1, the structured data model generation from hazard analysis result. In order to manipulate the unstructured data with MBE, we need first to design the unified metamodel in Ecore for the hazard analysis data in different format, then convert automatically the unstructured data to the EMF models through Epsilon Object Language (EOL) [16].

Step 2, to generate upper structure of SCs by instantiation of EMF models of hazard analysis data. We need to design the SC pattern according to the system property, and then design the instantiation rule with Epsilon Transformation Language (ETL) [16] to link the elements in the SC pattern with the instantiable EMF models. Here, we refer to the model weaving method [9]. But we do not need to create a standalone pattern model as the pattern has been integrated into the instantiation rule. Also, there is no need to design a specific SC metamodel as we use SACM as the SC metamodel.

Step 3, to generate the lower structure of SCs by querying system design models. We refer the model query concept in [11] in this step. The query rule is designed based on the property to be argued, and needs to obey the metamodels of RoboChart and SC, and the SC pattern. The difference from [11] is that we execute the query in Eclipse instead of a specific system development environment that is only applicable to certain system modelling language such as the Open Source AADL Tool Environment (OSATE) for AADL. This independence from the specific system modelling environment will allow the wider scope of the applicability.

Step 4, the integration of the SC structures. We create and insert an identifier keyword in the raw data of hazard analysis, instantiation rule of Step 2, and the query rule of Step 3. Through this identifier, the position in SC structure where system model query is required can be automatically identified and used to link the two parts of the SC structures as a whole.

Our framework can provide an automatic solution covering the entire SC generation. Compared with Section 3, our framework may automate the data processing, streamline the process by removing the pattern modelling and the SC metamodel design. It also closes the gap by integrating the SC structures generated from both structured and unstructured data. The proposal may have a wide scope of applicability as it can be applied to any system as long as the models can be converted into EMF models. Moreover, the utilisation of SACM metamodel instead of GSN-based metamodel may make our solution compatible with the upcoming SACM based tools in future.

V. Conclusion and Future Work

SCs are generated and evolve along with the system development. The automation of SC process reduces the workload and chances of errors. We believe MBE is a solution for this purpose. The paper discusses different MBE methods of SC generation and the automation capability of each method. The research gaps are identified as lacking of automatic processing of raw instantiable data, and of a solution for generating a complete SC from both structured and unstructured system data. We propose an SACM compliant framework for SC generation to close the gap. In future, we will apply our approach to an autonomous underwater vehicle, and revise the framework based on the implementation results.

Acknowledgment

This research is funded by the EU Horizon 2020 European Training Network “Safer Autonomous Systems” (Grant Agreement 812788) and the EPSRC-UKRI fellowship project CyPhyAssure (Grant EP/S001190/1).

References

[1] Assurance Case Working Group, “GSN Community Standard. Version 2,” 2018.
[2] ISO, “ISO 26262 Road vehicles–Functional Safety, Version 1,” 2011.
[3] “Claims-Argument-Evidence-Adelard LLP,” https://www.adelard.com/asce/choosing-asce/cae.html, online; accessed 6th March, 2021.
[4] Object Management Group (OMG), “Structured Assurance Case Metamodel (SACM), Version 2.1 beta,” 2020.
[5] D. Steinberg, F. Budinsky, E. Merks, and M. Paternostro, *EMF: eclipse modeling framework*. Pearson Education, 2008.
[6] OMG, “Meta object facility (mof) core specification,” 2019.
[7] T. P. Kelly and J. A. McDermid, “Safety case construction and reuse using patterns,” in *Safe Comp 97*. Springer, 1997, pp. 55–69.
[8] E. Denney and G. Pai, “Tool support for assurance case development,” *Automated Software Engineering*, vol. 25, no. 3, pp. 435–499, 2018.
[9] R. Hawkins, I. Habli, D. Kolovos, R. Paige, and T. Kelly, “Weaving an Assurance Case from Design: A Model-Based Approach,” in *2015 IEEE 16th International Symposium on High Assurance Systems Engineering*. IEEE, 2015, pp. 110–117.
[10] M. D. Del Fabro, J. Bézivin, and P. Valduriez, “Weaving models with the eclipse amw plugin,” in *Eclipse Modeling Symposium, Eclipse Summit Europe*, vol. 2006, 2006, pp. 37–44.
[11] A. Gacek, J. Backes, D. Cofer, K. Slind, and M. Whalen, “Resolute: an assurance case language for architecture models,” in *ACM SIGAda Ada Letters*, vol. 34, no. 3. ACM, 2014, pp. 19–28.
[12] M. Gleirscher, S. Foster, and Y. Nemouchi, “Evolution of Formal Model-Based Assurance Cases for Autonomous Robots,” *Lecture Notes in Computer Science*, vol. 11724 LNCS, pp. 87–104, 2019.
[13] T. Nipkow, L. C. Paulson, and M. Wenzel, *Isabelle/HOL: a proof assistant for higher-order logic*. Springer Science & Business Media, 2002, vol. 2283.
[14] Z. Diskin, T. Maibaum, A. Wassyng, S. Wynn-Williams, and M. Lawford, “Assurance via model transformations and their hierarchical refinement,” in *Proc. the 21th ACM/IEEE International Conference on Model Driven Engineering Languages and Systems*, 2018, pp. 426–436.
[15] A. Miyazawa, P. Ribeiro, W. Li, A. Cavalcanti, J. Timmis, and J. Woodcock, “Robochart: modelling and verification of the functional behaviour of robotic applications,” *Software & Systems Modeling*, vol. 18, no. 5, pp. 3097–3149, 2019.
[16] D. S. Kolovos, R. F. Paige, and F. A. Polack, “The epsilon transformation language,” in *International Conference on Theory and Practice of Model Transformations*. Springer, 2008, pp. 46–60.

User Safety Performance Evaluation from Complex Systems Design Phases: Application to Arduous Working Conditions

Remy Houssin
CSIP – ICube- University of Strasbourg
Strasbourg, France
e-mail : remy.houssin@unistra.fr

Muhammad Irshad Yehya
CSIP – ICube- INSA of Strasbourg,
Strasbourg, France
e-mail : muhammad.irshad_yehya@insa-strasbourg.fr

Amadou Coulibaly
CSIP – ICube- INSA of Strasbourg
Strasbourg, France
e-mail : amadou.coulibaly@insa-strasbourg.fr

***Abstract*— Considering user requirements in the design of production systems is a necessity imposed by directives and standards. However, in spite of standards application by companies, many user health problems still happen. So, it becomes a goal of companies to design machines and install manufacturing systems to improve the safety performance of their artefacts. In this paper, we propose to collect data and information concerning the difficult/harsh working conditions when using the artefacts (machine or system) in order to evaluate them from the conception phase to propose new more ergonomic systems/machines. To do this, we analyzed a system used by our partner company and completed our method, which is already proposed in the literature. The application hardness evaluation is presented in the article to demonstrate and evaluate the advantages and limitations of the proposed method.**

Keywords- Arduous working conditions; Design method; Performance evaluation; User safety.

I. Introduction

Since January 1st, 2015, in France, the “Pénibilité de travail”, (meaning, in English: difficult/harsh working conditions, arduous working conditions) has been included in the calculation of pension rights system. The related labor code is [1], taken from the European framework directive of June 12th, 1989. In the rest of the paper, we used “arduous working conditions” and not “Job penibility” as noted in [2]. This had three effects:

1) The first consists in establishing an inventory of working conditions in the existing production workshops.

2) The second, for works subject to arduous working condition tasks, it implements preventive measures to eliminate or reduce the arduous working conditions risk.

3) The third, for companies designing machines and installing manufacturing systems, is to take this difficulty into account when designing these systems.

The objective of this paper is to propose a method to formulate and evaluate ergonomic information (particularly related to arduous working conditions) and to use it in the design process. We know that the design from a technical point of view [3][4] is no longer sufficient to design an efficient system [5][6]. In this sense, the concept of integrated prevention has been defined and presented in numerous articles [7]-[13].

To be able to design a system that can be used in companies with a minimum level of ergonomic and safety risks authorized by law and standards, we propose to measure and evaluate the arduous working conditions during the use phase to estimate this for the design phase of a new complex manufacturing systems in an Industry 4.0 context [14].

A. Field data and method followed

In the unique safety document of each company, it is recommended to specify points such as the following:

- Risk assessment per workstation.
- Safety cards for the workstations.
- User safety data card.
- Assessment of musculoskeletal disorders for each workstation.
- Noise assessment for each workstation etc.

The question dealt with in this article is to identify and evaluate, based on good industrial practices, the information to be fed back in order to integrate the best ergonomic specifications in design, particularly related to arduous working conditions. For this, we used the DMAIC method: Define, Measure, Analyze, Improve and Control the preventive measures to be taken into account from the design stage. This method is applied on an existing system with two objectives, i.e., the first one is improving the design of future similar systems. The second one is to propose an approach that meets the conditions of use of such types of systems. For this, we have followed the following steps:

- Define the state of the art of the ergonomics and safety conditions of all workstations in the workshop.
- Choose and implement measurement tools and methods to measure and manage risk factors.
- Look for means and solutions to eliminate or reduce the risks exceeding the thresholds.
- Provide an assessment of the six factors increasing the arduous working conditions of work presented in the next section.

B. Components of the arduous working conditions

The Labor code stipulates that: it is necessary to eliminate any exposure of the worker to one or more occupational risk factors likely to leave permanent, identifiable and irreversible traces on his/her health. Since July 1st, 2016, L4121-3-1 [15] entered into force and ten risk factors were identified as the origin of the increase in arduous working conditions with their regulatory thresholds. The 10 risk factors associated with arduous working conditions are the following:

- Manual handling of loads
- Painful postures or forced positions
- Mechanical vibrations
- Activities carried out in a hyperbaric environment (high pressures)
- Hazardous chemicals, including dust and fumes
- Extreme temperatures
- Noise
- Night work and work in successive alternating teams
- Repetitive work

These ten factors are classified into three categories:

1) *Marked physical constraints*
2) *Aggressive physical environment*
3) *Certain working rhythms*

In Section 2, the method of integrating to use information from the first phase of the design is illustrated. In Section 3, we develop our work on the identification, measurement, evaluation and integration of arduous working conditions in design and present the results obtained. In the last section, we conclude and present some perspectives.

II. Integration Method to use System Information in Design Process

Considering the present methodologies' hysteresis and cost of the Human Factors and Ergonomics (HF/E) integration in the design phase, Sun et al. [6] attempt to develop a time saving, economic and standard approach for designers to integrate the HF/E from the early design phase. We use, in this work, the method proposed by Sun et al. in [6]. Based on the feedback from the field, the final objective is to demonstrate and analyze the feasibility of the method of integration to use information from the first phase of the design.

In [16][17], the authors presented rich state of the art containing the integration of human and ergonomic factors in the different phases and design processes. The key to achieving this integration is to understand the design, whose main goal is to get a product / system that matches the use and user requirements from the point of view, ease of use, user safety, reliability and efficiency in the workstation [18] [19].

Sun et al. in [20] proposed a systematic method taking into account related information to use. Sun et al. in [6] improved the first proposition by integrating the three-level "function-task-behavior" framework (Figure 1) and based on the simultaneous design of the product / system and its manual usage (Product manual).

The safety documents use in industries contain very little information on the evaluation of use under the conditions required by European directives. Many users do not rely on these documents in the day-to-day use of their machine [21].

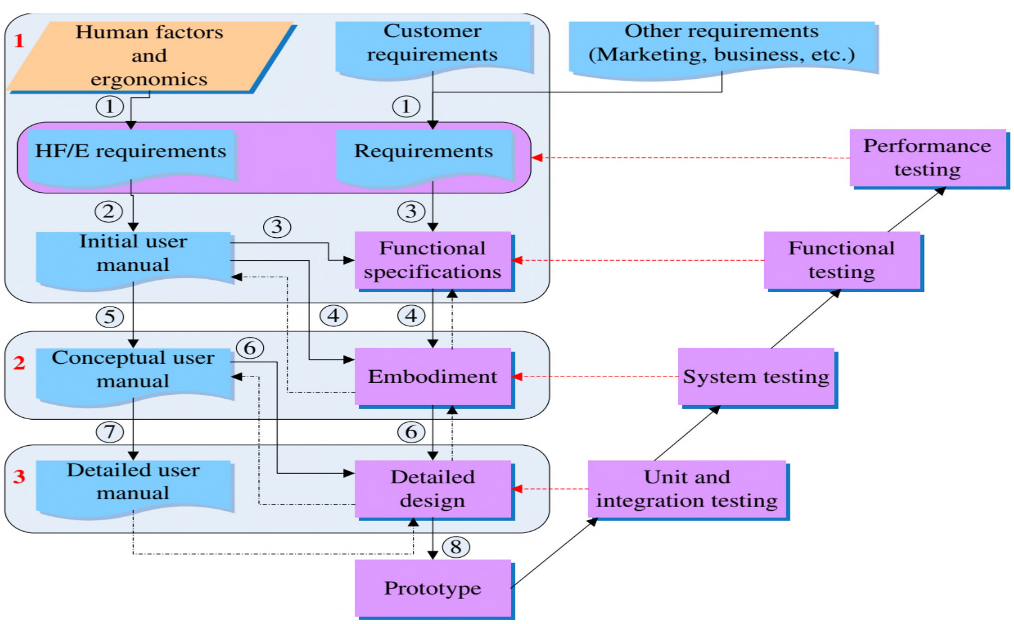

Figure 1. The Methodology proposed by [20]

In this method, the designer defines the initial product manual which directs the functional specifications and the mode of realization of the manual functions according to the requirements of the use. At this level, the designer defines the tasks to perform the functions provided for in the specifications. He distinguishes between the tasks performed by the product (system/machines) as technical tasks, and the tasks performed by the user as socio-technical tasks. At the second level, the initial product manual will be detailed to give a conceptual product manual which is the guideline of the detailed design. At this level, the designer will propose the structure that fulfills the technical functions compatible with the socio-technical (manual) tasks to be performed by the user.

Finally, at the third level, after having completed the detailed design of the structure, the designer refines the tasks performed by the user and those to be carried out by the technical structure after having completed the detailed design of the structure. Then, he analyzes the interaction between user behavior and system behavior in order to check the overall performance of the system (machine) and its user.

It was noted that the guideline of the method is to avoid bad interactions between the system (machine) and its user. Overall, all interactions that cause an ergonomic problem, or adversely affect the safety and health of the user should be eliminated.

However, Sun did not present how this product manual could be defined, served and evaluated on the three levels listed below, nor from what data and information.

Additionally, the method proposes some steps to analyze functions in tasks, then to characterize these tasks by identifying who does it, when, using what tools, on which part of system, etc. This method is a top-down method that begins from client, marketing, user and others possible requirements without any specific focus on how these requirements could be identified, set out and evaluated to know if they could be integrated in the design processes. Here in particular, we considered how to do that for the arduous working conditions that could appear during the use of the artifact (system or machine).

III. Taking into Account the Arduous Working Conditions from the Design Phase

First of all, we defined the criteria considered in our study:

- Meet the legal obligation, according to the article L4121-3-1 of the French Labor Art (Code).
- Preserve the health and safety of workers: the need to assess occupational risks does not only result from the observation of the large number of work accidents and occupational diseases, but also results from prevention of their occurrence from the design phase.
- Contribute to improving the performance of the system: The important consequences from the human point of view integration from design. This allows reducing direct and indirect costs.
- Improve and strengthen social relations: participatory prevention approaches make it possible to promote exchanges between user and designer.

Then, after having gathered the data necessary for a good approach from a legislative point of view, we identify the factors of arduous working conditions in the workshop of our partner company. We have identified existing workstations similar to the future workstation in which the system subject to the design will be implanted and installed. On each workstation, we observed and analyzed the working conditions in comparison with the work evaluation required in the unique safety document.

- Only the workstation operator has knowledge of the actual work. His/her active participation is the main key to the success of our process.
- Observation of workstations and especially dialogue with operators is, therefore, essential to extract information about their manner to use the system.
- These make it possible to consider the actual work of the operators, to visualize, to objectify and to assess the risks of arduous working conditions.
- In spite of standards application, the significant and intolerant risks presented in Table 1 were identified.

In order to respect the confidentiality imposed by the partner company, only two items are considered in Table 1.

TABLE I. Identified Risks

	Significant Risks
Raw Material Flow	Thermal environment
	Noise
	Energy
	Fire explosions
	Contact with other users
	Awkward postures
	Driving equipment
	Mechanical Vibration
	Manual handling
Milling Workshop	Noise
	Awkward postures
	Manual handling
	Working Organization
	External intervention
	Mechanical vibrations
	Hazardous chemical material

In comparison with the arduous working condition factors, the following risks are selected. In the following, we limit our observations to the factors related to the arduous working conditions that appeared in 2016. In the partner company only, the following factors were identified. The other factors do not exist in this business. For example, there is only one work shift and no night shift.

TABLE II. Risks Related To Arduous Working Conditions

	Significant Risks
Raw Material Flow	Noise
	Awkward postures
	Mechanical Vibration
	Manual handling
Milling Workshop	Noise
	Awkward postures
	Manual handling
	Mechanical vibrations
	Hazardous chemical product

A. Evaluation of arduous working conditions factor during raw material flow:

The raw material flow is used to receive, store and debit material either for subcontractors or for internal production orders. The following arduous working conditions factors are evaluated:

1) Noise: The sources of noise are saws and the machine that manufactures perforating blades. Personal protective equipment used to reduce exposure to noise is earplugs.

2) Awkward postures: Presence when pushing material onto the conveyor because it is very high in relation to the user.

3) Mechanical vibration: Exposure to vibration comes from the manual saw, but rarely comes into contact while cutting operation.

4) Manual handling: When transporting the material to a shipping pallet or to the saw, the operator has to push the long rods of material onto the forklift which is not very suitable because a lot of effort is needed to move the materials. For pushing the material onto the conveyor, this is very difficult due to the poor condition of the conveyor.

B. Evaluation of arduous working conditions factor in milling workshop:

In the milling workshop we observed certain factors identical to those observed in the raw material flow, but which do not have the same origins and their evaluations are different:

1) Noise: The combination of running machines presents a high exposure, to the point of raising one's voice to speak with a person a meter away. Personal protective equipment, ear plugs, are present.

2) Awkward postures: The material is stored on trolleys at a height close to the ground. The operator must bend to pick up the parts and certain measuring tools are placed at a height which implies restrictive positions.

3) Manual handling: Loads are carried regularly from the trolley to the workstation. For very heavy parts, an electric bridge is available to move them. Handling is also present when changing tools.

4) Mechanical Vibrations: The sources of vibration to which the operator may be exposed are all the machines that operate in the workshops.

5) Hazardous chemical agents: The products to which operators are most exposed are cutting oils and some grinding glues that will be identified later.

IV. ASSESSMENT OF RISKS RELATED TO ARDUOUSNESS

In order to be able to assess the arduous working conditions by factors, it is necessary to put in place some tools to collect the data and compare it with the exposure thresholds defined by the standards. Next, we detail the evaluation carried out for each factor.

A. Awkward postures

Awkward or strenuous postures are defined as forced positions of the joints of the human body. When there are situations with duration and intensity there is a risk of arduousness. We meaasured the different postions illustraited in Figure 2 and defined by standards as awkward postures.

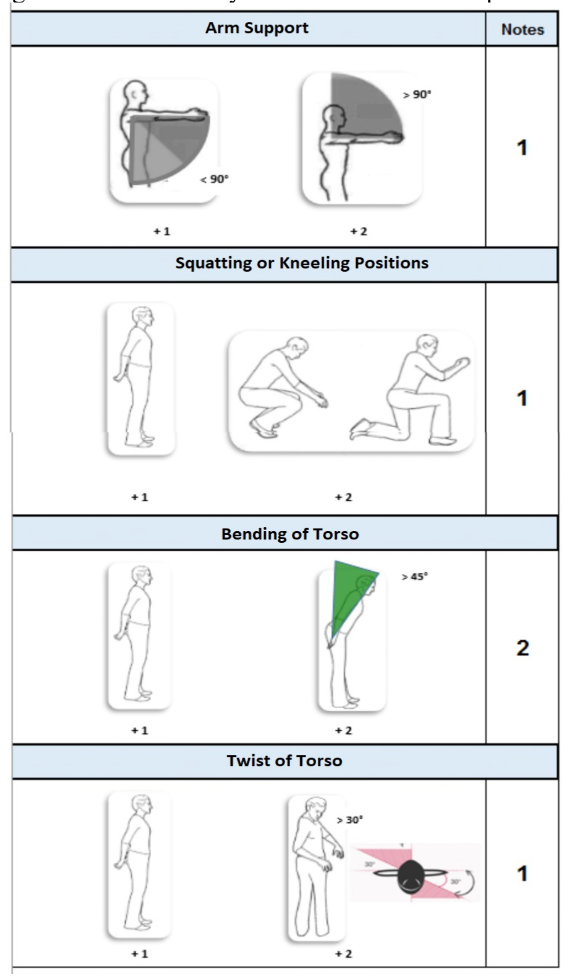

Figure 2. Different positions evaulated in Milling workshop

For each task done by the operator on each machine, we applied the following stepes

- Identified the angles of the position that exceeds the thresholds allowed by standards.
- Then, we timed the time of each task done in an awkword posture. These represent approximately 15% of the time spent on to do the machine setting-up tasks.
- For each awkward posture, we gave a grade as indicated in Figure 2.
- Evaluate the exposition time per year as a function of time and note.

Unfortunately, our industrial partner refused to communicate the final results of this evaluation.

B. Noise evaluation

We should remember that the exposure threshold is set by standards at 81 decibels (A) over a reference period of 8 hours, either a number of 120 "shocks" per year at 135 decibels (C). Article R. 4431-2 of the Labor Code prohibits companies from exposing employees to more than 87 dB (A). Thus, to analyze and diagnose exposure to arduous working conditions, a flowchart makes it possible to exclude or not the factor for each position (Figure 3).

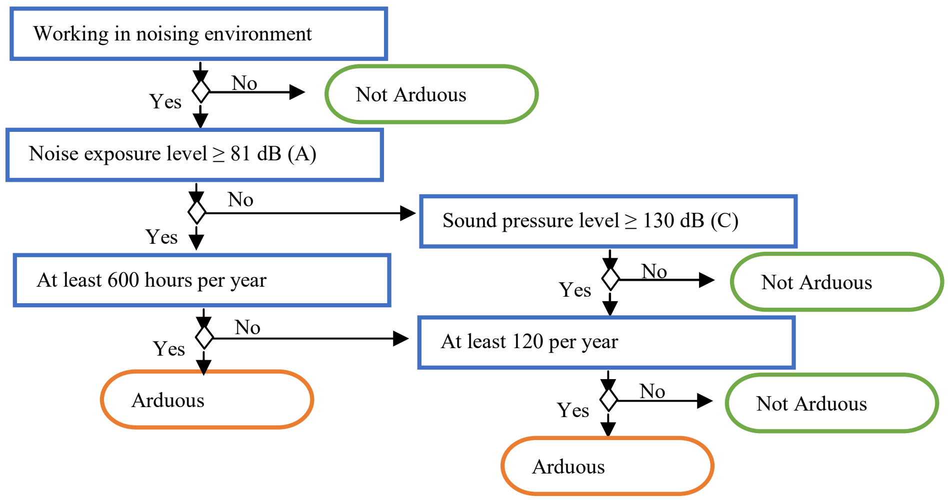

Figure 3. Flowchart for the noise factor

As soon as the environment is observed to be noisy, the sound intensity must be quantified. Here, we decided to find out about personal exposure to noise. To assess the noise and collect the necessary data, we used an Expositmeter to measure the intensity perceived by the operator. It is more accurate for measuring personal exposure to noise as operators move around a lot. It is necessary to map the entire production workshop to have usable data over time if there is no change in the location of the workstations.

C. Evaluation of mechanical vibrations

The 2016 reform requires cumulating the levels of vibration transmitted to the hands and arms with those transmitted to the whole body and comparing it to a threshold of 450 hours per year.

After identifying the positions exposed to vibrations, we quickly noticed that most machines exceed the threshold of 2.5 m / s² for vibrations felt in the hands and arms, where the Milling presents the greatest exposure compared to the other workstations. To assess this factor, we followed the same process by identifying the positions that cause vibrations. Then, it was necessary to determine the exposure times and compare the result with the exposure thresholds.

We noted the duration of exposure by timing the tasks performed by the different operators. The measurements are taken over a normal working week (not too busy and without layoffs). The maximum duration per day is 23 minutes which represents 15% of the time on a working time of 8:30 am. The overall duration of use of some machines does not exceed the thresholds per person exposed because several operators use it.

TABLE III. OVERALL DURATION OF USE

In hours	**Warehouse Trolley**	**Assembly Trolley**	**Milling**
Averages / Day	1.26	0.18	0.16
Provisional accumulation/Year	285.51	39,54	35.12
Max	1.90	0,53	0.31
Min	0.50	0.01	0.00

D. Evaluate hazardous chemical products

The chemical risk assessment required a great deal of investigation with the search for a way to assess and standardize an approach with chemical products. The assessment is based on the ND 2233 method and is a common language for doctors, CARSAT, and the labor inspectorate. The steps followed for the assessment of this factor are as follows:

1) Inventory of used chemical products and their location in workshops, workstations and tasks.

a) List all the products in the chosen software with their hazard statements.

b) Investigate their use by operators.

2) Comparison with ERP data to know the quantities used and ordered of each item codes.

3) Select the chemical products containing the hazard statements falling under the regulations on arduous working conditions.

4) Evaluate the duration of exposure for the products concerned and compare them to the exposure thresholds.

 ISBN: 978-1-61208-840-2

The products concerned are the products labelled as dangerous chemical, or emitted in the processes. To identify the products named to be eligible for the arduousness, we proceeded by funnel effect. The products with the terms of arduousness are identified and the inventory and classification by workstation and by machine made it possible to locate them.

Once the affected products were identified, we quantified the duration of exposure for each operator (times of use, duration and frequency of each exposure). By timing the operators working, we obtained an exposure time greater than the regulatory threshold of 150 hours / year. Products exceeding the thresholds are identified. These products are used for several tasks which multiply the total exposure time.

We obtain the following exposure times per operator (Table IV):

TABLE IV. EXPOSURE TIME TO CHEMICALS PRODUCT

	Exposure Hour/Year
Product 1	125.32
Product 2	323.76
Product 3	131.95

For products exceeding the thresholds, risk prevention means should be considered. Personal protective equipment is mandatory so that the operator is the least exposed. This includes a diving suit and a specific suit. For each of these products, exposure conditions must be reduced and prevention improved by redesigning systems in avoiding adding doors or boxing the machine which decrease the visibility and the accessibility of the operators. In Figure 4, we show an extract of our results (not clearly shown due to the confidentiality of data).

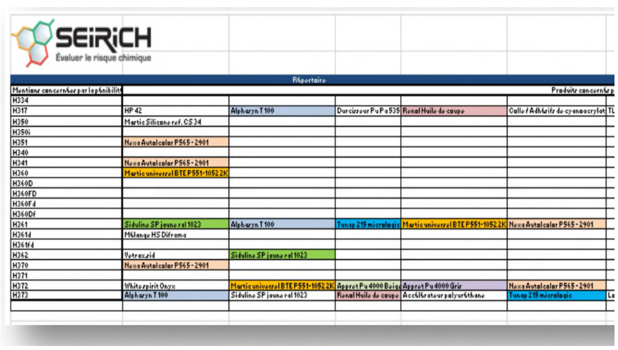

Figure 4. An extract of the evaluation of chimical factor

V. DISCUSSION

Our objective was to identify, through this field study, the data, parameters, factors, etc. necessary to take into account the arduous working conditions from the design phase. The data collected during this field study is richer than the data considered in the method proposed by Sun et al. in 2018. Indeed, Sun's method focused on the data for tasks to be done by users that 1) has been deemed necessary to define how the functions requested by the customer will be carried out and 2) those necessary for a safe use of the system. He took into account the factors: the duration of the task, who does the task (machine or operator), the order of the operating procedures as well as the structure of the task (a task can be broken down into sub-tasks, down to an elementary level).

On the other hand, the field data made it possible to establish the need to know the nature of the materials treated (chemical, wood, metals, etc.). But also, we were able to establish the work organization (a task that can be carried out by a single operator, it can be distributed over several operators and in several time frames).

Also, the thresholds imposed by the legislations are not sufficiently considered in the method employed by Sun. Indeed, the concepts of risk assessment are based on the product of a risk indicator calculated as a function of hazardous phenomena, exposure time, frequency of exposure and severity [22].

Once these safety parameters are identified, they have to be taken into account by the designer. Some methods could be used, like the ones proposed in [23] and [24], on the integration of safety user parameters in the design process. In both these works, the authors proposed a framework to consider standard data about user safety and some classical known parameters about hazardous situation, but not about Arduous Working Conditions.

Taking our results in consideration in the design process could influence the designer decision. For example, instead of trying to change the cheap technical solution that fulfills the function, but has very high level of vibration by another one (which may be more expensive, but cause less vibration), the designer could keep the first solution too. He/she can either automate some of the manual tasks to avoid or minimize human intervention and, therefore, minimize exposure time. Or he/she could specify in the documents provided to the user client that it is necessary to avoid having a single operator working on this machine all the time or for longtime and that it would be good to alternate two operators during the work time.

Our industrial partner is a constructor of paper machines. We did our analysis for them at a workshop of one of their clients. Their objective was to optimize the performance of their artefact in improving not only the user safety by reducing the dangerous conditions and dangerous zones in very short term (operating term) [24], but also, by considering the very long-term dangerous factors, like those of arduous working conditions. Our work helped them evaluate these factors for the next generation of machines.

VI. CONCLUSION AND PERSPECTIVES

We can see that the integration of human factors in the design of products, machines, systems has become more and more important in order to improve the final performance of the designed system. Many proposed methods are constantly improving to comply with regulations, but also go further than standards. In this article, we first defined the framework of this work by

 ISBN: 978-1-61208-840-2

assessing the arduous working conditions to comply with the labor code in order to be able to estimate it from the design phase. For this, we based the work on a method proposed in the literature to determine the data to be sought after in the field at the user workshop and potentially integrate it in the design of future similar systems. These works have shown that the method takes into account most technical and use data. However, we did not find in literature any method considering the data concerning the arduous working conditions and, in particular, the factors of which have recently changed. So, we identified and evaluated some arduous working conditions factors in existing systems. Then, we proposed to the designer to integrate them in his/her design process and refine his/her decisions and choices. We found that considering the materials used and the organization of work in the design is possible and makes compliance with standards easier. In future work, we will propose an evaluation of the identified relevant parameters. Also, other areas will be analyzed in other contexts of use to propose a global and more complete approach in order to provide designers with a method considering all field data related to use conditions, but also propose a method to integrate the identified parameters into the design process.

REFERENCES

[1] Law, “Labor Code.” [Online]. Available: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000023032092/2021-03-11/.

[2] A. Baurin and J. Hindriks, “Job penibility: measurements and policy discussions.” Université Catholique de Louvain, 2018, [Online]. Available: https://dial.uclouvain.be/memoire/ucl/en/object/thesis%3A14438/datastream/PDF_01/view.

[3] G. Pahl and W. Beitz, “Engineering design: a systematic approach (2d) Springer-Verlag.” London, 1996.

[4] W. B. Rouse and W. J. Cody, “On the design of man-machine systems Principles, practices and prospects,” *Automatica*, vol. 24, no. 2, pp. 227–238, 1988.

[5] D. Zhou, J. Chen, C. Lv, and Q. Cao, “A method for integrating ergonomics analysis into maintainability design in a virtual environment,” *Int. J. Ind. Ergon.*, vol. 54, pp. 154–163, 2016.

[6] X. Sun, R. Houssin, J. Renaud, and M. Gardoni, “Towards a human factors and ergonomics integration framework in the early product design phase: Function-Task-Behaviour,” *Int. J. Prod. Res.*, vol. 7543, pp. 1–13, 2018, doi: 10.1080/00207543.2018.1437287.

[7] NF EN ISO 12100 and CEN, “Safety of machinery: General principles for design, Risk assessment and risk reduction,” *Bruxelles*, p. 93p, 2010.

[8] A. C. Falck and M. Rosenqvist, “What are the obstacles and needs of proactive ergonomics measures at early product development stages?–An interview study in five Swedish companies,” *Int. J. Ind. Ergon.*, vol. 42, no. 5, pp. 406–415, 2012.

[9] D. E. 2006/42/CE, “Directive 2006/42/CE : 9.6.2006, Official Journal of the European Union, L157/24, Directive 2006/42/EC of the european parliament and of the council of 17 may 2006.” .

[10] J. Hoyos-Ruiz, J. F. Martínez-Cadavid, G. Osorio-Gómez, and R. Mejía-Gutiérrez, “Implementation of ergonomic aspects throughout the engineering design process: human-artefact-context analysis,” *Int. J. Interact. Des. Manuf.*, vol. 11, no. 2, pp. 263–277, 2017.

[11] R. Ghemraoui, L. Mathieu, and N. Tricot, “Design method for systematic safety integration,” *CIRP Ann.*, vol. 58, no. 1, pp. 161–164, 2009.

[12] M. Remiel , P. Martin, B. Daille-Lefevre, A. Etienne, J. Marsot, and A. Siadat, “Safety of machinery: requirement specification based on functional need and work situations analysis,” 2017.

[13] N. de Galvez, J. Marsot, P. Martin, A. Siadat, and A. Etienne, “EZID: A new approach to hazard identification during the design process by analysing energy transfers,” *Saf. Sci.*, vol. 95, pp. 1–14, 2017.

[14] P. Martin *et al.*, “New issues for workers safety in the factory of the future,” in *Advances on Mechanics, Design Engineering and Manufacturing II*, Springer, 2019, pp. 402–411.

[15] Legifrance, “Laborcode.” [Online]. Available: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000029336807/2021-04-16/.

[16] H. Sun, R. Houssin, J. Renaud, and M. Gardoni, “A review of methodologies for integrating human factors and ergonomics in engineering design,” *Int. J. Prod. Res.*, vol. 57, no. 15–16, pp. 4961–4976, 2019.

[17] L. Sadeghi, J. Y. Dantan, A. Siadat, and J. Marsot, “Design for human safety in manufacturing systems: applications of design theories, methodologies, tools and techniques,” *J. Eng. Des.*, vol. 27, no. 12, pp. 844–877, 2016, doi: 10.1080/09544828.2016.1235262.

[18] D. McRuer, “Human dynamics in man-machine systems,” *Automatica*, vol. 16, no. 3, pp. 237–253, 1980.

[19] J. Redström, “Towards user design? On the shift from object to user as the subject of design,” *Des. Stud.*, vol. 27, no. 2, pp. 123–139, 2006.

[20] H. Sun, R. Houssin, M. Gardoni, and F. de Bauvrond, “Integration of user behaviour and product behaviour during the design phase: Software for behavioural design approach,” *Int. J. Ind. Ergon.*, vol. 43, no. 1, pp. 100–114, 2013.

[21] D. A. Norman, *The psychology of everyday things.* Basic books, 1988.

[22] R. Houssin and M. Gardoni, “Software framework for the approach: computer aided Safety integration in design process (CASID),” *J. Adv. Manuf. Syst.*, vol. 8, no. 01, pp. 27–45, 2009.

[23] R. Hasan, A. Bernard, J. Ciccotelli, and P. Martin,. "Integrating safety into the design process: elements and concepts relative to the working situation." *Safety science.*, 41(2-3), 155-179 (2003).

[24] R. Houssin, A. Bernard, P. Martin, G. Ris, and F. Cherrier, “Information system based on a working situation model for a new design approach in concurrent engineering,” *J. Eng. Des.*, vol. 17, no. 1, pp. 35–54, 2006, [Online]. Available: http://www.tandfonline.com/doi/full/10.1080/09544820500276048#.VEkqLRbXy8w.