Complex Risk Predictions and Analyses of Designed Technical Product

Josef Dvořák(✉) and Stanislav Hosnedl

University of West Bohemia, Univerzitní 8, 301 00 Plzeň, Czech Republic
dvorakj@kks.zcu.cz

Abstract. There exist a lot of engineering design methodologies, methods and/or tools implemented in guidelines and standards which help engineering designers to reduce constructional, safety, environmental, etc. risks of designed and/or existing technical products. However, their common feature is especially high dependence on specialized experience of their users, time consuming, and their mutual both conceptual and terminological inconsistency resulting in very difficult compatibility with engineering designing itself. Our research has been therefore focused on risk predictions and analyses as complementary assisting processes when designing tangible technical products. Engineering Design Science and Methodology (EDSM), especially its core part Theory of Technical Systems (TTS), are being used as a basis for the developing comprehensive theory and methodology aiming at rationalization of the mentioned activities including their SW supports to achieve higher risk robustness of the designed technical products considered as Technical systems (TS).

Keywords: Risk · EDSM · Theory of Technical Systems · Methodology

1 Introduction

Based on search of professional literature, the experiences of authors in cooperation with industrial practice and consultations with colleagues in the field of design engineering, it turned out that the prediction and risk analyses of TS is an area that is still underestimated not only in the Czech Republic. Risk predictions and analyses of TS are hardly performed in domestic manufacturing companies (with the exception of the automotive industry in particular) and if so, engineering designers are very rarely used and these activities are processed only formally without almost any expectation of their benefits. It is very difficult for the engineering designers to orientate himself in the field of prediction and risk analysis of TS, most of them do not know any methods of prediction and risk analysis of TS and if so, they cannot use it correctly and effectively.

2 Theoretical Background

A number of strategic procedures for methodological support of the design solution of technical products (hereinafter referred to as technical systems - TS) are individually published in the professional literature, individually hierarchically divided into design

J. Homišin et al. (Eds.): ICMD 2020, AHE 17, pp. 215–226, 2023.
https://doi.org/10.2991/978-94-6463-182-1_23

phases and operations. Because of historical and many other reasons, these methodologies have different names. In the complex concept of Engineering Design Science and Methodology (EDSM) [1, 2], they are called as models of the design process, the best known of which are especially [3–5] etc., or also as guidelines, e.g., [14]. These have practically exclusively instructive character based on a systematic description of design processes and their parts. However, models of the design process need to be evaluated by the level of knowledge support. Therefore, the general design process (GMPD) EDSM based on the theory of technical systems (TTS), especially Theory of properties and structures of TS and the Theory of the design process, has proven to be the most effective in the current time. As a result, this model of the process is systematic, transparent, open and compatible (usually after the necessary terminological harmonization) with the other models of the design process (at all levels of knowledge support, including the completely intuitive and purely heuristic) which brings significant, otherwise unrealizable synergistic effects. When solving a specific design task, the GMPD concretizes itself in the plan of progress according to the design situation and finally to the individual way of proceeding according to the personal characteristics, knowledge and experience of a particular designer [1, 2]. Nevertheless, the resulting documentation of TS design proposals, thanks to GMPD based on EDSM, still has the same structure, which is the basis of hitherto unrealizable naturally updated databases for knowledge management of the development of other TSs.

2.1 Theory of Technical Systems in Engineering Design Science and Methodology

The aim of EDSM is systematic organization of theoretical and methodological knowledge about TSs and of design engineering of it for research, education and practice. The aim of EDSM is to provide a comprehensive systematic overview, "map", knowledge and methods of objects, processes and their relationships that affect the design process. In this paper the synergy effects between EDSM and theory of risk and its prediction and analyses is shown. “Maps” of knowledge based on EDSM can be used in appropriate application for the basis of knowledge management of the company. EDSM therefore allows, within the limits of the given possibilities:

- To get familiarize with rational knowledge and methods for construction and to use and further develop them creatively and effectively;
- To predict and analyze „emergency“ situations. i.e. risk events/situations (Fig. 1).

The basic structure, the “map” of EDSM knowledge (Fig. 2) is divided into four basic areas:

- Theory of technical systems to structures (s) – TTSs;
- Theory of technical systems for processes (p) – TTSp;
- Theory of structural systems) to structures (s) – TdesS;
- Theory of structural systems for processes (p) – TDesP and Methodology of structural process – MDesP.

The mentioned concept of EDSM presented in [1] is a significant complexity and logical interconnection of theoretical and methodological knowledge about and for design

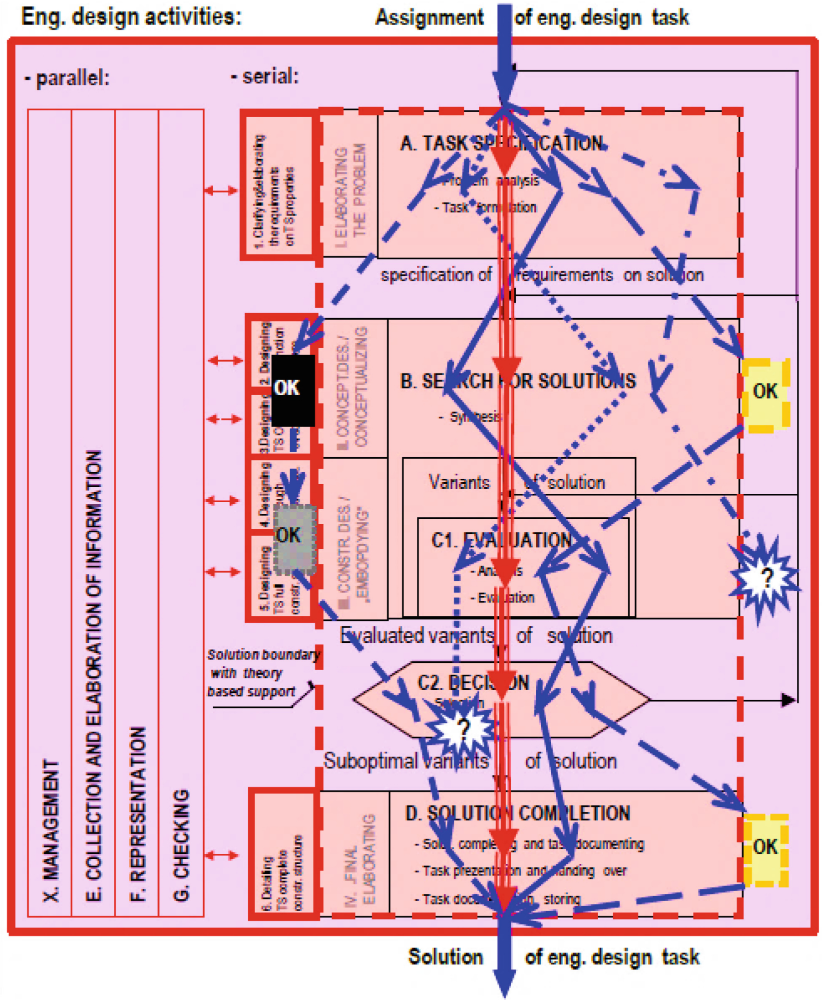
Eng. design activities:
Assignment of eng. design task
- parallel:
- serial:
X. MANAGEMENT
E. COLLECTION AND ELABORATION OF INFORMATION
F. REPRESENTATION
G. CHECKING
1. Clarifying&elaborating the requirements on TS properties
2. Designing
3.Designing TS
4. Designing
5.Designing TS full constr.
6. Detailing TS complete constr. structure
OK
OK
OK
OK
?
?
I. ELABORATING THE PROBLEM
II. CONCEPT.DES./ CONCEPTUALIZING
III. CONSTR. DES./ „EMBODYING"
IV. „FINAL ELABORATING
A. TASK SPECIFICATION
- Problem analysis
- Task formulation
specification of requirements on solution
B. SEARCH FOR SOLUTIONS
- Synthesis
Variants of solution
C1. EVALUATION
- Analysis
- Evaluation
Evaluated variants of solution
C2. DECISION
Selection
Suboptimal variants of solution
D. SOLUTION COMPLETION
- Solution completing and task documenting
- Task prezentation and handing over
- Task documentation storing
Solution boundary with theory based support
Solution of eng. design task

Fig. 1. Principle of the theory based strategy of the TS design engineering within the EDSM "map of the real word" - in the case of the EDSM based knowledge support where risk prediction and analyses are considered to be part of parallel processes (See G. Checking) [6])

engineering, including external links to other processes falling into integrated TS development. This logical interconnection is also supported by terminological interconnection (in Czech, English and German). Other known world "schools" such as Design theory and methodology (DTM) are focused only on partial areas of EDSM, especially in the area of instructive methodological procedures in design (incl. VDI 2221, BS 7000 and others), i.e. only the methodological part of the content (upper right) "quadrant" (MDesP). This reduces their complexity and thus, unlike EDSM, their compatibility with both theoretical and practical knowledge and methods at all levels of knowledge design support.

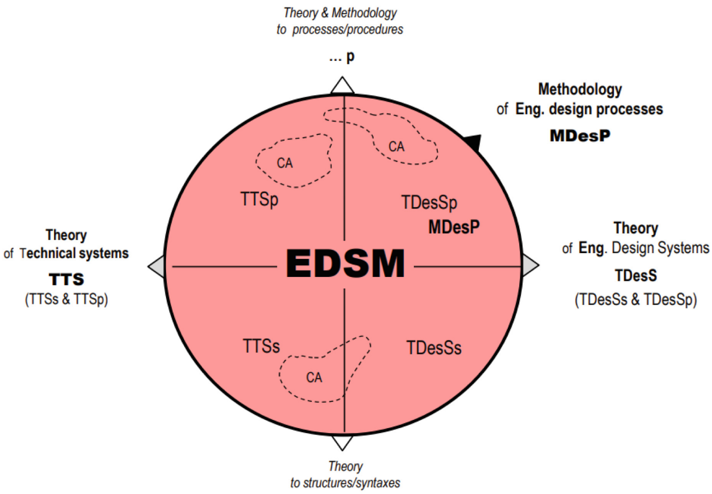

Fig. 2. Basic Structure of Topic "map" of EDSM based on the TTS incl. Illustrative representation of its computer supported (CA) areas, which are its integral parts [1]

2.2 Technical Product in TTS

The success of manufacturing companies in a highly competitive globalized market is determined, among other things, by the technical products that the company offers on the market. In the engineering industry, we mainly refer to them as technical products. The product according to [7] is the output of the organization (i.e. the result of the process as a set of interrelated or interacting activities that transform inputs into outputs). An example of such a product can be a book, computer software, pastries, etc. TS is a product with a dominant engineering content [2]. An example of TS can be a machine tool, vehicle, mobile phone, etc. In EDSM terminology, technical product is understood as a technical system (TS) in all its intangible and tangible forms occurring in the stages of its life cycle (LC TS(s)) [6].

2.3 General Model of Transformation System

The basic theoretical structure, which is based on the Theory of Technical Systems to Structures [Hubka & Eder 1988, etc.] is a model of an (artificial) transformation system (TrfS) with a transformation process (TrfP), see Fig. 3. This model generally expresses that each activity (e.g. technological operation Tg) is a transformation of a transformed object, marked as OPERAND in a certain input state to OPERAND in a desired state at its output, which is achieved by direct or mediated by the effects of OPERATORS, i.e. the effects of Humans (HuS), Technical Systems (TS), Active and Reactive Environment (AREnv), Information Systems (IS) and Management Systems (MgtS) on the transformed OPERAND.

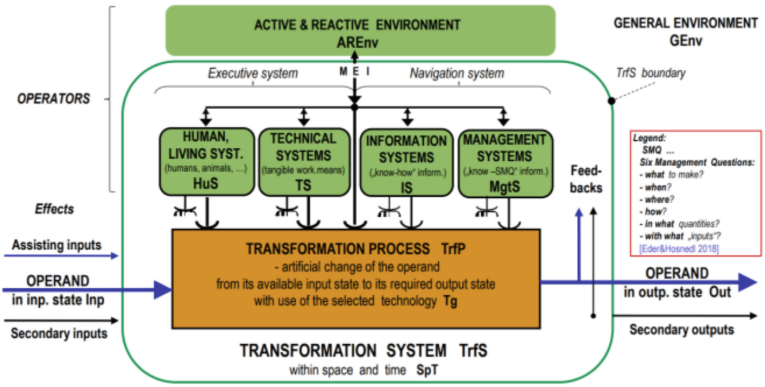

Fig. 3. General Model of Transformation system with Transformation process [1, 2, 8]

2.4 TS Life Cycle

TS Life Cycle (LC) structuring can be performed according to various aspects (e.g. according to the place of implementation, according to development phases, or cost aspects, sales phases on the market, etc.), but for the needs of designing of TSs their distribution according to dominant transformations - transformation processes (TrfP) [6]. Using the general model of the transformation system (TrfS) (Fig. 2) with its transformation process (TrfP), a general model of the life cycle of a technical product can be illustrated [1]. The individual stages of the general life cycle of TS are modeled by a serial arrangement of individual stages expressed using these models.

TS life cycle is shown in Fig. 4, is distinguished by index (s) from other technical systems in individual stages. TS (s) is in the initial phase in the form of information (dashed flows), starting with production it is transformed into a material / material form (full flows). TS (s) has mainly the function of an operand, but in the operational /working phase it becomes an operator (with the exception of assisting maintenance and repair processes, when it temporarily becomes an operand). The resulting TS must meet all the requirements for its properties in terms of the entire product life cycle (from planning to disposal) [6].

However, it can be shown that the life cycle model of a technical system such as the TrfP series and the corresponding TTS-based TrfS (Fig. 4) can be considered as a suboptimal life cycle model, due to the fact that in life cycle models from the managerial point of view or from the point of view of environmental management, for example, the life stage of Technological preparation of production (and processes in the next stages of LC!) is completely missing. In the managerial concept [9], for example, a technical product is practically not mentioned at all. Also in the model the stages of Technological preparation of production and other processes in the next stages of LC and the planning stage are fundamentally missing. CA models of LC (e.g. PLM), for example, do not consider the stage of distribution, planning or technological preparation of production and other processes and stages of LC. As already indicated above, for the needs of designing of TS, the optimal division of its life stages according to all key "life" Transformation Processes (transformations) is optimal. All stages of the life cycle then

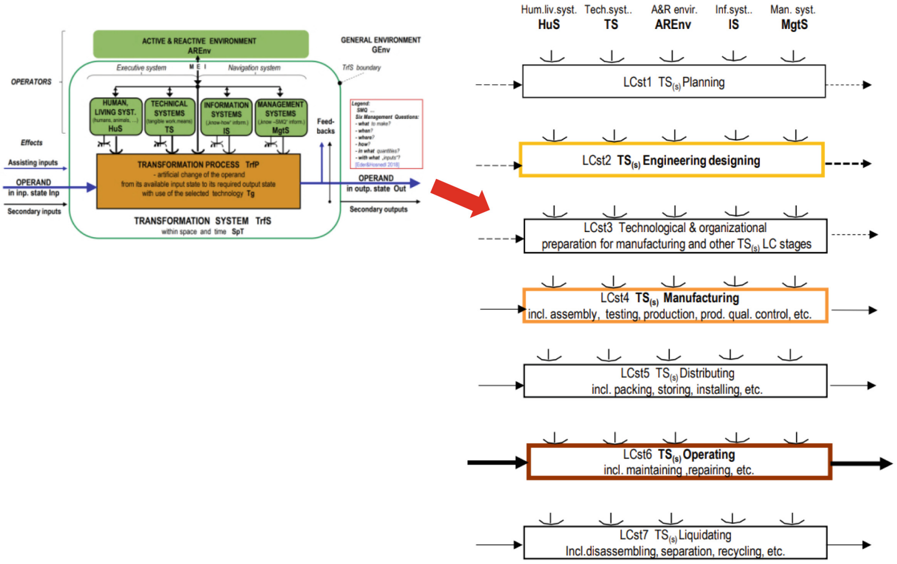
ACTIVE & REACTIVE ENVIRONMENT AREnv
GENERAL ENVIRONMENT GEnv
OPERATORS
Executive system
M E I
Navigation system
TrfS boundary
HUMAN, LIVING SYST. (humans, animals, ...) HuS
TECHNICAL SYSTEMS (tangible work means) TS
INFORMATION SYSTEMS ('know-how' inform.) IS
MANAGEMENT SYSTEMS ('know –SMQ' inform.) MgtS
Feed-backs
Legend: SMQ ... Six Management Questions: - what to make? - when? - where? - how? - in what quantities? - with what 'inputs'? [Eder&Hosnedl 2018]
Effects
Assisting inputs
OPERAND in inp. state Inp
Secondary inputs
TRANSFORMATION PROCESS TrfP - artificial change of the operand from its available input state to its required output state with use of the selected technology Tg
OPERAND in outp. state Out
Secondary outputs
TRANSFORMATION SYSTEM TrfS within space and time SpT
Hum.liv.syst. HuS
Tech.syst.. TS
A&R envir. AREnv
Inf.syst.. IS
Man. syst. MgtS
LCst1 TS(s) Planning
LCst2 TS(s) Engineering designing
LCst3 Technological & organizational preparation for manufacturing and other TS(s) LC stages
LCst4 TS(s) Manufacturing incl. assembly, testing, production, prod. qual. control, etc.
LCst5 TS(s) Distributing incl. packing, storing, installing, etc.
LCst6 TS(s) Operating incl. maintaining ,repairing, etc.
LCst7 TS(s) Liquidating Incl.disassembling, separation, recycling, etc.

Fig. 4. TS(s) Life cycle stages as a sequence of the key transformation processes (TrfP) and respective transformation systems (TrfS) [1, 6, 8]

have a completely identical structure (Fig. 4) of the Transformation System [6]. This LC TS (s) model is therefore a comprehensive and consistent system, which none of the other available (mostly process) life cycle concepts found allows.

2.5 Theory of Risks

According to [10, 11] and others, the risk can be seen as a combination of the severity of a possible failure and the probability of this damage occurring during a specified hazardous event within the investigated TS. The risk is defined according to the following relationship:

$$R = S.P \tag{1}$$

where:

R = risk.
S = a dimensionless number that classifies the severity, i.e. an estimate of how strongly the consequences of the failure will affect the system or the user.
P = a dimensionless number that indicates the probability of failure.

The most common general methods of TS risk prediction and analysis being used TS in particular are:

FMEA - Failure Mode and Effects Analysis
WI - What if Analysis
FTA - Fault Tree Analysis

ETA - Event Tree Analysis
CCA - Cause and consequences analysis
SR - Safety Review
HAZOP - Hazard and operability study
HRA - Human reliability analysis
CL - Checklists
PHA - Preliminary hazard analyzes
RR - Relative Ranking

3 Complex Risk Prediction and Analyses Methodology

The term risk is here in the proposed methodology replaced by a more concise and general term risk event/situation - R|E/S| taken from [ČSN ISO EN 12100, 2011]). From the analysis of the generalized TS EDSM life cycle model (Fig. 4), mainly thanks to its systematic structure, it transparently shows that the carrier(s) of R|E/S|. In general, the following can be the following typical Object (sub) systems (ObjS):

3.1 Object System

From analysis of the generalized TS EDSM life cycle model (Fig. 4) with proven systematic structure, it transparently shows that the carrier of R|E/S| in general, could be the following typical Object (sub) systems (ObjS):

- assessed TS (s) (i.e. reliability of TS (s) in its whole LC of TS(s), which is in professional publications, including standards, often erroneously referred to “only” as reliability, moreover only with implicit or even explicit focus only on operation TS (s)).
- TS (s) & ∑Human/Living Being Systems assessed (i.e. safety of TS (s) for humans and other living beings throughout the life cycle of TS (s)), which is often incorrectly labeled in the professional publications, including standards, “only “as safety against injury/death during the operation of TS (s), moreover only with an implicit or even explicit focus only on the operation of TS (s)).
- assessed TS (s) & ∑other TS (i.e. safety of TS (s) for other tangible work equipment in the whole life cycle of TS (s), which is not mentioned in professional publications, incl. Standards etc.)
- assessed TS (s) & ∑Environment (i.e. safety of TS (s) for working, natural and space environment in the whole life cycle of TS (s), which is mentioned in professional publications, including standards, but very unsystematically).
- assessed TS (s) & ∑Information systems (i.e. security of TS (s) for information systems in the whole life cycle of TS (s), which is mentioned in professional publications, including standards, very unsystematically, mainly only with a focus on cybersecurity etc.)
- assessed TS (s) & ∑Management systems (i.e. safety of TS (s) for management systems in the whole life cycle of TS (s), which is mentioned in professional publications, including standards, very unsystematically, mostly only with a focus on strategic organization management), see Fig. 5, 6, 7.

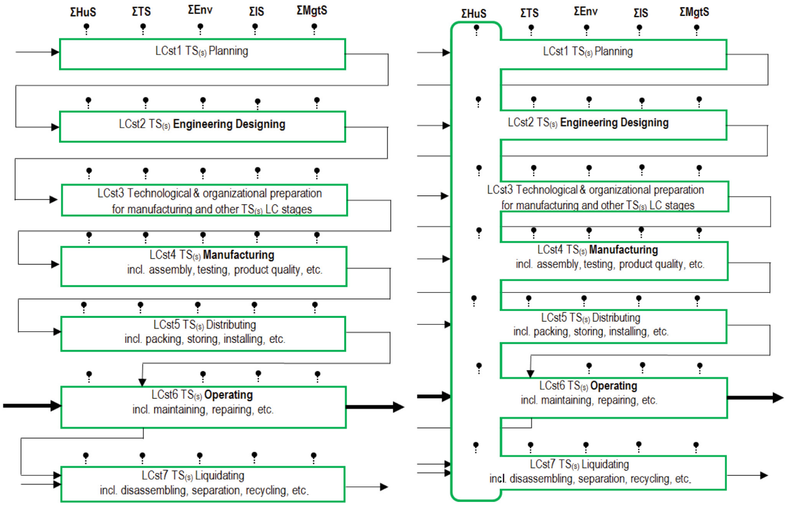
ΣHuS
ΣTS
ΣEnv
ΣIS
ΣMgtS
LCst1 TS(s) Planning
LCst2 TS(s) Engineering Designing
LCst3 Technological & organizational preparation for manufacturing and other TS(s) LC stages
LCst4 TS(s) Manufacturing incl. assembly, testing, product quality, etc.
LCst5 TS(s) Distributing incl. packing, storing, installing, etc.
LCst6 TS(s) Operating incl. maintaining, repairing, etc.
LCst7 TS(s) Liquidating incl. disassembling, separation, recycling, etc.
ΣHuS
ΣTS
ΣEnv
ΣIS
ΣMgtS
LCst1 TS(s) Planning
LCst2 TS(s) Engineering Designing
LCst3 Technological & organizational preparation for manufacturing and other TS(s) LC stages
LCst4 TS(s) Manufacturing incl. assembly, testing, product quality, etc.
LCst5 TS(s) Distributing incl. packing, storing, installing, etc.
LCst6 TS(s) Operating incl. maintaining, repairing, etc.
LCst7 TS(s) Liquidating incl. disassembling, separation, recycling, etc.

Fig. 5. EDSM based knowledge "maps" for R|E/S| identification in the LC stages of TS (s) for Object Systems) TS (s) (left), TS (s) & ∑HuS (right) (part I of III)

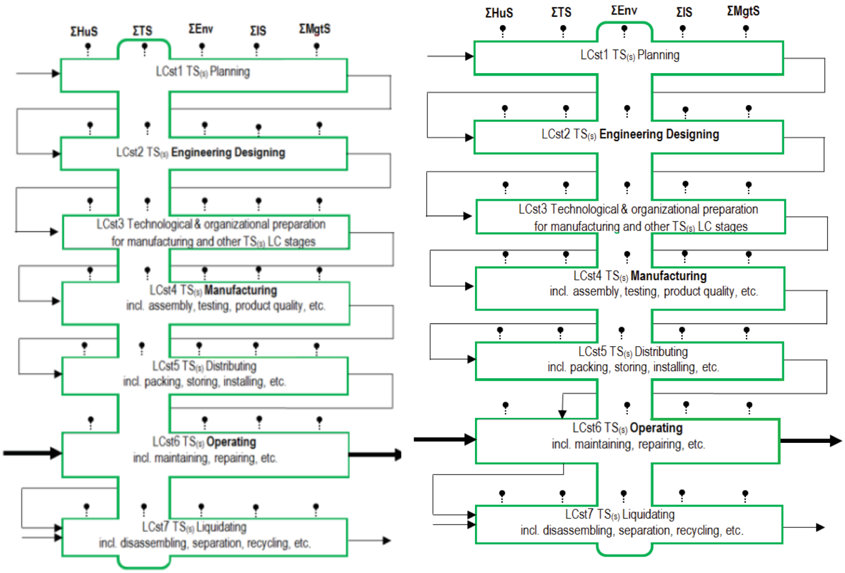
ΣHuS
ΣTS
ΣEnv
ΣIS
ΣMgtS
LCst1 TS(s) Planning
LCst2 TS(s) Engineering Designing
LCst3 Technological & organizational preparation for manufacturing and other TS(s) LC stages
LCst4 TS(s) Manufacturing incl. assembly, testing, product quality, etc.
LCst5 TS(s) Distributing incl. packing, storing, installing, etc.
LCst6 TS(s) Operating incl. maintaining, repairing, etc.
LCst7 TS(s) Liquidating incl. disassembling, separation, recycling, etc.
ΣHuS
ΣTS
ΣEnv
ΣIS
ΣMgtS
LCst1 TS(s) Planning
LCst2 TS(s) Engineering Designing
LCst3 Technological & organizational preparation for manufacturing and other TS(s) LC stages
LCst4 TS(s) Manufacturing incl. assembly, testing, product quality, etc.
LCst5 TS(s) Distributing incl. packing, storing, installing, etc.
LCst6 TS(s) Operating incl. maintaining, repairing, etc.
LCst7 TS(s) Liquidating incl. disassembling, separation, recycling, etc.

Fig. 6. EDSM based knowledge "maps" for R|E/S| identification in the LC stages of TS (s) for Object Systems and TS (s) & ∑TS (left), TS (s) & ∑Env (part II of III)

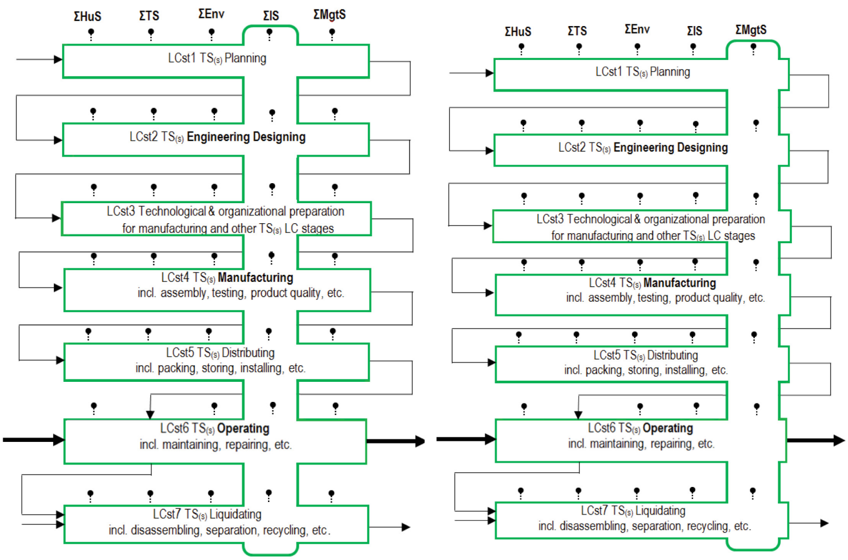
ΣHuS
ΣTS
ΣEnv
ΣIS
ΣMgtS
LCst1 TS(s) Planning
LCst2 TS(s) Engineering Designing
LCst3 Technological & organizational preparation for manufacturing and other TS(s) LC stages
LCst4 TS(s) Manufacturing incl. assembly, testing, product quality, etc.
LCst5 TS(s) Distributing incl. packing, storing, installing, etc.
LCst6 TS(s) Operating incl. maintaining, repairing, etc.
LCst7 TS(s) Liquidating incl. disassembling, separation, recycling, etc.
ΣHuS
ΣTS
ΣEnv
ΣIS
ΣMgtS
LCst1 TS(s) Planning
LCst2 TS(s) Engineering Designing
LCst3 Technological & organizational preparation for manufacturing and other TS(s) LC stages
LCst4 TS(s) Manufacturing incl. assembly, testing, product quality, etc.
LCst5 TS(s) Distributing incl. packing, storing, installing, etc.
LCst6 TS(s) Operating incl. maintaining, repairing, etc.
LCst7 TS(s) Liquidating incl. disassembling, separation, recycling, etc.

Fig. 7. EDSM based knowledge "maps" for R|E/S| identification in the LC stages of TS (s) for Object Systems and TS (s) & ∑IS (left), TS (s) & ∑MgtS (part III of III)

3.2 Relation of Basic Methodologies for Risk Prediction Analysis of Reliability and Safety of TS (s) with Proposed Theory and Methodology of Complex Risk Prediction and Analysis

Using the generalized LC TS (s) model (Fig. 4), in which the carrier R|E/S| can be identified, when reliability is predicted and analyzed, the object system Obj(s) consists of the assessed TS. The complementary system for prediction and analysis of reliability of TS (s) then consists of all generalized operators ∑HuS, ∑TS, ∑Env, ∑IS and ∑MgtS. For TS (s) safety prediction and analysis, Obj(s) consists of the technical system (TS (s)) & ∑ Human/Living Being Systems i.e. (TS (s) & ∑HuS). From the mutual comparison of areas of knowledge support identification R|E/S| according to EDSM and specific normative methods according to [16], it is obvious that these specific methods, which are not supported by EDSM knowledge, covers only partial areas of EDSM knowledge support used in the proposed comprehensive methodology of prediction and analyses of R|E/S| (see Fig. 8). The examples of successful use of proposed methodology were already published in [12] or [13].

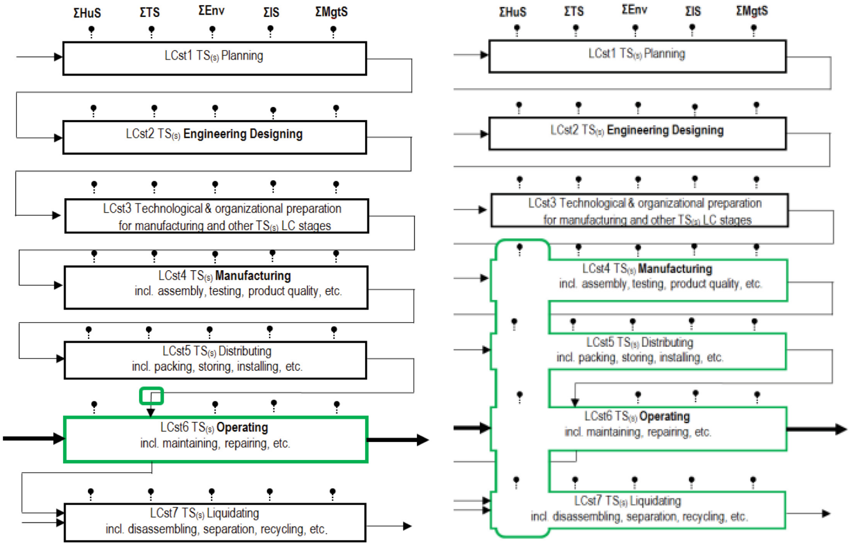
ΣHuS
ΣTS
ΣEnv
ΣIS
ΣMgtS
LCst1 TS(s) Planning
LCst2 TS(s) Engineering Designing
LCst3 Technological & organizational preparation for manufacturing and other TS(s) LC stages
LCst4 TS(s) Manufacturing incl. assembly, testing, product quality, etc.
LCst5 TS(s) Distributing incl. packing, storing, installing, etc.
LCst6 TS(s) Operating incl. maintaining, repairing, etc.
LCst7 TS(s) Liquidating incl. disassembling, separation, recycling, etc.

Fig. 8. Knowledge "maps" of normative methods of risk prediction and analyses and its carriers R|E/S|: TS (s) (reliability) in connection with [15] (left) and TS (s) & ∑HuS (safety) in connection with [16] (right)

4 Conclusions

Presented methodology serves as a support tool for designers and employees of related engineering professions, who can comprehensively or even partially use it as feedback and control of their design activities and use this knowledge in building their own "knowledge map", which each designer creates during their practice. It offers designers the opportunity to use it as an effective tool for building own portfolio of knowledge, for experienced (so-called senior designers) the methodology can offer a different "perspective" on predicting the risks of technical products and confirming or refuting their routine approaches [1].

The above presented methodology allows to perform risk prediction and analysis for object systems TS(s), TS(s) & ∑HuS, TS (s) & ∑TS, TS (s) & ∑Env, TS (s) & ∑IS and TS (s) & ∑MgtS in all considered stages of the LC of the designed TS or even existing TS. Methodology also performs risk prediction and analyses of failure mode analysis for object systems TS(s) with connection to [ČSN EN 60812, 2007], and performs also prediction and analysis of safety for object systems TS (s) & ∑HuS with connection to [16] but in all considered stages of the life cycle of the TS. It is also possible to perform identification of all R|E/S|: for object systems TS (s), TS (s) & ∑HuS, TS (s) & ∑TS, TS (s) & ∑Env, TS (s) & ∑IS and TS (s) & ∑MgtS actually or potentially caused by multiple causes in all LC stages of the TS. This methodology also include to determine the degree of risk all available risk factors used for risk prediction and analyses appeared in available methods of risk prediction and analyses of reliability, safety and of prediction of environmental risks.

References

1. Hubka, V., Eder, W.E: Theory of Technical Systems. Berlin Heidelberg: Springer - Verlag, 1988, (2. vyd. něm. 1984) ISBN 3–540–17451–6
2. Eder, W. E., Hosnedl, S.: Introduction to Design Engineering: Systematic Creativity and Management. CRC Press / Balkema, Taylor & Francis Group, Leiden, The Netherlands, 2010, ISBN: 978-0-415-55557-9
3. Pahl, G., Beitz, W.: Engineering Design, A Systematic Approach. London: Springer, 1995. ISBN 3-540-19917-9
4. Roth, K.: Konstruieren mit Konstruktionskatalogen, Berlin Heidelberg: Springer-Verlag, 1994. ISBN 3-540-57324-0 (Band 1), ISBN 3-3540-57656-8
5. Roozenburg, N. F. M., Eekels J.: Product Design: Fundamentals and Methods. Chichester, UK: Wiley, 1995, ISBN 0-471-94351-7
6. Hosnedl, S.: Systémové navrhování technických produktů KKS/ZKM. Lectures in Power Pointu. Plzeň: ZČU, KKS, 2019
7. ČSN EN ISO 9000, 2006, Quality management systems - Fundamentals and vocabulary. Prague: Czech Normalization institute, 2006
8. Eder, W. E., Hosnedl, S.: Design Engineering, A Manual for Enhanced Creativity. CRC Press, Taylor & Franciss Group, Boca Raton, Florida USA 2008, 600 s., ISBN 978–1–4200–4765–3
9. Tomek, G.,Vávrová, V.: Product and its success on the market. Praha: Grada Publishing, a.s.. ISBN 80–247–0053–0
10. Marek, J., Blecha, P., Hlinovský, J. (in memoriam), Krčálová, E. a Mareček, J.: Management rizik výrobních strojů: MM Průmyslové spektrum, 2009, ISSN 1212–2572
11. Ramroth, W. G.:Risk Management for Design Professionals. New York: Kaplan Publishing, 2007, ISBN 978-1-4277-5476-9
12. Dvořák, J.: *Methodological Support for Risk Analysis during the Whole Life Cycle When Designing Technical Products.* In: Proceedings of The 30th International Business Information Management Association Conference: Innovation Vision 2020, 2017, p. 4642 - 4650, ISBN: 978–0–9860419–9–0
13. Dvořák, J, Teplý, R.: *Complex risk analyses of the cable winder*. In: Proceedings of The 32nd International Business Information Management Association Conference: Innovation Vision 2020: Suistanable Economic development an Application of Innovation Management, 2018, p. 5753 - 5759, ISBN 978–0–9998551–1–9
14. BS7000:1989: Guide to managing product design. London, UK: 1989
15. ČSN EN 60812, 2007 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA). Praha: Czech normalization institute, 2007
16. ČSN EN ISO 12100, 2011 Safety of machinery - General principles for design - Risk assessment and risk reduction. Prague: Czech Normalization institute, 2000
17. Hubka,V., Eder, W. E.: Design Science. London, Springer, 1996, ISBN 3-540-19997-7