Modelling of Resilient Coping Strategies within the Framework of the Resilience Design Methodology for Load-Carrying Systems in Mechanical Engineering

Fiona Schulte^(✉), Hermann Kloberdanz, and Eckhard Kirchner

Darmstadt University of Technology, Darmstadt, Germany
schulte@pmd.tu-darmstadt.de

Abstract. During the development of load-carrying systems uncertainty caused by nescience can be handled applying resilience design. With this systematic approach, in addition to robust design, resilient system properties can be achieved. The resilience design methodology comprises new and extended models and methods. The central aspect of resilient properties is an adaptivity of the system. The procedure for resilience design starts with choosing a ‘general coping strategy’ appropriate for the design task. Based on this, a more detailed ‘system coping strategy’ is developed. This concrete strategy is based on the resilience functions responding, monitoring, anticipating and learning. The coping strategies always contain the function ‘responding’ because it represents the actual adaption of the system. The central, most abstract synthesis model for developing robust and resilient systems is the functional structure model. In this model the system functions and their interconnection by signals, material and energy flows are depicted. However, the realisation of resilience properties requires additional signals and flows. Hitherto, the functional structure for robust systems is static, whereas adaptivity requires flexible control of functions and flows. Therefore, an extension of the functional structure model is proposed to be able to depict the resilient system coping strategy and adaptivity. Within the resilient system the coping strategy is depicted by adaption functions based on the four resilience functions. Via an introduced interface and an enabler-structure the adaption functions are connected to the robust functional structure. The application of the proposed extension is illustrated by the example of a by-wire car brake system.

Keywords: Resilience design · Functional structure · Adaptivity

1 Introduction

The concept of resilience is known from living organisms and socioeconomic systems. It is based on the efficient use of resources. Living organisms are compelled to get by with limited resources and thus cannot be resistant to any kind of disruption, like injuries, because this would require excessive access to resources. Hence, robustness only evolved for common events, while for seldom extreme situations natural organisms

evolutionary developed the ability to continue living with a reduced capability, adapt to lasting condition changes and recover from disruptions. Therefore, efficient strategies to cope with disruptions have evolved. Human beings, e.g., suffer from severe symptoms during influenza illnesses but do survive and fully recover [1].

Resilience offers potential for technical systems, too. Accepting, that a technical system cannot be robust, i.e. able to withstand, towards all disruptions, resilient behaviour in load-carrying systems would guarantee essential system functions, while non-substantial functions may fail. Furthermore, the system would be able to recover, when disruptions decline, as defined by the Collaborative Research Centre 805 for resilience in load-carrying systems [2]. In contrast to natural organisms for technical systems coping strategies to achieve resilient behaviour have to be planned during the development process. The general strategies are similar to natural coping strategies [1].

A high potential is estimated for highly safety relevant systems like, e.g., car brake systems [3] and upon occurrence of unknown or neglected uncertainty. Events addressing uncertainty caused by nescience, that are expected to cause severe disruptions, which cannot be covered by the system's robustness, are presumed. The objective of realising resilience in load-carrying systems is to deal with those severe disruptions and prevent risks due to complete system failures. In this context resilience also offers economic potential. Disruptions, that are neglected during the robust design process, because of too high economical effort regarding resources and considering the low exposure to the disruption, can be addressed using the resilience concept [1, 3].

2 Fundamentals

Based on resilience theories from other fields of research, basics for resilience engineering have been devised. However, to be able to realise resilient technical systems, related fields of research have to be considered, too. In case of load-carrying systems the vulnerability analysis can serve as a support for resilience engineering by pointing out the system's weaknesses and focusing on the crucial influences regarding resilient properties. Thus, vulnerability is understood as a partially complementing approach to resilience, here. Similarly, resilience design is understood as an extension of robust design. A robust system is even comprehended as a prerequisite for resilience design. Thus, also robust design and its methodologies in general as well as the inherent robust properties of a technical system have to be taken into account. In a resilience design methodology for developing comprehensive resilience concepts for load-carrying systems, robustness, vulnerability and resilient properties as well as their close interrelation have to be embedded.

2.1 Resilience

Resilience in technical systems describes the system's ability to "[...] guarantee [...] a predetermined minimum of functional performance even in the event of disturbances or failure of system components, and a subsequent possibility of recovering at least the set point function [2]." As mentioned above resilience design is understood as an extension

of the robust design methodology. While a robust system is designed to withstand disturbances in a predefined range of the influencing parameters without significant reduction in its functionality, resilience design aims at mastering disruptions, like extreme variations of the influencing parameters. To address disruptions beyond those handled by robust design, a resilient system adapts to the disturbed conditions and accepts a reduction of the functionality, as long as the essential minimum functional performance is still provided. Consequently, robust design is applied for known uncertainty in a system, while resilience allows to handle disruptions beyond the common and well known range of the influencing parameters. Resilience Design therefore comprises adjusted methods of robust design and particular new models, procedures and methods.

For analysing a system's resilience properties a resilience application model has been developed [4]. It comprises the resilient behaviour of a technical system, which is depicted by the progression of the system's functional performance over time, showing the system's reaction to a disruption. To describe the system completely, it is also required to look at the static resilience characteristics and related metrics that describe the functional performance depending on influencing parameters according to [2]. For resilience engineering the interdependency of the properties with the disruption progression and potential correlating signals are considered, additionally [4].

Furthermore, functional resilience characteristics, also referred to as resilience functions, allow to describe a system's resilient properties. The functional resilience characteristics [2, 5] are based on the four abilities of resilience Hollnagel [6] postulated: Responding, monitoring, anticipating and learning. To realise the characteristic learning in technical systems a human operator or an artificial intelligence system would be required. Since neither can be assumed in most technical systems, only responding, monitoring and anticipating are taken into account in the following [4]. The degree a system is able to apply the functional resilience characteristics to a disruption, provides information about the system's resilience level [6]. Simple systems only feature responding, which describes the system's reaction to disruptions, whereas more sophisticated systems are characterised by monitoring the disruption progression and correlating signals and anticipating of an upcoming disruption by interpreting the monitored data [4, 5].

2.2 Vulnerability

According to Turner et al. [7] vulnerability can be defined as “[...] the degree to which a system [...] is likely to experience harm due to exposure to a hazard [...]” [7]. To use the knowledge about the system's vulnerability, first it needs to be identified. One approach to do so, is a vulnerability analysis using the scenario technique [8–10]. With the scenario technique possible future situations are developed to assess the potential changes of conditions for the system. From these condition changes disruptions of the system, which could be either external disturbances or internal damages, can occur [11]. Afterwards, based on a system analysis the sensitivity of the system towards the disruptions is determined considering implemented measures or inherent abilities of the system to deal with certain disruptions leaving the critical disruptions [8, 12]. This identification of the system's weaknesses is requisite for resilience design because it provides information about the critical quantities, the system needs to be resilient towards.

2.3 Functional Structure Modelling

During the systematic product development process for robust systems one of the first steps is modelling the functional structure. In the functional structure all functions and the flows of energy, material and signals interconnecting them, which are required to realise the overall function of a system, are depicted. The use of functional structures improves the understanding of the system and its aspired operating principles and enables to derive the required subfunctions and flows, regardless of possible function carriers, before choosing the appropriate components and modules for their realisation [13].

3 Research Question

The concept of resilience in load-carrying systems is understood as an extension of robust system design. As the extension by resilient functionality requires a different mindset compared to robust design, for a systematic system development it is crucial to also extend the development methodologies [1]. For resiliently mastering extreme situations resilience characteristics and resilience behaviour have to be combined appropriately, which requires determining strategies that exceed design principles. The resilient reaction of a system to a disruption is described as *coping*. Hence, the basic characteristic of the system's reaction is defined as a *coping strategy*, here [14].

The identification of the critical system conditions caused by unknown influences or unexpected component failures are determinable using the vulnerability analysis. As soon as the crucial vulnerabilities are identified a *basic coping strategy* is required to deal with the disruption in case it occurs. The static and dynamic resilience properties, depicted in the resilience application model, are a first concretisation of the coping strategy. It can be further concretised based on the functional resilience characteristics as the *system coping strategy*. The obvious coping strategies known from natural organisms are mainly characterised by utilising signals, material and energy resources. Hence, to realise the coping strategy during the systematic product development process, modelling the system coping strategy in combination with the functional structure is essential, because the signal, material and energy flows are first described within the functional structure during the development process. As the coping strategies always require the functional resilience characteristic responding, they implicitly require a purposive system adaptivity [3, 15]. Thus, for the development of resilient load-carrying systems this adaptivity has to be modelled within the functional structure, which is not possible using the conventional functional structure model for robust design [3]. In this context the objective of this contribution is to answer the following research question.

- How to define basic resilient coping strategies as an extension of robust design and model the mandatory system adaptivity in functional structures for methodological development of resilient systems?

4 Modelling Resilient System Structures

During the product development process, including resilient system behaviour, first resilient requirements are deduced using the vulnerability analysis as described in

Sect. 2.2. The current as well as the aspired system properties are depictable in the resilience application model, which also enables to quantify the resilience requirements as shown in [3]. Afterwards, the deduction and formulation of the resilient coping strategy follow in two steps. First a suitable *basic coping strategy* for the whole system is identified. Thereafter, the realisation of the coping strategy is concretised as a *system coping strategy*. The system coping strategy is modelled in the functional system structure as an extension using *adaption functions* based on the functional resilience characteristics. The adaption functions are depicted outside the robust system boundary and connected to the robust subfunctions and flow parameters.

4.1 General and Basic Resilient Coping Strategies

Defining coping strategies different consideration horizons have to be taken into account. The robust system structure is assumed to be predetermined and located in the central position. It is describable by the conventional functional structure model. The resilient consideration horizon exceeds the robust system boundary and takes the superordinate system into account, as well, because in case of extreme disruptions resilient systems may rely on external resources as well as flexible functions. For some approaches of realising resilient design an even wider, so called extended, consideration horizon is applied. The extended consideration horizon additionally comprises the system environment and enables to identify threats and utilise resources from beyond the superordinate system boundary.

Three suitable *general coping strategies* based on nature have been identified for load-carrying systems, as a first exemplary result: internal/external degradation, usage of alternative internal/external resources and purposeful overload. The internal degradation looks at the robust system, wherein less important functions are switched off or reduced in performance to maintain full performance of essential functions. External degradation uses an extended consideration horizon, which also regards the superordinate system. The degradation then is executed outside the robust system boundary but safes, e.g., resources for the regarded subsystem. The usage of alternative internal or external resources allows the system to draw on resources, which are not originally intended to be used by this subsystem or function. Alternative external resources are available in the superordinate system or the environment and taken into account by the extended consideration horizon. The strategy of purposeful overload uses a certain subsystem or function, of which the demand increased overly, excessively, accepting a possible damage. The choice of a coping strategy depends on the system's requirements and properties, as well as the disrupted quantities. Exemplary assignments of general coping strategies for typical vulnerabilities are given in Table 1.

After choosing a suitable *general coping strategy*, it has to be substantiated with the characteristics required by the system to a *basic coping strategy*, which means, e.g. the used external resource is specified as energy. Afterwards, the *system coping strategy* has to be derived and modelled as a combination of the resilience functions. The simplest system coping strategy only includes the resilience function responding. Thus, the system reacts upon occurrence of a disruption. Enhanced resilience functionality can be attained by including the resilience functions monitoring and anticipating.

Table 1. Exemplary assignment of general coping strategies for typical vulnerabilities

Vulnerability	Applicable general coping strategies
Lack of resources	Usage of alternative resources Internal/external degradation: reduction of resource consumption within the system boundary/in the system's direct environment
Increased power/performance demand	Purposeful overload: partly accepting system damage Increased functionality: booster, change of function characteristic Usage of alternative resources

4.2 Modelling of Adaptivity for Resilient System Coping Strategies

After the system coping strategy is defined it has to be modelled in combination with the functional system structure. Therefore, new elements to depict the adaptivity of the system structure and function elements to model the coping strategy are required and have been developed exemplary [3]. This contribution shows how the interface between the system coping strategy, modelled by resilient and adaption functions, and the robust functional structure is complemented. The adaptivity is modelled using the enablers and disablers for functions, signals and flows shown in Table 2. The enablers are connected to the adaption functions. The adaption functions are based on the functional resilience characteristics and defined as ‘execute adaption’ as the functional element for responding, ‘gather data’ for monitoring and ‘interpret data’ for anticipating. In Table 3 their general functionality and exemplary design principles used for their realisation are listed. The adaption functions are depicted by a greyed out rhomboid and additionally required robust functions for the realisation of resilience (resilient functions) are represented by a greyed out cuboid as depicted in Fig. 1.

Table 2. Enabler elements

Designation	Representing element	
function enabler/disabler	<div>enable function </div>	<div>disable function </div>
signal enabler/disabler	<div>enable signal </div>	<div>disable signal </div>
flow enabler/disabler	<div>enable additional flow, enable flow </div>	<div>disable additional flow, disable flow </div>

Table 3. Adaption functions

Adaption function	Description	Design principles
Execute adaption	Adjusts system according to a new situation/condition	Physical/functional redundancy, fail-safe functionality
Gather data	Detects influencing parameters' values	Sensory functionality
Interpret data	Analyses gathered data and concludes which adaption to execute	Algorithms

Fig. 1. Depiction of a) adaption functions and b) resilient functions

5 Example of by-wire Car Brake System

The application of the extended functional structure model is discussed looking at a by-wire car brake system. The by-wire car brake system consists of an electronic unit, including the brake control system and the brake force amplifier, and a hydraulic unit, including the functions of building up and reducing the hydraulic braking pressure, and consequently the brake force to decelerate the wheel. The parking brake is included within the brake system's robust system boundary, too. The brake system is powered by the central board net, which is also connected to other consumers within the superordinate system, the car. The functional structure of the by-wire brake system is shown in Fig. 2 with the engine starter as one exemplary external consumer of the board net energy [3, 16].

Due to the many consumers connected to the board net, which, depending on their particular application, require high currents, and disturbances of the vehicle battery that arise, e.g., from low battery temperatures, a decrease of the power supply voltage can occur. The brake system is based on the electronic unit, which breaks down eventually as the power supply voltage decreases. Thus, the brake system's functionality is reduced to the hydraulic unit. The hydraulic unit then is controllable by the human operator via a hydraulic crackdown activated by muscular power [3]. This solution follows the fail-safe principle as it keeps up an option to brake, but the measure only applies when the disruption already occurred, no defined minimum functionality is guaranteed and the recovery time until full braking functionality is available again after the disruption's decline, is determined by the duration of the reboot of the electronic unit [3, 16].

As the full functionality of the brake system is aspired to be available at any time the relatively long recovery time of over two seconds is considered as the crucial vulnerability. A significant improvement of the resilient system behaviour shall be achieved by reducing the recovery time. The reboot of the whole control unit is decisive for the recovery time. If the CPU of the control unit can be kept running the recovery time is reduced to less than one second. To realise this, a minimum power supply voltage is required, that consequently defines the minimum functionality of the brake system [3].

Fig. 2. Functional structure for a combined robust and resilient car brake system, following [3]

The described disruption falls in the category ‘lack of resources’. According to Table 1, i.e., a degradation strategy is suitable for this disruption and is exemplary chosen, here. For the basic coping strategy the lacking resource is specified as energy, whose consumption shall be reduced using degradation. Applying the degradation means switching off expendable functions, which consume energy, in case of a decreasing power supply voltage. Looking at the brake system expendable functions are assistant systems like ABS for an internal degradation.

The system in the resilient configuration using internal degradation as a coping strategy is depicted in Fig. 2 according to the introduced additional elements for integrating the system adaptivity in the functional structure. The resilient consideration horizon is given below the robust system and the coping strategy consists of the three possible adaption functions, whereas no additional resilient function is required. The gather data function is connected to signal enablers for detecting the ambient temperature, the engine starter signal and the current conduction within the power supply unit. The collected data are processed by the interpret data function, which enables the system to anticipate a potential disruption of the power supply voltage and, in case of the occurrence of the disruption, activates the execute adaption function, which switches off expendable assistant functions within the electronic unit and enables the alternative load path of the hydraulic crackdown, depicted by the dis- and enablers connected to these functions and flows. The disrupted function here is the energy supply, which is crossed with dashed lines. The disrupted signal, material and energy flows, which arise from the disrupted energy supply, are denoted with dashed arrows and the flows manipulated by the resilient adaption functions are marked with thick grey arrows. These are also either solid for enabled flows or dashed for disabled flows.

6 Summary and Conclusions

Resilience design for load-carrying systems in addition to robust design offers a high potential, especially for highly safety relevant systems, like the shown car brake system. For the systematic development of resilient load-carrying systems the system needs to be analysed with regard to its weaknesses and inherent resilient behaviour using, e.g., the vulnerability analysis taking into account an extended consideration horizon, including the robust system itself as well as the superordinate system and the environment.

For the system description and the deduction of required resilient properties the resilience application model has been developed. Based on the analysis an appropriate basic coping strategy can be derived according to the disruption’s character, the system properties and the environmental conditions. The definition of an appropriate basic coping strategy can be supported by a catalogue of general coping strategies derived from, e.g. successful resilient natural organisms as exemplary presented. Afterwards, the basic coping strategy is transferred into a system coping strategy.

For systematically realising the system coping strategy the static robust functional structure has to be extended to a dynamic resilient functional structure. Within the resilient functional structure flows and functions are controlled via a newly developed interface. The interface comprises mainly enablers and disablers controlled by the adaption functions. Having developed the resilient functional structure the conventional systematic product development process can be followed using resilient solution principles,

in addition [4]. The depicted functional structure of a by-wire car brake system shows that resilient approaches in load-carrying systems are already realised, like the introduced degradation strategy.

Using a comprehensive resilience design approach as aspired with the introduced new or extended models and methods holistic resilience concepts for technical systems including all identified vulnerabilities are achievable.

Acknowledgement. Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – Projektnummer 57157498 – SFB 805.

References

1. Hollnagel, E., Woods, D.D.: Prologue: resilience engineering concepts. In: Hollnagel, E. et al. (eds.) *Resilience Engineering - Concepts and Precepts*. Ashgate Publishing Ltd, Farnham (2006)
2. Altherr, L.C., et al.: Resilience in mechanical engineering - a concept for controlling uncertainty during design, production and usage phase of load-carrying structures. In: Pelz, P.F., Groche, P. (eds.) *Applied Mechanics and Materials*, vol. 885, pp. 187–198. Trans Tech Publication Ltd, Zurich (2018)
3. Schulte, F., et al.: Beitrag zur Entwicklungsmethodik für resiliente Systeme des Maschinenbaus. In: *Proceedings of the 30th Symposium Design for X (DFX 2019)*, pp. 1–12. Jesteburg, Germany, 18–19 September 2019, The Design Society (2019)
4. Schulte, F., et al.: Analysis and synthesis of resilient load-carrying systems. In: *Proceedings of the 22nd International Conference on Engineering Design (ICED19)*, pp. 1403–1412. Delft, Netherlands, 5–8 August 2019, Cambridge University Press (2019)
5. Woods, D.D.: Essential characteristics of resilience. In: Hollnagel, E. et al. (eds.) *Resilience Engineering - Concepts and Precepts*. Ashgate Publishing Ltd, Farnham (2006)
6. Hollnagel, E.: RAG-The resilience analysis grid. In: Hollnagel, E. et al. (eds.) *Resilience Engineering in Practice: A Guidebook*, pp. 275–296. Ashgate Publishing Ltd., Farnham (2011)
7. Turner, B.L., et al.: A framework for vulnerability analysis in sustainability science. In: *Proceedings of the National Academy of Sciences of the United States of America (PNAS)*, vol. 100, no. 14, pp. 8074–8079. National Academy of Sciences, Washington (2003)
8. von Gleich, A., et al.: Resilienz als Leitkonzept - Vulnerabilität als analytische Kategorie. In: Fichter, K. et al. (eds.) *Theoretische Grundlagen für erfolgreiche Klimaanpassungsstrategien*, Nordwest 2050, pp. 13–51. Oldenburg, Bremen (2010)
9. Ratter, B.M.W.: Island vulnerability and resilience. In: Ratter, B.M.W. (ed.) *Geography of Small Islands - Outposts of Globalisation*, pp. 173–200. Springer International Publishing, Cham (2018)
10. Rowan, E., et al.: Indicator approach for assessing climate change vulnerability in transportation infrastructure. *Transportation Research Record: Journal of the Transportation Research Board* No. 2459 (1), pp. 18–28. Transportation Research Board of the National Academies, Washington (2014)
11. Döniz, E.J.: Was ist die Szenariotechnik? In: Döniz, E.J. (ed.) *Effizientere Szenariotechnik durch teilautomatische Generierung von Konsistenzmatrizen - Empirie, Konzeption*, pp. 6–44. Fuzzy- und Neuro-Fuzzy-Ansätze, Gabler, Wiesbaden (2009)

12. Gallopin, G.C.: Linkage between vulnerability, resilience, and adaptive capacity. *Global Environ. Change* **16**(3), 293–303 (2006)
13. Feldhusen, J., Grote, K.-H.: *Pahl/Beitz Konstruktionslehre – Methoden und Anwendung erfolgreicher Produktentwicklung*“. 8th completely revised edition, pp. 237 ff. Springer Vieweg Verlag, Berlin (2013)
14. Cutter, S.L., et al.: A place-based model for understanding community resilience to natural disasters. *Global Environ. Change* **18**(4), 598–606 (2008)
15. Schlemmer, P.D., et al.: Adaptivity as a property to achieve resilience of load-carrying systems. In: Pelz, P.F., Groche, P. (eds.) *Applied Mechanics and Materials*, vol. 885, pp. 77–87. Trans Tech Publication Ltd, Zurich (2018)
16. Breuer, B., Bill, K.H.: *Bremsenhandbuch – Grundlagen, Komponenten, Systeme, Fahrodynamik*. Springer, Wiesbaden (2017)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.