Applied Mechanics and Materials
ISSN: 1662-7482, Vol. 885, pp 240-252
doi:10.4028/www.scientific.net/AMM.885.240

Submitted: 2018-04-30
Revised: 2018-07-26
Accepted: 2018-07-27
Online: 2018-11-20

On Obligations in the Development Process of Resilient Systems with Algorithmic Design Methods

Lena C. Altherr[1], Laura Joggerst[2], Philipp Leise[1], Marc E. Pfetsch[3], Andreas Schmitt[3*] and Janine Wendt[2]

[1]TU Darmstadt, Chair of Fluid Systems, Otto-Berndt-Straße 2, 64287 Darmstadt, Germany

[2]TU Darmstadt, Chair of Civil Law and Business Law, Hochschulstraße 1, 64289 Darmstadt, Germany

[3]TU Darmstadt, Research Group Optimization, Department of Mathematics, Dolivostraße 15, 64293 Darmstadt, Germany

altherr@sfb805.tu-darmstadt.de, joggerst@sfb805.tu-darmstadt.de, leise@sfb805.tu-darmstadt.de, pfetsch@sfb805.tu-darmstadt.de, schmitt@sfb805.tu-darmstadt.de, wendt@sfb805.tu-darmstadt.de

Keywords: legal obligations, product liability, design of technical systems, optimization, resilience

Abstract. Advanced computational methods are needed both for the design of large systems and to compute high accuracy solutions. Such methods are efficient in computation, but the validation of results is very complex, and highly skilled auditors are needed to verify them. We investigate legal questions concerning obligations in the development phase, especially for technical systems developed using advanced methods. In particular, we consider methods of resilient and robust optimization. With these techniques, high performance solutions can be found, despite a high variety of input parameters. However, given the novelty of these methods, it is uncertain whether legal obligations are being met. The aim of this paper is to discuss if and how the choice of a specific computational method affects the developer's product liability. The review of legal obligations in this paper is based on German law and focuses on the requirements that must be met during the design and development process.

Introduction

The usage of simulation and optimization tools in the development of technical systems has been increasing continuously over the last few decades. Moreover, improvements in computer hardware and software development reduce barriers to the use of these techniques in all phases of product development processes. This usage leads to improvements in productivity and economic benefits. For example, in today's automotive industry, state-of-the-art software tools are used with simulation techniques such as Finite Element Methods (FEM), Computational Fluid Dynamics (CFD), Multibody Simulation (MBS), Crash Simulations and Topology Optimization techniques, all of which reduce the overall development time and improve the accuracy and safety.

In addition to simulation software, there is a growing interest in optimization methods. These tools enable the computation of optimized parts or of optimized topologies consisting of multiple components. Examples of this are the optimization of the topology and geometry of sheet metal components [1] and of the topologies of water networks [2].

A current trend in mathematical optimization is to consider the failure of system components, such as single trusses, fans, valves or pipes, and to develop resilience optimization techniques that allow topologies guaranteeing a predefined minimal functional performance even for the failure of arbitrary components. This explicit consideration of failures during the development process will lead to more resilient systems.

Unfortunately, due to their complexity, the usage of optimization software during the development of technical systems also leads to potential liability risks. In this paper, we assess these risks. We begin in the following section with an introduction to the relevant legal literature for German law. Since we are illustrating the research questions addressed in this paper with case

studies of usage, we provide an overview of the relevant engineering basics and standard development procedures in the following section. Moreover, we identify possible sources of errors that occur when algorithmic design methods are employed. As case studies we discuss the development of a bridge truss topology and of a ventilation system for subway systems. We conclude with derived legal methods and matters for consideration in the usage of optimization software for engineering products. We also examine liability issues that occur during the development of resilient systems.

Legal Liability in Germany

Products on the market can, and often enough have, caused harm to a person's life, health or property. The same applies to safety-critical infrastructures in the public space, such as bridges or subway networks. This can result in liability charges being brought up against the party responsible for the damage. These charges can arise either from a breach of contract or from legal liability, as in strict liability or tortious law. The producers and operators of the afore-mentioned facilities try to calculate their risks, especially the financial risks, very carefully. Therefore, it is essential for them to know how to avoid liability claims. Any uncertainty related to liability can hamper the uptake of innovations because of the unknown risk. Liability due to a breach of contract by one of the contracting parties is far more manageable and easier to predict. Due to the vast variation in contractual agreements and the fact that they are less likely to be subject to uncertain risks, this paper focuses on legal liability.

Section 823 of the German Civil Code, the Product Liability Act and the Product Safety Act provide the legal framework for the producer's or product liability in Germany. The following only provides a brief overview of conditions of liability regarding Section 823 of the German Civil Code, since the other mentioned legislation acts are not of concern to the engineering examples presented in this article..

Liability in respect to Section 823 paragraph 1 of the German Civil Code. Section 823 paragraph 1 of the German Civil Code states that anyone who injures a person's life, health or property through an unlawful action, is liable for the resulting damages. Therefore, producers or operators of dangerous facilities can be held liable for damage done to these specifically mentioned rights. The requirement for negligence or intention restricts the scope of the rule to such actions. Intent refers to fulfilling the requirements of section 823 paragraph 1 of the German Civil Code knowingly and on purpose. Negligence requires a failure to exercise reasonable care. The uncertainty that arises in connection with legal liability stems mostly from the difficulty in specifying this requirement for reasonable care. Intentional actions are not discussed any further in this paper.

It is reasonable to expect that safety obligations are met. Safety obligations can arise from the usage of any source of danger [3]. Conflicting interests of the parties involved are considered when determining safety obligations. For example, the operator of a potentially dangerous facility operates the facility for economic reasons. On the other hand, third parties and their rights need to be protected. If a party's rights are jeopardized by usage of a dangerous facility, the operator who profits from this usage must implement safety measures to prevent damage. It is therefore necessary for the operator of a dangerous facility to analyze potential risks to third parties. As a result of this analysis, appropriate safety measures need to be taken. With regard to both the safety measures and the risk analysis itself, only what is actually possible considering state-of-the-art standards, can be expected from the operator or producer. If there is no possibility of identifying a specific risk using state-of-the-art technology, then no safety obligations have been breached, even if this unidentifiable risk results in the injury of a third party. Thus, state-of-the-art technology has a direct impact on what can be reasonably expected from any producer of products or operator of a facility. It is therefore necessary to analyze the latest technology most carefully and always be up to date.

From a legal point of view, state-of-the-art technology sets safety standards that cannot be disregarded. Any technology which is ready to be implemented for serial production is subject to this aspect [4]. Consequently, producers or operators have to implement a system that allows them

to actively track the latest technology and any possible security improvements that go along with it. Often they rely on complying with technical standards, such as DIN standards or ISO standards. These standards aim to specify the applicable legal provisions and necessary safety measurements. It is important though to mention that compliance with these standards cannot per se prevent liability as they are not legally binding. Nevertheless, compliance with technical standards is still recommended as they set the bar for the minimum safety expected. In some cases, it may be necessary to exceed this safety minimum, in so far as it is possible with regard to state-of-the-art technology [5, 6].

Engineering Application

To illustrate the research questions addressed by this paper, we consider two different examples of applications: the design of a truss bridge and the design of a ventilation system for a subway network. In the following two sections, the relevant basics and standards for the development of such systems are presented. Furthermore, the concept of resilience is explained and possible errors in the design stage are sketched.

Truss topology bridge design. One possible design for bridges is a truss topology. A truss is a mechanical construction given by a set of nodes which are linked by elastic bars. A popular example is the Eiffel Tower. Within the design phase, the forces and displacements of the different trusses are simulated using FEM simulations. Alongside this, CFD simulations are also used to compute different wind loads on the structure. Furthermore, optimization methods can be used to determine the best possible structure. The relevant standards and guidelines are [7-13]. These standards and guidelines define the different possible loads, assumptions for the construction and fatigue tests based on Wöhler experiments to ensure long-term stability under varying loads. Additional standards are used for the special case of potential earth quakes [14] and to design the structural bearings [15]. The monitoring of bridges and other civil structures in Germany is regulated by a standard [16]. These documents regulate the process for inspecting and controlling the stability, security and durability of civil structures such as bridges. Detailed instructions and a summary for the design of bridges can be found in [17].

Ventilation systems in public infrastructure. Multiple public infrastructure systems, such as subway systems, highway tunnels or non-residential buildings like airport terminal buildings need ventilation systems. The main functionality of fan systems is the provision of fresh and clean air. In case of fire events, a ventilation system helps to provide visibility during the evacuation phase. Standards [18-21] are used in Germany to design such systems for both daily usage and for rare events such as fires. Potential failures in these systems and appropriate design options are currently being considered in the scientific community, cf. [22-24]. Multiple system topologies for the overall design of these ventilation systems are possible and as an objective, it is possible to compute the most energy efficient topology by optimization algorithms, cf. [25]. The smoke stratification and mitigation of a final topology design can be simulated with CFD techniques [26, 27]. In addition to this, model-based and large-scale experiments, cf. [28], are used to verify the simulation results.

Resilience. To improve the overall availability and functionality of technical systems, especially for systems involving safety, the consideration and anticipation of several possible failures in the design phase is a promising strategy for increasing the resilience of technical systems. A resilient technical system guarantees a predetermined minimum of functional performance even in the event of disturbances or the failure of arbitrary system components and offers the subsequent possibility of recovering at least the functionality at the design point. One possible way to include resilience in a truss topology design problem is to consider only solutions that tolerate each possible combination of up to k bar failures. In this case, the total number of arbitrary component failures the system can withstand is a degree of freedom in the topology design. The resilient design guarantees a minimal functionality in all these cases. A design has a so-called *buffering capacity* of k if it guarantees a predefined minimal functional performance in each possible combination of up to k bar failures. Nevertheless, if a system has a buffering capacity of k, this does not provide any

information about its performance in the case of a combination of more than k component failures. The number of possible failure scenarios and their impact increase rapidly with the complexity of the system under consideration and the number k. For small systems, an enumeration of all possible failure scenarios is possible. However, with an increasing number of design choices and components, it becomes impossible to enumerate all the possible combinations within an acceptable time.

Possible errors in the development process. During the algorithmic design of technical systems, several errors might occur that have an influence on the validity of the computed solution. If this leads to bad design decisions, it can have a considerable impact on the legal aspects.

One important source of error is the fact that any virtual development is based on a model which only partly represents reality. Usually, there are many model variants available that provide more or less accurate approximations of reality. In practice, it is often known in which regime of parameters an approximation is good or not. However, if the wrong model is chosen or used in a parameter regime for which the model was not designed, serious deviations arise between the reality and the predicted outcome. One important restriction for practice is that the most reliable models are often too time consuming to handle, both from a computational viewpoint when simulating or optimizing and for setting up the model (for which reliable detailed data is needed). Moreover, optimization models often require smaller models (i.e., less details, less degrees of freedom) in order to be computable within an acceptable time.

Another source of error is the wrong implementation of models either by mistake or as a result of a misunderstanding of the task. Furthermore, any computation performed in floating point numbers (as used by virtually any method that is fast enough in practice) has an intrinsic source of rounding errors. Finally, programming errors arise frequently and can have a severe impact on the correctness of the computations.

All these sources of error are well known and several counter measures have been developed, e.g., software engineering processes. Moreover, models should be verified, i.e., checked for consistency and if possible validated. Validation can happen in two ways. One can compare the results of the computation to measurements in practice and one can compare them to results from simulations using a finer model. Both methods are usually time consuming and are not always used in practice.

An important special case arises when resilient or robust systems are to be designed. In this case, the computations have an intrinsic two-level structure, which guarantees that the design is able to capture a certain domain of loads. That is, the first level contains decisions about the design, while the second level makes sure that every load is captured. For instance, a bridge should withstand different loads. If the set of loads is finite, it is in principle possible to use a finer simulation model to check each particular case. However, this might not be practical if the set is very large or impossible if it is infinite. If it is necessary for such a large set of loads to be captured, it is not clear how the design/optimization process should be set up to guarantee a given level of safety.

Note that the amount of additional work that is necessary to make computations reliable, i.e., independent from possible floating-point errors can be significant. For instance, Gleixner [29] reports a slowdown factor of about 3 if linear programs are made exact. Moreover, Cook et al. [30] report a maximal slowdown factor of 20 if mixed-integer programs are made exact. However, in both cases this requires a significant implementation effort and non-standard software. A further possibility is to record the essential decisions made during a solution algorithm and to check this certificate using an independent implementation. This has been investigated in Cheung et al. [31]. Note that this will often lead to an enormous output size of more than one Tera-Byte. Moreover, all these techniques have been developed for the mixed-integer linear case only. So far, only very little software is able to reliably handle nonlinear or PDE-constrained optimization problems. Finally, to make resilient decisions safe, it would in the worst case be necessary to test all failing cases. For instance, for guaranteeing a buffering capacity of $k = 4$, 4 out of 1000 failure possibilities would have to be checked which already gives 4 billion cases. A brute force enumeration is then not practically possible (it would take more than 300 years if one case could be checked per second).

From a legal perspective, a certain level of verification, validation and/or software engineering would be required, depending on the particular application. If the application is safety-critical, higher levels would be necessary. However, it is in general not easy to determine the appropriate amount of checking, and it would be helpful in practice if some legal advice were available.

Legal Case Studies

To research legal requirements on algorithmic design we consider two case studies, presented in the following.

Algorithmic bridge design. As the first case study, we consider the failure of a footbridge. The bridge was designed as follows. In the first phase, the main properties of the bridge were designed by using conventional methods of civil engineering. This leads to a truss topology prototype which describes the placement of around 100 beams. Mathematical optimization was then used to optimize material consumption. The diameter of the beams is minimized, subject to the condition that the bridge must be able to sustain the maximal load determined in the previous phase. While conventional methods would have assumed a fixed diameter for all beams, with the aid of mathematical optimization is possible to control the high complexity of the huge number of beam interactions and to omit redundant beams.

The optimized bridge is built. It collapses, when a large number of people use it as an observation point for fireworks on New Year's Eve. A subsequent investigation reveals that one potential design error was a false assumption in the model used in the optimization phase. A newly developed material had been picked for the beams in the first phase. The material's elasticity changes considerably at low temperatures, which had not been considered in the optimization model. Together with the unusually high load this led to its failure.

Algorithmic design of a ventilation system for a subway network. Multiple designs are possible for the ventilation of tunnels, e.g., transverse ventilation, partial transverse ventilation or longitudinal ventilation [32]. Furthermore, design choices also comprise the number of fans and their position. Within the design space of these options, a resilient and energy-efficient system topology can be found by using an algorithmic design approach. Prerequisite for such an approach is a suitable model. In this particular example, the characteristic curves of different fans can be approximated with polynomial functions. Additional model assumptions for the law of friction for air in exhaust shafts for transverse and partial transverse ventilation and for the law of friction for tunnels for longitudinal ventilation include further simplifications of reality. Partial models are validated by experiments, but the risk of exceeding the overall model horizon by a combination of multiple minor approximation errors is less foreseeable for complex optimizations, and a validation of the optimization result is only possible with high levels of input and expenditure. On the other hand, a reduction of model simplifications would lead to an increase in computation time and is therefore not possible.

In the second legal case study, we consider a reduced smoke outlet when an accident with smoke emission occurs in a newly built tunnel causing injury to many persons. The tunnel ventilation was built using resilience optimization demanding a buffering capacity of$k = 1$. In case of one arbitrary failing fan, the system should still provide a minimal functionality, namely a predefined volume flow and pressure increase.

To allow inspection/repair, one fan of an array near a vehicle involved in the accident is shut down, but according to the computed buffering capacity, the system should withstand the failure of an arbitrary fan and still provide minimal functionality. However, in this incident functionality below this predefined limit was detected. The aforementioned combination of approximation errors in the underlying model causes this lower functionality and is responsible for the high number of persons injured.

Review of Legal Obligations

In the following, legal principles are applied to the two case studies. In particular we discuss the question of duty of care when selecting a model of the system during the design phase as well as the obligation to adapt this model once the system is already in use. In this section the article also tries to identify legal requirements for the use of optimization and resilience optimization methods. Finally, an outlook is given for resilient operating systems.

Should a fault in the bridge or the ventilation system lead to an injury of an uninvolved third party, then the question of compensation for damage arises. As no contractual relationship exists between the injured parties and the party responsible for the damage, the claim for damages in these cases can only be decided in accordance with tort law. Having established these introductory thoughts with regard to this basis for liability, it is then important to consider whether the operator of the ventilation system had breached a duty of care to protect the legal right in question.

The danger that transpired in the case of the ventilation system was related to its operation, namely that as a result of insufficient ventilation during a fire, personal injury was inflicted. The operator is obliged to take appropriate precautions to prevent anything endangering the legal rights of third parties. The bridge builder also has a duty to prevent danger to third parties. This duty is based on the general legal principle established in Section 823 of the German Civil Code and in Sections 836, 837 of the German Civil Code.

This means those measures must be taken which are technically possible, given the state of technology at the relevant time, to eliminate the danger effectively. The technical norms and standards of private standardization associations can be taken into account in deliberations to ascertain the minimum standard that must be observed [33, 5, 6, 34].

Breach of duty of care in the selection of the model. The design of a system is based on models, as in our examples. The approximation of a system and its real environment that this involves enables the application of mathematical solutions such as the optimization methods already described. However, not the entire system with all its physical relationships is reproduced. Only a simplified representation is used in the development stages. The uncertainty factor that arises from this also persists in the use of the system. If the real system experiences a load for which it has not been designed because the relevant scenario could not be reproduced with the model used, this can lead to a system failure. In the case of the footbridge, the load caused by the large number of people had actually been taken into consideration, but not the fact that the parameters of the material used are affected by temperature. When third parties suffer an injury as a result, the question arises as to whether the load that led to that injury could have, and should have been taken into consideration at the point the model was selected. If the developer, in these cases the operator of the ventilation system or the bridge builder, relies upon the approximation of models, he must ensure that the actual model chosen supplies reliable conclusions for the scope of usage he envisages. As a rule, this is checked by validating the model with the aid of experimental data or using the results of simulations. Comparing the behavior of the model with the way the system behaves in reality, exposes flaws in the model allowing its limits to be identified. From a legal point of view, the validation of the model can be brought as evidence to exonerate the operator from liability. Validation demonstrates that the approximation of the system as a mathematical model for the type of usage described replicates reality closely enough. If the design of the system is based on this model, it can be assumed that the operator's duty to prevent danger has been met at this stage of the development. However, this only holds true if safety aspects are reproduced by the model. If the limits of what can be measured are merely disregarded when selecting a model, this would be a case of negligence. In the case of the bridge, there had been a failure in the development phase to recognize that the model on which the optimization was based could not provide any information about system conditions at very low temperatures. The fact that the elasticity of the material used changes considerably at low temperatures could have, and should have, been recognized. Particularly when new materials are being employed, it is to be expected that a careful examination of their qualities and suitability for the planned usage is carried out. The care expected of the developer demands that he is aware of the limits of the model and the parameters of the material and takes these into consideration in the selection process.

On the question of whether aspects concerning safety are reproduced in the model, it is also necessary to take into account which risks and dangers are foreseeable. The developer cannot be expected to foresee all the conceivable conditions of the system and to then take these into account in the selection of the model. Realistically, it is not possible to demand one hundred percent safety [35 - 38]. The boundary between what is foreseeable and what is not is fluid and must be judged case by case. However, certain points can be drawn from examining decisions in case law in the field of tortious liability. For example, natural catastrophes and the damage caused by these are as a rule not foreseeable. However, this is only true when it is a question of natural events that occur so rarely that they are not to be expected. If it is a matter of events that experience shows occur more frequently, such as floods, then they are foreseeable. In such cases, the system must be designed to cope with these natural events in such a way that there is no injury to the legal rights of third parties [39]. Particular regional variations must also be catered for in this respect.

Should it come to a failure of the bridge system, as in the example selected, the question then arises as to whether existing norms and standards have been met. If, despite having met those standards, a damaging event occurred, the question of whether the danger that transpired was foreseeable depends on the circumstances of the particular incident.

In a case of a falling roof tile, the court assumed that storms with speeds of up to 12-13 on the Beaufort scale are foreseeable and appropriate safety precautions against falling tiles should have been taken [40].

Duty to adapt the model during the use phase. In this context, the question arises as to what duties the developer of the system has, if in the course of time the system parameters change and as a consequence no longer conform to the limits of the model. The model's limitations restrict the foreseeability of the system's behavior to a certain area of usage. For example, in the case of the bridge, the chosen model produces reliable findings for a bridge which is rarely used but cannot reproduce the vibrations that may occur in the event of an increased traffic. Here too, the developer must take account of the limitations of the model and at the same time also consider the resulting limits to the system. If there is a departure from the scope of usage originally defined, the system must be adapted accordingly by changes to the underlying model and where necessary by taking safety measures. The operator of the system must also ensure that limits for its use are observed during the use phase (similar [41]). Only when this is done, can it be assumed that the system will behave as expected during its design.

Requirements for the use of optimization methods. In the design of more complex systems, mathematical tools are used to simplify selection from the numerous possible combinations of the relevant parameters. These tools include optimization methods, which work on a model of the system and its environment. The optimization parameters are set by the developer. The number of parameters that feed into the optimization process is finite. However, in the real environment a multiplicity of factors affect the system. It is not possible to foresee all the factors that can have an effect. Even if it were possible, the solution of an optimization problem like this would challenge the limits of computational power. Safety as such cannot be used as an input parameter as it depends on numerous factors.

It is mainly economic and structural factors that are input into the optimization. The developer cannot therefore just assume the optimized system also accords with the safety expected of it. Safety can actually come at the expense of the input parameters, something which is made very clear when, for example, the goal is to make savings on materials. The developer would have to add a later process to the optimization to check whether the optimized system also supports the required safety. In this respect it is no different to designing and developing a system without using optimization methods. However, here it is not possible to refer back to the earlier deliberations between alternative solutions for its construction. The whole point of using optimization methods is to come up with just one solution for the system's construction at the end. This will be the optimum solution in view of the problem defined. All other alternatives have already been excluded prior to this by the algorithm. In some cases, it would indeed be possible to list all the possible combinations for the given parameters and then check them for safety. However, in practice this can

only be done at the cost of considerable time and expense. The advantage of a shorter optimized development stage offered by mathematical methods would be completely lost. The development of newer and more complex methods for finding solutions would hold no attraction, if its potential could not be exploited. It is therefore necessary to be able to carry out a check on just one of the many possible constructions to demonstrate its safety.

However, the particular cases presented also demonstrate that practical safety tests would not be feasible for the prototypes of larger systems in their entirety. Yet the interaction between different components means that this would be the only way to reduce the risk of safety issues to a minimum. Both operator and developer must rely on proving the safety of their system mathematically and with the aid of simulations.

Yet again, these are based on simplifications, models and assumptions. Accordingly, the same requirements must be made for its operating principles that were made for the model for the system.

The limits of what can be reproduced by the model must be recognized and kept to. Once again, it is not possible to demand that all possible examples of use are tested. Absolute safety is not expected or demanded of traditional tests on physical prototypes either [35 - 38].

Requirements for the use of resilience optimization methods. Methods for resilience optimization are based on conventional optimization techniques, but differ in their outcome. Resilience optimization produces a system that is designed to cope with numerous different situations incurring loads and stresses without these having to be specified precisely at the outset. With this method, the system can withstand a defined number of unknown real failures and maintain its functionality. The problem of being restricted to only being able to optimize a predetermined characteristic is overcome. An optimized system can be achieved without having to predict all the environmental parameters. In the case of the bridge, a structure optimized for resilience would improve safety from systems failure due to unknown causes. In the case of the ventilation system optimized for resilience, ventilation can be guaranteed if a defined number of ventilators fail. In a fire, this would increase the safety of those in the tunnel, as smoke extraction and the prevention of an uncontrolled rise in temperature were ensured.

Methods for resilience optimization are currently still relatively rare, which is the reason why no attempt has been made to establish standardization. As yet, there are no technical rules specifying minimum standards for optimization. This problem usually arises when developments in technology are driven by manufacturers of technical products and operators of technical systems. As for the interests of third parties that require protection, it has to be assumed that safety standards will continue to develop as technology continues to develop. More up-to-date technology should not be left lagging behind with safety standards applicable to older technology [4]. With regard to the question of whether the system operator in the presented case breached his duty of care, the question of how it can be proved that these duties have been carried out is of particular relevance in cases where advanced technology is being employed. If technical rules and standards offer no pointers for this, then in cases of doubt the operator must be able to supply proof himself. The problem lies in the fact that in areas optimized for resilience such as the framework of a bridge and the network of the tunnel ventilation system, the analysis of the possible danger to the legally protected rights of third parties is technically no longer necessary. The assumption made by the developer is that as long as the system's functionality is maintained, there will be no injury to the legally protected rights of third parties. With regard to the criteria relevant to the duty of care, the extent to which danger can be foreseen and prevented can no longer be of any significance if there is no analysis of danger carried out prior to designing the system. In addition to which, with systems optimized for resilience it is not possible to predict exactly how the system will behave during its use. To be able to predict this behavior, it would have to be possible to model all the possible disruptions for the system. This issue can be compared to the examination of the method of optimization with one difference: the number of possible combinations to be calculated is much higher. Checking the results using standard methods or simulations is only possible at the cost of considerable time and expense. The duty of care that the operators and developers must meet is in general based on the level of safety that can be implemented with state-of-the-art technology and

can justifiably be expected by the users in question. But only measures that are reasonable in practice have to be taken. To determine what is reasonable for the developer or operator, a balance must be drawn between the increase in safety gained by the measure and the time and labor incumbent upon the developer or operator that are inherent in its implementation [39]. Economic considerations may also play a part in this discussion, cf., [4]. However, the operator and the developer can reasonably be expected to take more costly measures depending on the risk probability and the legally protected right at risk [42, 43]. An objective benchmark cannot be set independently from an individual case. As mentioned, in the case of resilient optimization, a way to make resilient decisions safe would be to test all failing possibilities. For 4 out of 1000 possibilities this test phase would take more than 300 years if one case would require one second. It cannot reasonably be expected of a developer to invest this amount of time only during the development process of a new system. Although this example seems to be exaggerating, it shows why some risks cannot be totally eradicated.

It is clear though that, ideally, one would expect the resilience optimization method to result in increased safety. However, as shown above, the level of risk of failure in this method and the consequent risk of damage or injury is uncertain. There is as yet no experience to fall back on. If the use of a new method promising increased safety in comparison to conventional methods includes other risks, there must be an assessment to decide whether this method should be used at all [4]. The ventilation system optimized for resilience was actually designed to increase personal safety in the case of a fire. The complexity of the method and the interplay of several different components in the system meant that some significant approximations had to be made in the underlying model. It was not possible to reproduce the system and its environment exactly and due to the loss of one ventilator this ultimately led to the failure of the entire system.

The increased safety is balanced against the increased risk with the aid of the probability of the risk materializing and in accordance with the type and scope of the damage or injury that might be expected as well as its practical usefulness for the users in question, cf., [4]. To assess the risk, trials and tests would have to be carried out that can provide information about the failure rate. Once the failure rate falls below a specified value, the method could be employed as a safe alternative to state-of-the-art technology in use until now. What is doubtful however, is how this value could be determined. Starting from conventional methods where the risk can be calculated, resilience optimization would by comparison have to offer an advantage in a way that the failure rate would be lower. As there are currently no methods that can guarantee to verify this for resilience optimized systems, they would have to be developed. Otherwise the developer of such a system could run the risk of being accused of having set a safety standard below the current state of technology.

In the case of the bridge, a design for enhanced resilience will require a test of its load-bearing capacity to be carried out in accordance with currently accepted state-of-the-art technology so that the structure can be proved to offer the same performance when there are no failures. Exceptional circumstances that must be explicitly considered, such as collisions with individual struts, must be checked separately from this in accordance with state-of-the-art technology. Ideally when there is a failure of additional components, the construction of a resilient structure increases the resilience of the entire structure. This means that a minimum level of safety equivalent to that of current technology continues to be guaranteed. In the development of the ventilator system, an analogous process is needed to meet current safety requirements.

In cases where it is possible to calculate the risk compared to conventional methods, as shown in the case of the given examples, it must be noted that the information supplied by the comparison is limited. Comparisons can only be made for those areas of risk that are actually comparable. In the case of the bridge, a test for load-bearing capacity for conventionally designed bridges was developed. This test can then be used to compare the bridge designed for resilience with conventional systems, but only for the scenario where no truss fails. So this conventional test can provide no information with regard to the actual scope of use of the bridge designed with resilience optimization methods. If the use of this method is basically justifiable, although some known risks

concerning safety remain that should not be underestimated, then the system must be monitored particularly carefully during its use phase [44]. The manufacturer's duty of care is extended to firstly selecting and implementing suitable measures for monitoring and using the results to minimize damage and injury. It would also be advisable for him to use the data produced by the monitoring process to make improvements to the method and the model underlying the system. Those flaws or damage events that occur during the course of monitoring are, from that point onward, foreseeable for the developer and they must therefore be taken into account appropriately to ensure the duty of care is being met [45, 46].

Characteristics of resilient operation – the prospects. The next stage in the development of resilient methods will see research exploring not only questions on resilient optimization but also issues around the resilient operation of a system. From a legal point of view, the capacity to anticipate, react and learn provides key information for making an assessment. On the basis of resilience optimization, a system could permanently monitor its own status during its service life and, in the event of component failure it could react independently without in any way compromising the functional principles of the system. One can imagine this type of operation being used in the example of the ventilation system. The operation of the ventilators would be continuously monitored by the system and, in the case of a failure, it would react to the incident by adjusting other system components and maintaining the full functionality of the ventilation system. All this is possible without any human intervention and without the necessity to foresee the particular scenario causing this failure.

So in addition to the difficulties arising in cases of resilience optimization, there is the issue of the resilient operation of a system reacting independently to environmental factors and changing and adapting itself. By learning from the problems it encounters, it is even possible for the system to adapt its behavior independently and ideally improve it for dealing with future problems. In the case of a damage event, from a legal point of view it would be necessary to explore how the cause of the damage or injury can be attributed to the system operator. For an overview see [47]. If the legal basis on which the operator must assume responsibility for the behavior of the system is clear, the question is how he could avoid liability. The discussion about the duty of care of an operator of self-learning and self-adaptive systems has only just begun. The approaches for resilience optimization developed in this paper provide initial pointers. How ways of dealing with the potential dangers posed by technical progress develop from here remains to be seen. Socio-political developments will play a considerable part in shaping the public's expectations of safety and thereby influence the safety standards developers and operators must meet. The question of permissible risk will play a key role in this. Ultimately, there needs to be socio-political consensus about the degree of permissible risk; this task cannot be left to the manufacturers and developers of new technology.

Conclusion

In this paper we have analyzed legal requirements on the development of technical systems using optimization techniques. Summarized, the following obligations have been identified:

- The models used to design complex subsystems must be validated for the actual scope of their usage.
- Developers must be aware of the limits of the underlying model right from the design stage of a system and document them.
- During the use phase, it is essential to check whether the limits of the model are respected. If this is not the case, the model can provide no information about the system's behavior and appropriate safety measures must be taken.
- After optimization processes have been used to design a system, the result must be checked for safety aspects.

- The use of resilience optimization requires testing for evidence that at the very least the safety standard by current state-of-the-art technology is being met. Where this test is successful, the failure rate of the system designed with resilience optimization must be compared with conventional systems. Should it transpire that the failure rate is lower, then increased safety obligations must be placed on the monitoring of the system during the use phase.

The implementation of these requirements is in part common practice, e.g. the validation of models [48]. Resilience optimization however introduces new legal requirements, which to our knowledge have not been treated before. Especially, the means to compare the safety standard of resilient and classic design are unclear and need to be researched. Possible ideas include the comparison of both designs on load-scenarios or the computation of worst-case loads.

Acknowledgment

The authors thank the German Research Foundation for funding this research within the Collaborative Research Center SFB 805 "Control of Uncertainties in Load-Carrying Structures in Mechanical Engineering".

References

[1] T. Göllner, W. Hess, S. Ulbrich, Geometry Optimization of Branched Sheet Metal Products. Proceedings in Applied Mathematics and Mechanics. 12:1 (2012) 619-620.

[2] A. Morsi, B. Geißler, A. Martin, Mixed integer optimization of water supply networks, Mathematical optimization of water networks. Springer, Basel, 2012, 35-54.

[3] BGH, decision of 10/7/1975 - VI ZR 43/74.

[4] BGH, decision of 06/16/2009 - VI ZR 107/08 Rn. 16.

[5] BGH, decision of 09/18/1984 - VI ZR 223/82 = Neue Juristische Wochenschrift (NJW) 1985, 47 (49).

[6] BGH, decision of 09/09/2008 - VI ZR 279/06 = NJW 2008, 3779 Rn. 16.

[7] Eurocode: Basis of structural design; German version EN 1990:2002 + A1:2005 + A1:2005/AC:2010. (2010).

[8] DIN EN 1991-2:2010-12 Eurocode 1: Actions on structures - Part 2: Traffic loads on bridges; German version EN 1991-2:2003 + AC:2010. (2010).

[9] DIN EN 1992-2:2010-12 Eurocode 2: Design of concrete structures - Part 2: Concrete bridges - Design and detailing rules; German version EN 1992-2:2005 + AC:2008. (2010).

[10] DIN EN 1993-2:2010-12 Eurocode 3: Design of steel structures - Part 2: Steel Bridges; German version EN 1993-2:2006 + AC:2009. (2010).

[11] Eurocode 4: Design of composite steel and concrete structures - Part 1-2: General rules - Structural fire design; German version EN 1994-1-2:2005 + AC:2008, 2010. (2010).

[12] Bundesamt für Straßenwesen, ZTF-ING; Zusätzliche Technische Vertragsbedingungen und Richtlinien für Ingenieurbauten. (2018).

[13] Bundesamt für Straßenwesen, RAB-ING; Richtlinien für das Aufstellen von Bauwerksentwürfen für Ingenieurbauten. (2017).

[14] Eurocode 8: Design of structures for earthquake resistance - Part 1: General rules, seismic actions and rules for buildings; German version EN 1998-1:2004 + AC:2009, 2010. (2010).

[15] DIN 1337-1:2011-09, Structural bearings – German version EN 1337. (2011).

[16] DIN 1076:1999-11, Engineering structures in connection with roads - inspection and test. (1999).

[17] G. Mehlhorn, M. Curbach, Handbuch Brücken: Entwerfen, konstruieren, berechnen, bauen und erhalten, Springer, 2014.

[18] VDI 6029:2000-03, Ventilation plants for road tunnels. (2000).

[19] DIN 12101-2:2017 Smoke and heat control systems - Part 2: Natural smoke and heat exhaust ventilators; German version EN 12101-2:2017. (2017).

[20] DIN EN 16798-3:2017-11, Energy performance of buildings - Ventilation for buildings - Part 3: For non-residential buildings - Performance requirements for ventilation and room-conditioning systems (Modules M5-1, M5-4); German version EN 16798-3:2017. (2017).

[21] DIN 13779:2007-09 Ventilation for non-residential buildings - Performance requirements for ventilation and room-conditioning systems; German version EN 13779:2007. (2007).

[22] P. Sturm, M. Beyer, M. Rafiei, On the problem of ventilation control in case of a tunnel fire event, Case Studies in Fire Safety 7 (2017) 36-43.

[23] W. K. Chow, L. Qu, E. C. Pang, Incidents on fire and ventilation provision in subway systems in Hong Kong, International Journal On Engineering Performance-Based Fire Codes, 10.3 (2011) 41-47.

[24] M. Tabarra, D. Abi-Zadeh, S. Sadokierski, Design of a modern subway ventilation system, Tunnels & Tunnelling International. 36.11 (2004) 45-50.

[25] H. Liu et al, Multi-objective optimization of indoor air quality control and energy consumption minimization in a subway ventilation system, Energy and Buildings, 66 (2013) 553-561.

[26] P. J. Woodburn, R. E. Britter, CFD simulations of a tunnel fire—Part I, Fire Safety Journal.26.1 (1996) 35-62.

[27] P. J. Woodburn, R. E. Britter, CFD simulations of a tunnel fire—Part II, Fire Safety Journal. 26.1 (1996) 63-90.

[28] H. Ingason, Y. Z. Li, A. Lönnermark, Tunnel fire dynamics, Springer, 2014.

[29] A. M. Gleixner, Exact and fast algorithms for mixed-integer nonlinear programming, Dissertation, TU Berlin, 2015.

[30] W. Cook, T. Koch, D. E. Steffy, K.Wolter, A Hybrid Branch-and-Bound Approach for Exact Rational Mixed-Integer Programming, Mathematical Programming Computation, 5.3 (2013) 305-344.

[31] K. K. Cheung, A. Gleixner, D. E. Steffy, Verifying Integer Programming Results, in International Conference on Integer Programming and Combinatorial Optimization, Springer, 2017, pp. 148-160.

[32] J. S. M. Li, W. K. Chow, Numerical studies on performance evaluation of tunnel ventilation safety systems, Tunnelling and underground space technology. 18.5 (2003) 435-452.

[33] BGH, decision of 12/17/1982 - V ZR 55/82 = NJW 1983, 751 (752).

[34] OLG Hamm, decision of 12/21/2010 − 21 U 14/08 = NJW-RR 2011, 893 f.

[35] BGH decision of 11/08/2005 - VI ZR 332/04= NJW 2006, 610 marginal 10.

[36] BGH decision of 06/03/2008 - VI ZR 223/07 = NJW 2008, 3775 marginal 9.

[37] BGH decision of 03/02/2010 - VI ZR 223/09 = NJW 2010, 1967 marginal 6.

[38] BGH decision of 10/02/2012 – VI ZR 311/11 = NJW 2013, 48 marginal 7.

[39] BGH, decision of 02/08/1972 – VI ZR 155/70 = BGHZ 58, 149-162, juris recital 21.

[40] BGH, decision of 03/23/1993 - VI ZR 176/92 = NJW 1993, 1782.

[41] G. Spindler, Braucht das Recht neue Haftungskategorien? Computer und Recht (CR) 2015, 766-776 (769).

[42] BGH decision of 12/09/1986 - VI ZR 65/86 = Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 1987, 191 (193).

[43] BGH decision of 03/17/2009 - VI ZR 176/08 marginal 8.

[44] G. Spindler, IT-Sicherheit und Produkthaftung - Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer, NJW 2004, 3145-3150 (3147).

[45] K. Meier, A. Wehlau, Produzentenhaftung des Softwareherstellers, CR 1990, 95-100 (97).

[46] U. Foerste, in: Produkthaftungshandbuch, part 2, 3rd edition, 2012, § 24, recital 372.

[47] S. Horner, M. Kaulartz, Haftung 4.0, CR 2016, 7-14.

[48] R. G. Sargent, Verification and validation of simulation models, in Simulation Conference, IEEE, 2007, pp. 124-137.