The survival signature for quantifying system reliability: an introductory overview from practical perspective

Frank P.A. Coolen and Tahani Coolen-Maturi

Abstract The structure function describes the functioning of a system dependent on the states of its components, and is central to theory of system reliability. The survival signature is a summary of the structure function which is sufficient to derive the system's reliability function. Since its introduction in 2012, the survival signature has received much attention in the literature, with developments on theory, computation and generalizations. This paper presents an introductory overview of the survival signature, including some recent developments. We discuss challenges for practical use of survival signatures for large systems.

1 Introduction

Reliability of systems is very important in every day life and quantification of system reliability has been a topic of research over many decades. It has led to a huge literature, a large part of it with at best spurious links to real world systems and challenges. Methods for analysis are often presented for very small systems with quite straightforward structures, and important practical considerations, e.g. the conditions under which the system has to function, the actual tasks it has to perform and the required level to which it performs these, tend to be avoided in many research papers.

In 2012, we introduced the concept of *survival signature* [7], which is a summary of the system structure function that is sufficient to derive the system survival function, and hence several important reliability metrics. While this can easily be

Frank P.A. Coolen
Department of Mathematical Sciences, Durham University, Durham DH1 3LE, United Kingdom,
e-mail: frank.coolen@durham.ac.uk

Tahani Coolen-Maturi
Department of Mathematical Sciences, Durham University, Durham DH1 3LE, United Kingdom,
e-mail: tahani.maturi@durham.ac.uk

seen as another mathematical concept with little practical relevance, the opposite has always been the intention. This paper presents an introductory overview of the survival signature, with emphasis on practical use and the required additional research to enable this. There are many research challenges to bring the survival signature methodology to fruition for application to large scale real-world systems, this paper aims to discuss recent contributions in this direction and further challenges.

Section 2 of this paper provides a brief introduction to the survival signature. Section 3 discusses the assumption of exchangeability of component failure times, which sits at the heart of the survival signature method. Section 4 discusses some computational issues related to implementing the survival signature, and also aspects of simulation and statistical inference. Section 5 briefly presents recent developments, including resilience through the possibility of swapping components in a system, and new survival signatures for multi-phase systems, for multiple systems which share components, and for multi-state systems. Section 6 concludes the paper with further considerations, including an explanation of the practical need for generalizing the system structure function to be probabilistic and the challenges this brings.

2 Survival Signature

The survival signature was introduced by Coolen and Coolen-Maturi [7]. It is a summary of a system structure function which, together with the probability model for the components' failure times, is sufficient for computing the survival function (also known as reliability function) of the system failure time.

Consider a system with $K \geq 1$ types of components, with n_k components of type $k \in \{1, 2, \ldots, K\}$ and $\sum_{k=1}^{K} n_k = n$. It is crucial to understand what is meant by 'types of components', we discuss this in detail in Section 3, the essential assumption is that the random failure times of components of the same type are exchangeable [16]. The state vector $\underline{x} \in \{0,1\}^n$ of the system describes the states of its components, with 1 representing functioning of a component and 0 that it does not function. The system structure function $\phi(\underline{x}) \in \{0,1\}$ describes the functioning of the system given the component states $\underline{x}$, where 1 represents that the system functions and 0 that it does not function. Due to the arbitrary ordering of the components in the state vector, components of the same type can be grouped together, leading to a state vector that can be written as $\underline{x} = (\underline{x}^1, \underline{x}^2, \ldots, \underline{x}^K)$, with $\underline{x}^k = (x_1^k, x_2^k, \ldots, x_{n_k}^k)$ the sub-vector representing the states of the components of type k.

The *survival signature*, denoted by $\Phi(l_1, l_2, \ldots, l_K)$, with $l_k = 0, 1, \ldots, n_k$ for $k = 1, \ldots, K$, is defined as the probability that the system functions given that *precisely* l_k of its n_k components of type k function, for each $k \in \{1, 2, \ldots, K\}$.

There are $\binom{n_k}{l_k}$ state vectors $\underline{x}^k$ with $\sum_{i=1}^{n_k} x_i^k = l_k$; let S_l^k denote the set of these state vectors for components of type k and let $S_{l_1,\ldots,l_K}$ denote the set of all state vectors for the whole system for which $\sum_{i=1}^{n_k} x_i^k = l_k$, $k = 1, 2, \ldots, K$. Due to the exchangeability assumption for the failure times of the n_k components of type k, all the state vectors $\underline{x}^k \in S_l^k$ are equally likely to occur, hence

$$\Phi(l_1,\ldots,l_K) = \left[\prod_{k=1}^{K}\binom{n_k}{l_k}^{-1}\right] \times \sum_{\underline{x}\in S_{l_1,\ldots,l_K}} \phi(\underline{x}) \tag{1}$$

The survival signature requires specification at $\prod_{k=1}^{K}(n_k+1)$ inputs while the structure function must be specified at 2^n different inputs; in particular for large values of n and relatively small values of K, so large systems with few component types, the difference is enormous. We will comment on computational aspects in Section 4, but note that storage of the structure function may also be a problem for large systems, and this could be substantially easier for the survival signature if there are not many component types. If all components are of different type, so $K = n$, then the survival signature does not provide any advantages, in the sense of reduced representation, over the structure function. If all components are of the same type, so $K = 1$, then the survival function is closely related to Samaniego's system signature [30, 31]. That signature has led to a substantial literature, for example considering properties like stochastic dominance relations between different system lay-outs, but its practical value was limited as most real-world systems consist of multiple types of components. Generalizing Samaniego's system signature to systems with multiple types of components was an open problem which was solved by the introduction of the survival signature [7], which was an important break-through with particular relevance to reliability quantification for real-world systems [32].

Before we present a basic example of the survival signature and discuss further important aspects, we explain why it is a convenient tool for quantification of system reliability. Let $C_k(t) \in \{0,1,\ldots,n_k\}$ denote the number of components of type k in the system which function at time $t > 0$. The probability for the event that the system functions at time $t > 0$, so for $T_S > t$ where T_S is the random system failure time, can be derived by application of the theorem of total probability,

$$\begin{aligned} P(T_S > t) &= \sum_{l_1=0}^{n_1}\cdots\sum_{l_K=0}^{n_K} P(T_S > t | \bigcap_{k=1}^{K}\{C_k(t) = l_k\}) P(\bigcap_{k=1}^{K}\{C_k(t) = l_k\}) \\ &= \sum_{l_1=0}^{n_1}\cdots\sum_{l_K=0}^{n_K} \Phi(l_1,\ldots,l_K) P(\bigcap_{k=1}^{K}\{C_k(t) = l_k\}) \end{aligned} \tag{2}$$

Equation (2) is the essential result at the centre of the survival signature theory. It shows that the system survival function can be computed with the required inputs, namely the information about the system structure and about the component failure times, being completely separated. Hence, the effect of changing a system's structure on its survival function can easily be investigated. One can also compare different system structures in general, without assumptions for the random failure times, by comparing the systems' survival signatures [32]. The system survival function is sufficient for important metrics such as the expected failure time of the system, or its remaining time till failure once it has been functioning for some time. It is important to emphasize that Equation (2) only required the assumption that failure times of components of the same type are exchangeable. This allows dependencies between

components' failure times to be taken into account, which is discussed further in Section 3.

If one assumes that the failure times of components of different types are independent, then Equation (2) becomes

$$P(T_S > t) = \sum_{l_1=0}^{n_1} \cdots \sum_{l_K=0}^{n_K} \left\{ \Phi(l_1, \ldots, l_K) \prod_{k=1}^{K} P(C_k(t) = l_k) \right\} \tag{3}$$

If, in addition, one assumes that the failure times of components of the same type are independent and identically distributed (*iid*), with known cumulative distribution function (*CDF*) $F_k(t)$ for type k, then this leads to

$$P(T_S > t) = \sum_{l_1=0}^{n_1} \cdots \sum_{l_K=0}^{n_K} \left\{ \Phi(l_1, \ldots, l_K) \prod_{k=1}^{K} \binom{n_k}{l_k} [F_k(t)]^{n_k - l_k} [1 - F_k(t)]^{l_k} \right\} \tag{4}$$

In many reliability scenarios one may have a good idea about suitable parametric probability distributions for components' failure times, and one may wish to use statistical inference methods for the unknown parameter. Using general notation $F_k(t|\theta_k)$ for the CDF with parameter θ_k (which can be multi-dimensional) for the failure times of components of type k, and the assumption that the component failure times are conditionally independent and identically distributed (*ciid*), where the conditioning is with respect to the parameter value, the previous equation becomes

$$\begin{aligned} &P(T_S > t|\theta_1, \ldots, \theta_K) = \\ &\sum_{l_1=0}^{n_1} \cdots \sum_{l_K=0}^{n_K} \left\{ \Phi(l_1, \ldots, l_K) \prod_{k=1}^{K} \binom{n_k}{l_k} [F_k(t|\theta_k)]^{n_k - l_k} [1 - F_k(t|\theta_k)]^{l_k} \right\} \end{aligned} \tag{5}$$

This equation can be used in a Bayesian statistical approach to system reliability, where prior distributions for the θ_k are required, as illustrated by Aslett et al. [4].

The survival signature can be applied for any system if the components and the system itself all have two states, functioning or not. If the system is coherent, which means that $\phi(\underline{x})$ is not decreasing in any of the components of $\underline{x}$, then the survival signature is an increasing function, which has substantial advantages as will be discussed in Section 4. While there has been quite some attention in the reliability theory literature to non-coherent systems, most practical systems are coherent. Typical examples of non-coherent systems in the literature are such that two component failures cancel each other out, but in practice such situations are likely to lead to a different overall state of the system compared to its state when the two components involved function properly, and this may require a more detailed system state description than simply functioning or not.

As a basic example of the survival signature, consider the system in Figure 1, for which the survival signature is given in Table 1. Verification of the survival signature is straightforward as the structure function can be easily derived for this small system.

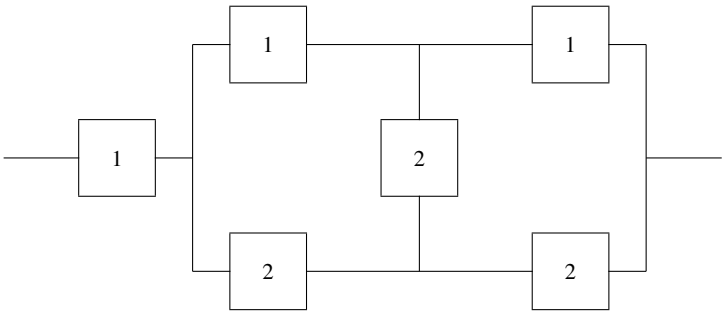

Fig. 1 System with 2 types of components

l_1	l_2	$\Phi(l_1, l_2)$	l_1	l_2	$\Phi(l_1, l_2)$
0	0	0	2	0	0
0	1	0	2	1	0
0	2	0	2	2	4/9
0	3	0	2	3	6/9
1	0	0	3	0	1
1	1	0	3	1	1
1	2	1/9	3	2	1
1	3	3/9	3	3	1

Table 1 Survival signature of the system in Figure 1

3 Exchangeability of components' failure times

As explained in Section 2, the key assumption underlying the survival signature is that the random failure times of components of the same type are exchangeable, so this defines what it means that components are of the same type. What does this mean?

In De Finetti's theory of probability [16], two random quantities, X and Y, are exchangeable if $P(X = x, Y = y) = P(Y = x, X = y)$ for all possible x and y, and similarly generalized to more than two random quantities. So, X and Y have the same marginal distributions, but it is important to emphasize that they do not need to be independent. Exchangeability is an important concept in Bayesian statistics when one wishes to learn about one random quantity by observing another one [16]. In a system reliability setting, exchangeability of the failure times of the n_k components of type k is perhaps easiest understood as follows: If you learn that one component

of type k in the system has failed, you do not know which component it is, and you consider each of these n_k components to have probability $1/n_k$ to be the failed component. This should hold at any moment in time, and generalizes logically to any subset of these components having failed, which must have the same probability independent of which specific components of type k are in the subset. A crucial consideration here is that this is likely to depend not only on the physical nature of the components, e.g. if they are all produced by the same manufacturer, but it also depends on the specific functioning in the system. For example, if one knows that of all components of type k in the system, one has a larger load and hence is more prone to failure, then one would doubt that the assumption of exchangeability of their failure times is appropriate.

The assumption of exchangeability of components' failure times raises a crucial issue for practical quantification of system reliability and related decision support, namely at which level of detail one should model the system. Despite the huge literature on system reliability, this topic has received very little attention. For a large practical system with many components, one may wish to consider the failure times of a group of components to be exchangeable, and hence judge these components to be of the same type, even though one could describe the components' requirements and functioning in so much detail that one could distinguish between their probabilities of failing at specific times. In such a case, the exchangeability assumption would be motivated by a decision not to include more details of the components in the model, and it is important to realize that a model is not identical to the system in its real world functioning, but a reduced representation which should be of sufficient quality for its task, which is often support of a specific decision or trust in failure-free functioning of the system over a period of time. For example, if we wish to consider reliability of a large rail network, we may judge different stretches of rails, of the same length, to have exchangeable failure times even though environmental aspects could enable us to distinguish between them, and could make a failure more likely to occur at one stretch than another.

So, the decision to consider different components to be of the same type, and therefore to have exchangeable failure times, is directly related to the choice of the level of detail in the reliability model. How to decide the appropriate level of detail? This is particularly important for large real world systems, and the answer depends on the task, so the reason of creating the reliability model in the first place, and the available information. But it also depends on time and budget available for the modelling, and the expected benefits which perhaps can also be expressed in terms of money, reduced risk or benefits which may be harder to measure and quantify. Research on this important topic is best done in direct relation to a real reliability study for a large system, as it requires meaningful inputs from management and details of the system. While we have not engaged in such research, a study with similarities was part of a long term collaboration the first author had with an industrial partner about two decades ago, where to support software testers in their complicated tasks a statistical approach based on Bayesian graphical models was developed [12, 35]. These models also required assumptions of exchangeability, which in that setting meant that possible software failures were deemed to be exchangeable, and a project

viability approach was developed that would enable managers to decide, before start of such a study, the level of detail of the model in order to support testers whilst staying within budget and time constraints [11, 36]. Similar guidance on decisions about the level of modelling for large scale system reliability studies is much needed, the fact that the survival signature methodology explicitly requires exchangeability of components' failure times to be considered ensures that it fits with the natural questions one needs to answer when choosing a suitable level of model detail. A further challenging research topic is the practical need to zoom in on problem areas, once these become apparent during the system's functioning. Indeed, there are many great research challenges in this topic area, several more are discussed later in this paper.

A further modelling decision is needed with regard to dependence of components' failure times. As emphasized, components of the same type must have exchangeable failure times for the survival signature approach, and these can be dependent. Furthermore, failure times of components of different types can also be dependent. As explained in Section 2, the general formula for the system survival function is Equation (2), different assumptions on the components' failure times can lead to simplifications of this equation. In practice, there can be many reasons for modelling components' failure times as dependent, for example there may be common-cause failure modes, a risk of cascading failures, load sharing between components and so on. Initial studies into several of such possibilities have been published [8, 17, 18], but there are many related research topics left. The main conclusion is that the separation of the system structure and the random components' failure times, in Equation (2), enables all required dependencies between failure times to be included in the investigation, but the detailed modelling requires of course an extra effort compared to the simpler situation of independent failure times.

4 Computation, simulation and inference

An immediate question for application of the survival signature is how to compute it. For very small systems, like the one in the example in Section 2, one can simply derive the system structure function and use Equation (1). This approach can be applied to somewhat larger systems as well, supported by standard computational methods for the structure function, based on cut sets and path sets. This approach has been implemented in R [2], and can be used without problems for systems of about 20 components with relatively little computational effort, and for somewhat larger systems as well although the computational effort increases enormously. Reed [27] presented a substantial improvement on the required computation time by using binary decision diagrams, which however still requires the availability of the full structure function. While the survival signature provides advantages over the full structure function, mainly in terms of storage requirements but also when one wishes to simulate system failure times, as will be discussed later in this section, the main idea of introducing the survival signature was to enable inference on system reliability

for large real world systems, for which one normally would not have the full structure function available.

There are already some opportunities to make the computational demands somewhat less daunting than one may fear. Of course, brute computational force can be applied to compute the structure function, and from this the survival signature, for larger systems, as computational powers are ever increasing and, crucially, a system's survival signature only needs to be computed once. Coolen et al. [10] provide a simple combinatorial expression to compute the survival signature of a system consisting of two subsystems in either series or parallel configuration, if the survival signatures of those subsystems are available. By repeated application this implies that computation of large series-parallel systems can quite easily be implemented. They also addressed the issue of re-computing a survival signature if a component is replaced and the new component is to be considered as being of a new type. For very large systems, it may be sufficient to use either an approximation to the survival signature, or bounds for it. This is particularly feasible for coherent systems because their survival signatures are increasing functions. It will also be of interest to explore the use of modern simulation and emulation methods to find the part of the entire input space where the function actually increases from 0 to 1. It should be noted that many modern engineering systems, or systems in other application fields such as social-economic systems or computer networks, tend to have some but not very much redundancy, such knowledge can of course also help in computing the survival signature or suitable approximations or bounds for it. This is a substantial area for research with huge possible impact.

The survival signature enables very efficient simulation to learn the system survival function, as presented by Patelli et al. [26] and extended by George-Williams et al. [20] for inclusion of dependent failures. The key idea is as follows: for a system with n_k components of type k, for $k = 1, \ldots, K$, one simulates n_k component failure times for each type k. Instead of investigating which of these component failure times would actually be the system failure time, and using only that as the output of one simulation run, one orders all these observation times and builds up a full simulated stepwise survival function, which at each of these failure times takes on the value of the survival signature with the corresponding values of the l_k, the number of still functioning components of each type k. This procedure turns out to be very efficient, with all simulated component failure times being used instead of the perhaps more intuitive method where each simulation run only leads to one simulated system failure time [26]. Therefore, this enables fast inference about the system reliability based on only the survival signature and components' failure time distributions, where further details about the exact structure of the system is not needed.

This points to another advantage of the survival signature approach that may prove very valuable in practice, namely that statistical analysis of the system reliability is possible without the need to know the full structure of the system, as long as the survival signature is available, or a good approximation to it. It should be emphasized that the full system structure cannot be deduced from the survival signature if there are many components but relatively few types, except of course in special cases such

as systems without redundancy. Aslett [3] has taken this aspect further and developed a system which enables evaluation of a system's reliability if information held by different parties, namely the manufacturer of the system and the manufacturers of different types of components, is not shared, and cannot even be deduced by the different parties. This work is an important first step towards practical inference about system reliability without the need for major commercial interests to be revealed, and it is only possible through the use of the survival signature as a sufficient summary of the structure function.

Statistical inference for system reliability is a topic of major interest, as learning from data, possibly in combination with the use of expert judgements, is crucial in many applications. If one has data available on the individual component types, then inference on the system's failure time is quite straightforward. Nonparametric predictive inference [6], a frequentist approach using few modelling assumptions made possible by the use of imprecise probabilities [5], can be used to derive bounds for the system survival function [10]. The application of Bayesian methods has been presented as well [4], this is particularly useful if one has relatively little data on component failures and therefore wishes to include expert judgements. Walter et al. [34] generalized the Bayesian approach combined with the survival signature by using sets of priors, as typically done in theory of robust Bayesian methods. They showed that, by choosing the sets of priors in a specific way, one can enable detection of conflict between prior judgements and data, when data become available and are used to update the prior distributions. This can be of great practical importance, as it can point to prior judgements being too optimistic, hence the system reliability may be substantially lower than was originally thought.

A major challenge is development of suitable statistical methodology to learn the survival signature from observations of the system, so from information which can consist of system failure times, component failure times, outcomes of inspections or condition monitoring and so on. Due to the inverse nature of such inferences, Bayesian methods are well placed to enable such learning, and it is likely that one can learn the survival signature far easier than the full structure function. Aslett [1] presented such inverse inference for systems with only a single type of component, using Samaniego's system signature. While conceptually such inference does not pose many problems, it is extremely computationally expensive, so there are substantial research opportunities for useful contributions to the methodology.

5 Recent developments

In recent years, the use of the survival signature has been presented for a range topics in reliability. Component important measures have become popular management tools for guidance on aspects of system reliability, and the survival signature can be used both to assess importance of specific components and importance of components of a specific type [19]. The former requires a bit more information than just the survival signature for the full system, namely two such signatures with

conditioning on the specific component of interest functioning or not. The latter is an interesting difference to the usual idea of component importance measures, where the importance only relates to a specific type of component. For a number of practical decision problems this may be the most relevant information, for example if one needs to decide on immediate availability of spare components in case the system fails, then it may not be crucial to know which specific component is likely to fail next but the type of component to fail next could be most important. Eryilmaz et al. [17] considered marginal and joint component importance for dependent components, while linking survival signatures to logic differential calculus has also been shown to provide useful tools to identify important components in system reliability analysis [28], and the survival signature also enables useful new approaches to sensitivity analysis for system reliability [22]. A challenging problem in system design is reliability-redundancy allocation, where under budget or other constraints a system designer must choose between increasing the quality of components or the level of redundancy in the system. Since it is natural to assume that any quality improvement will equally affect all components of a particular type, it is clear that the survival signature can be used to support such decisions. This was considered by Huang et al. [23], who present a fast heuristic algorithm that provides excellent solutions to the problem and that can be implemented for systems of substantial size, as long as the survival signature, or a good approximation of it, is available. All these developments are initial results, with many related research opportunities including computional challenges to enable upscaling to large real world systems.

A further recent contribution resulted from the practical need to make systems resilient in case things go wrong. The idea was simple: if a system fails due to one or more failing components, it may be possible to swap a failing component with another component in the system which still functions. This approach brought an interesting question with regard to the definition of a component: namely is a component defined as the specific location (or better 'role') in the system, or the part that could actually be moved to another location. It turned out that the latter interpretation is by far easier, as it means that the component does not change its random remaining failure time when moved to another location. The survival signature approach enables quite straightforward investigation of the improvement of the system reliability if specific component swaps are possible [25]. This may be important in practice when such a component swap might provide sufficient time to prepare a substantial maintenance activity on the system.

It is worth to emphasize that, although emphasis and terminology in this paper is mainly on engineering systems, the survival signature methodology can also be applied to systems in other fields, including socio-economic and health systems. Swapping of components could, for example, be relevant in an organisation where staff members can be regarded as components. It may be beneficial if some staff members can take over other roles in case colleagues become ill, and one may want to consider training people to enable such swaps of their roles. There are many related research questions, including the option to swap components of different types or even to swap components which have not yet failed, the latter could make sense if loads vary during different periods of system functioning. As with all topics

discussed here, it will be ideal if practical issues for real world systems can be analysed to guide the further development of theory and methods.

All the contributions to system reliability methodology discussed above use the survival signature in the basic form as given in Equation (2). However, several important practical scenarios require different survival signatures, which can be seen as generalizations of the basic form, due to the increased complexity of the system or its use. We briefly describe three such generalizations, while referring to the respective papers for more details. These new survival signatures are all starting points for substantial further research with regard to similar issues as discussed before in this paper, to ensure wide applicability to real-world systems.

The first scenario for which a generalized survival signature has recently been presented is phased mission systems, which are common in practice as many systems have to perform different tasks sequentially. Huang et al. [21] present a new survival signature for this scenario. The main issue here is that not all components need to function in each phase, so one needs to keep a clear record of any component failures, where it is assumed that a failed component does not function anymore for all remaining phases. While the system's functioning in each phase can be presented by a basic survival signature, the definition of 'components of the same type' needs care, because components that do not need to function in one phase are likely to have different failure behaviour after that phase, compared to similar components which did have to function in that phase. In the earlier literature on phased mission systems, this important aspect seems to have been overlooked, mostly components with exponential failure time distributions seem to have been considered for systems such that all components need to function in each phase. In practice these common assumptions are often unrealistic, the survival signature approach by Huang et al. [21] enables more realistic scenarios to be modelled. Building on that work, Coolen et al. [13] considered the opportunity to swap components within the system, either at the time of system failure or at phase transitions. Huang et al. [24] studied component importance for such phased mission systems using the new survival signature.

A second scenario for which a generalized survival signature has recently been presented, is when multiple systems share some components, which can be of different types. One can think, for example, about multiple computers linked to a single server, or multiple academic departments at one university during an exams period with strict marking deadlines, which all depend on one central information technology support group which can be regarded as a component shared by the different departments. This scenario applies also to the important situation of one system which has to perform multiple functions, and can be further generalized to multiple systems performing multiple functions. Coolen-Maturi et al. [15] have recently presented the survival signature for such situations, which is a major step in the development of the survival signature methodology for large scale practical applications. Crucial in this work is that one may wish to consider the functioning of different systems at different moments in time, where the status of the shared components must be considered at the different time points. This enables inferences on, for example, the probability that one system still functions at a specific time, given that another system with which it shares some components functioned at an

earlier time, or that it had failed at an earlier time, without further information about the status of the shared components.

The third scenario for which a generalized survival signature has recently been presented, is multi-state systems with multi-state components. While the reliability literature has traditionally mainly considered binary state systems and components, many real world scenarios require modelling of multiple states, e.g. including an intermediate state between perfect and not functioning, during which maintenance or replacement of components may be possible. Qin and Coolen [29] present the survival signature methodology for such systems, where the probability distribution of the system over its possible states is considered as function of the numbers of components of all types in the possible states. The computation of the survival signature for this scenario becomes rather complicated, but Qin and Coolen [29] present an efficient algorithm to combine the survival signatures of two subsystems if the state of the system depends only on the states of these subsystems. As is the case for the basic survival signature for binary states [10], repeated application of this algorithm may enable fast computation of the multi-state survival signature for some large systems.

6 Further considerations

There remains a large discrepancy between system reliability as presented in textbooks and many journal papers, and methods needed to assist analysts and managers in real world problems concerning reliability of large systems. These differences are not only the size of the systems typically presented, but also the actual problems studied, where in real life the system survival function is usually only the input to a more complicated decision problem which determines the required level of detail of the system model and accuracy of approximations to the survival function if it cannot be computed exactly. Perhaps the most important difference, however, is that several important aspects of applications of large real world systems tend not to be reflected in typical reliability models and methods, and they lead to additional uncertainties. It is often not clear what is meant by functioning of the system because the specific tasks, or number of tasks, may not be known, or the environment in which the system has to function may not be fully known or indeed be variable. The level of modelling of the system is also difficult in the real world, and it must be possible to study a system's reliability as function of a subset of its components or subsystems. For example, one may want to model reliability of a car as function of its main components like engine, breaks and tyres, but not take into account every minor component that could by itself, or in combination with some other minor components, prevent the car from being used.

We have advocated that, to enhance theory of system reliability and to make it far more flexible for real world use, the system structure function should not be deterministic but probabilistic, so $\phi(\underline{x}) \in [0,1]$ instead of $\phi(\underline{x}) \in \{0,1\}$, which can also be generalized to imprecise probabilities [9], which have proven to be useful in

many reliability problems [14, 33]. This will provide a tool to deal with the additional uncertainties mentioned above. For example, if one only models system reliability as function of some main components, and one wishes to apply statistical inference about the reliability from failure observations, it is quite possible that for the same states of the components included in the model, one has both observed the system to fail and not to fail. In the example of the car mentioned above, one may not have included the car's heating system as a component in the system reliability model, but if the task at hand is to drive a long distance on a very cold winter day, its failure may prevent the car from being used even though all main components function. This example also illustrates the problem of defining the system's functioning and possible uncertainty about the tasks and environment in which it needs to operate.

Moving from deterministic to probabilistic structure function seems mathematically quite straightforward, and the good news from the perspective of this paper is that it would not provide any difficulties for the survival signature approach, as Equation (1) can still be used if the structure function is a probability, and if imprecise probabilities are used then the generalization is also straightforward. The main challenges, however, are with probabilistic structure functions themselves. Clearly, the probabilities would need to be assessed, which may require creating models to do so, and computations to derive a structure function will require new theory to be developed because concepts like path sets and cut sets do not carry over to probabilistic structure functions.

There are great opportunities for application of the survival signature methodology to networks, an initial example was presented by Aslett et al. [4]. These can be regarded as systems, and typically have at least two types of components, namely nodes and links between nodes. However, networks typically require many different routes through the network to be available, but there may be possibilities to use some alternative routes that would still be satisfactory. Due to the huge importance of reliability networks in modern life and the fact that they tend to be large but often have a limited number of component types, this promises to be an application area where the survival signature can make very substantial contributions, and which in turn can guide future research to extend the survival signature methodologically in meaningful directions.

Acknowledgements This paper is closely related to a presentation at The International Workshop on Reliability Engineering and Computational Intelligence (October 2020). We thank the organisers, in particular Elena Zaitseva, for the invitation to present our work.

References

1. Aslett, L.J.M. (2012). MCMC for Inference on Phase-type and Masked System Lifetime Models. PhD Thesis, Trinity College Dublin.
2. Aslett, L.J.M. (2012). ReliabilityTheory: Tools for structural reliability analysis. R package, *www.louisaslett.com*

3. Aslett, L.J.M. (2016). Cryptographically secure multiparty evaluation of system reliability. arXiv:1604.05180 [cs.CR].
4. Aslett, L.J.M., Coolen, F.P.A., Wilson, S.P. (2015). Bayesian inference for reliability of systems and networks using the survival signature. Risk Analysis 35, 1640-1651.
5. Augustin, T., Coolen, F.P.A., de Cooman, G., Troffaes, M.C.M. (Eds) (2014). Introduction to Imprecise Probabilities. Wiley, Chichester.
6. Coolen, F.P.A. (2011). Nonparametric predictive inference. In: International Encyclopedia of Statistical Science, Editor: Lovric. Springer, pp. 968-970.
7. Coolen, F.P.A., Coolen-Maturi, T. (2012). On generalizing the signature to systems with multiple types of components. In: Complex Systems and Dependability, Editors: Zamojski, Mazurkiewicz, Sugier, Walkowiak, Kacprzyk. Springer, pp. 115-130.
8. Coolen, F.P.A., Coolen-Maturi, T. (2015). Predictive inference for system reliability after common-cause component failures. Reliability Engineering and System Safety 13, 27-33.
9. Coolen, F.P.A., Coolen-Maturi, T. (2016). The structure function for system reliability as predictive (imprecise) probability. Reliability Engineering and System Safety 154, 180-187.
10. Coolen, F.P.A., Coolen-Maturi, T., Al-nefaiee, A.H. (2014). Nonparametric predictive inference for system reliability using the survival signature. Journal of Risk and Reliability 228, 437-448.
11. Coolen, F.P.A., Goldstein, M., Wooff, D.A. (2003). Project viability assessment for support of software testing via Bayesian graphical modelling. In: Safety and Reliability (Proceedings ESREL'03), Editors: Bedford, van Gelder. Swets & Zeitlinger, pp. 417-422.
12. Coolen, F.P.A., Goldstein, M., Wooff, D.A. (2007). Using Bayesian statistics to support testing of software systems. Journal of Risk and Reliability 221, 85-93.
13. Coolen, F.P.A., Huang, X., Najem, A. (2020). Reliability analysis of phased mission systems when components can be swapped upon failure. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems - Part B: Mechanical Engineering, June 2020, 6(2): 020905.
14. Coolen, F.P.A., Utkin, L.V. (2011). Imprecise reliability. In: International Encyclopedia of Statistical Science, Editor: Lovric. Springer, pp. 649-650.
15. Coolen-Maturi, T., Coolen, F.P.A., Balakrishnan, N. The joint survival signature of coherent systems with shared components. In submission.
16. De Finetti, B. (1974). Theory of Probability (2 Vols). Wiley, Chichester.
17. Eryilmaz, S., Coolen, F.P.A., Coolen-Maturi, T. (2018). Marginal and joint reliability importance based on survival signature. Reliability Engineering and System Safety 172, 118-128.
18. Eryilmaz, S., Coolen, F.P.A., Coolen-Maturi, T. (2018). Mean residual life of coherent systems consisting of multiple types of dependent components. Naval Research Logistics 65, 86-97.
19. Feng, G., Patelli, E., Beer, M., Coolen, F.P.A. (2016). Imprecise system reliability and component importance based on survival signature. Reliability Engineering and System Safety 150, 116-125.
20. George-Williams, H., Feng, G., Coolen, F.P.A., Beer, M., Patelli, E. (2019). Extending the survival signature paradigm to complex systems with non-repairable dependent failures. Journal of Risk and Reliability 233, 505-519.
21. Huang, X., Aslett, L.J.M., Coolen, F.P.A. (2019). Reliability analysis of general phased mission systems with a new survival signature. Reliability Engineering and System Safety 189, 416-422.
22. Huang, X., Coolen, F.P.A. (2018). Reliability sensitivity analysis of coherent systems based on survival signature. Journal of Risk and Reliability 232, 627-634.
23. Huang, X., Coolen, F.P.A., Coolen-Maturi, T. (2019). A heuristical survival signature based approach for reliability-redundancy allocation. Reliability Engineering and System Safety 185, 511-517.
24. Huang, X., Coolen, F.P.A., Coolen-Maturi, T., Zhang, Y. (2020). A new study on reliability importance analysis of phased mission systems. IEEE Transactions on Reliability 69, 522-532.
25. Najem, A., Coolen, F.P.A. (2019). System reliability and component importance when components can be swapped upon failure. Applied Stochastic Models in Business and Industry 35, 399-413.

26. Patelli, E., Feng, G., Coolen, F.P.A., Coolen-Maturi, T. (2017). Simulation methods for system reliability using the survival signature. Reliability Engineering and System Safety 167, 327-337.
27. Reed, S. (2017). An efficient algorithm for exact computation of system and survival signatures using binary decision diagrams. Reliability Engineering and System Safety 165, 257-267.
28. Rusnak, P., Zaitseva, E., Coolen, F.P.A., Kvassay, M., Levashenko, V. Logic differential calculus for reliability analysis based on survival signature. In submission.
29. Qin, J., Coolen, F.P.A. Survival signature for reliability evaluation of a multi-state system with multi-state components. In submission.
30. Samaniego, F.J. (1985). On closure of the IFR class under formation of coherent systems. IEEE Transactions on Reliability 34, 69-72.
31. Samaniego, F.J. (2007). System signatures and their applications in engineering reliability. Springer, New York.
32. Samaniego, F.J., Navarro, J. (2016). On comparing coherent systems with heterogeneous components. Advances in Applied Probability 48, 88-111.
33. Utkin, L.V., Coolen, F.P.A. (2007). Imprecise reliability: an introductory overview. In: Computational Intelligence in Reliability Engineering, Volume 2: New Metaheuristics, Neural and Fuzzy Techniques in Reliability, Editor: Levitin. Springer, pp. 261-306.
34. Walter, G., Aslett, L.J.M., Coolen, F.P.A. (2017). Bayesian nonparametric system reliability using sets of priors. International Journal of Approximate Reasoning 80, 67-88.
35. Wooff, D.A., Goldstein, M., Coolen, F.P.A. (2002). Bayesian graphical models for software testing. IEEE Transactions on Software Engineering 28, 510-525.
36. Wooff, D.A., Goldstein, M., Coolen, F.P.A. (2018). Bayesian graphical models for high complexity testing: aspects of implementation. In: Analytic Methods in Systems and Software Testing, Editors: Kenett, Ruggeri, Faltin. Wiley, pp. 213-243.