Reliability Engineering and System Safety 124 (2014) 171–200

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

# Probability of loss of assured safety in systems with multiple time-dependent failure modes: Representations with aleatory and epistemic uncertainty

Jon C. Helton [a,*], Martin Pilch [b], Cédric J. Sallaberry [c]

[a] Department of Mathematics and Statistics, Arizona State University, Tempe, AZ 85287-1804, USA
[b] Thermal Sciences and Engineering Department, Sandia National Laboratories, Albuquerque, NM 87185-0828, USA
[c] Applied Systems Analysis and Research Department, Sandia National Laboratories, Albuquerque, NM 87185-0748, USA

ARTICLE INFO

*Article history:*
Received 12 March 2013
Received in revised form
18 October 2013
Accepted 26 November 2013
Available online 4 December 2013

*Keywords:*
Aleatory uncertainty
Epistemic uncertainty
Probability of loss of assured safety
Strong link
Uncertainty analysis
Weak link

ABSTRACT

Weak link (WL)/strong link (SL) systems are important parts of the overall operational design of high-consequence systems. In such designs, the SL system is very robust and is intended to permit operation of the entire system under, and only under, intended conditions. In contrast, the WL system is intended to fail in a predictable and irreversible manner under accident conditions and render the entire system inoperable before an accidental operation of the SL system. The likelihood that the WL system will fail to deactivate the entire system before the SL system fails (i.e., degrades into a configuration that could allow an accidental operation of the entire system) is referred to as probability of loss of assured safety (PLOAS). Representations for PLOAS for situations in which both link physical properties and link failure properties are time-dependent are derived and numerically evaluated for a variety of WL/SL configurations, including PLOAS defined by (i) failure of all SLs before failure of any WL, (ii) failure of any SL before failure of any WL, (iii) failure of all SLs before failure of all WLs, and (iv) failure of any SL before failure of all WLs. The indicated formal representations and associated numerical procedures for the evaluation of PLOAS are illustrated with example analyses involving (i) only aleatory uncertainty, (ii) aleatory uncertainty and epistemic uncertainty, and (iii) mixtures of aleatory uncertainty and epistemic uncertainty.



## 1. Introduction

Weak link (WL)/strong link (SL) systems are important parts of the overall operational design of high-consequence systems [1–6]. In such designs, the SL system is very robust and is intended to permit operation of the entire system under, and only under, intended conditions (e.g., by transmitting a command to activate the system). In contrast, the WL system is intended to fail in a predictable and irreversible manner under accident conditions (e.g., in the event of a fire) and render the entire system inoperable before an accidental operation of the SL system. Possible configurations of a WL/SL system with one WL and one SL are illustrated in Fig. 1 of Ref. [7].

The likelihood that the WL system will fail to deactivate the entire system before the SL system fails (i.e., degrades into a configuration that could allow an accidental operation of the entire system) is referred to as probability of loss of assured safety (PLOAS). The descriptor loss of assured safety (LOAS) is used because failure of the WL system places the entire system in an inoperable configuration while failure of the SL system, although undesirable, does not necessarily result in an unintended operation of the entire system. Thus, safety is "assured" by failure of the WL system. In the context of accident conditions, the descriptor "failure of the WL system" is an oxymoron as such failure is actually a success in the sense that it results in a desired deactivation of the entire system.

An electrical circuit with two switches provides a simple example of a WL/SL system, where (i) one switch (i.e., the SL) must close to allow the transmission of a signal to initiate a potentially dangerous operation and (ii) the other switch (i.e., the WL) is closed under normal conditions but is intended to open under accident conditions (e.g., in the event of an electrical surge) and thus prevent the possible transmission of a signal to initiate the indicated operation. The closing of the SL switch under accident conditions without the opening of the WL switch corresponds to LOAS because this places the system in a configuration that could allow the unintended transmission of a signal to initiate the indicated operation. In turn, PLOAS corresponds to the conditional probability that, under accident conditions, the SL switch closes before the WL switch opens.

Two previous publications [7,8] develop time-dependent values $pF(t)$ for PLOAS for accidents involving fire for a variety of

* Correspondence to: Department 1514, Sandia National Laboratories, Albuquerque, NM 87185-0748, USA. Tel.: +1 505 284 4808.
*E-mail address:* jchelto@sandia.gov (J.C. Helton).

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.11.012

WL/SL configurations (Table 1). Further, two related publications [9,10] develop verification test problems for the PLOAS representations in Refs. [7,8]. The test problems involve assigning the same failure properties to all links, which results in (i) the same cumulative distribution function (CDF) for link failure time for all links and (ii) the indicated verification values shown in Table 1. The verification problems entail an exercising of all the conceptual development and numerical procedures underlying the PLOAS representations in Table 1 and yet have the simple numerical values for PLOAS shown in Table 1.

As illustrated in this presentation, the separation of aleatory uncertainty and epistemic uncertainty is an important part of appropriately designed analyses for complex systems [11–14]. Specifically, aleatory uncertainty arises from an inherent variability in the behavior of the system under study (e.g., the variability in the possible properties of a manufactured item or the possible weather conditions at the time of an accident). In contrast, epistemic uncertainty arises from a lack of knowledge about the true value of a quantity that has a fixed, but poorly known, value in the context of a specific analysis (e.g., the failure strength of an existing structure or a parameter in a distribution used to characterize aleatory uncertainty). Maintaining a distinction between aleatory uncertainty and epistemic uncertainty is important as the presence of this distinction makes it possible to communicate the effects and implications of (i) random variability that is known to exist in the behavior of the system under study and (ii) a lack of knowledge about the appropriate values to use for system properties that are believed to have fixed values. Additional discussion of the role of aleatory uncertainty and epistemic uncertainty in the analysis of complex systems is available in a number of presentations (e.g., [15–22]). With respect to terminology, probabilistic risk assessments for nuclear power plants that maintain a separation of aleatory uncertainty and epistemic uncertainty are sometimes described as using a "probability of frequency" approach owing to the use of (i) frequencies to characterize the aleatory uncertainty in the occurrence of initiating events for nuclear power plant accidents and (ii) probability to characterize epistemic uncertainty [23–25].

**Table 1**
Representation of time-dependent values $pF_i(t)$, $i=1, 2, 3, 4$, for PLOAS and associated verification tests for alternate definitions of LOAS for WL/SL systems with (i) $nWL$ WLs and $nSL$ SLs and (ii) independent distributions for link failure time ([8], Table 10).

Case 1: failure of all SLs before failure of any WL (Eqs. (2.1) and (2.5), Ref. [10])

$$pF_1(t) = \sum_{k=1}^{nSL} \left( \int_0^t \left\{ \prod_{\substack{l=1 \\ l \neq k}}^{nSL} CDF_{SL,l}(\tau) \right\} \left\{ \prod_{j=1}^{nWL} [1 - CDF_{WL,j}(\tau)] \right\} dCDF_{SL,k}(\tau) \right)$$

Verification test: $pF_1(\infty) = nWL!nSL!/(nWL+nSL)!$

Case 2: Failure of any SL before failure of any WL (Eqs. (3.1) and (3.4), Ref. [10])

$$pF_2(t) = \sum_{k=1}^{nSL} \left( \int_0^t \left\{ \prod_{\substack{l=1 \\ l \neq k}}^{nSL} [1 - CDF_{SL,l}(\tau)] \right\} \left\{ \prod_{j=1}^{nWL} [1 - CDF_{WL,j}(\tau)] \right\} dCDF_{SL,k}(\tau) \right)$$

Verification test: $pF_2(\infty) = nSL/(nWL+nSL)$

Case 3: Failure of all SLs before failure of all WLs (Eqs. (4.1) and (4.4), Ref. [10])

$$pF_3(t) = \sum_{k=1}^{nSL} \left( \int_0^t \left\{ \prod_{\substack{l=1 \\ l \neq k}}^{nSL} CDF_{SL,l}(\tau) \right\} \left\{ 1 - \prod_{j=1}^{nWL} CDF_{WL,j}(\tau) \right\} dCDF_{SL,k}(\tau) \right)$$

Verification test: $pF_3(\infty) = nWL/(nWL+nSL)$

Case 4: Failure of any SL before failure of all WLs (Eqs. (5.1) and (5.4), Ref. [10])

$$pF_4(t) = \sum_{k=1}^{nSL} \left( \int_0^t \left\{ \prod_{\substack{l=1 \\ l \neq k}}^{nSL} [1 - CDF_{SL,l}(\tau)] \right\} \left\{ 1 - \prod_{j=1}^{nWL} CDF_{WL,j}(\tau) \right\} dCDF_{SL,k}(\tau) \right)$$

Verification test: $pF_4(\infty) = 1 - [nWL!nSL!/(nWL+nSL)!]$

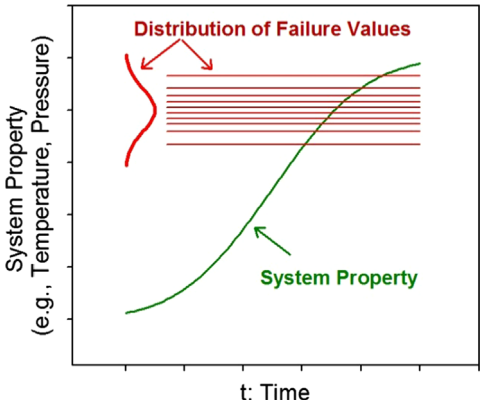


**Fig. 1.** Notional example of a time-dependent system property (e.g., temperature or pressure) and a corresponding distribution of failure values.

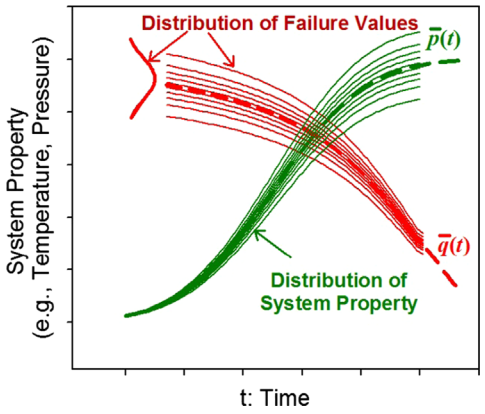


**Fig. 2.** Notional example of a distribution for a time-dependent system property (e.g., temperature or pressure) and a corresponding distribution for time-dependent failure values.

The PLOAS values developed in Refs. [7,8] derive from aleatory uncertainty (i.e., random variability) in the failure temperatures for the individual links. As illustrated in the notional example of Fig. 1, there is a distribution of possible failure values for the link under consideration, with link failure occurring when the temperature curve reaches a failure temperature. In turn, the distribution of failure temperatures leads to a distribution of failure times and a corresponding CDF for link failure time (i.e., $CDF(t)$ is the probability of link failure at or before time $t$). In the development of Ref. [7], a link is assumed to fail at the instant that its failure temperature is reached; Ref. [8] treats the more general situation in which there is a delay between when a link reaches its failure temperature and when the link actually fails. These differences affect the definitions of the CDFs for link failure time; however, once these CDFs are obtained, PLOAS can be determined as indicated in Table 1 for both definitions of link failure time.

The developments in Refs. [7–10] always refer to the link properties under consideration as temperature. However, there is nothing in the development of the results in Table 1 that is specific to temperature. The results hold for any time-dependent property that has the potential to cause link failure. Further, different properties could be associated with the failure of different links. For example, some links might fail on the basis of temperature while other links fail on the basis of pressure or some other system property. Whatever the failure modes are for the individual links, PLOAS can be determined as indicated in Table 1 once the CDFs for failure time are determined.

The results contained in this presentation extend the results in Ref. [7] in three ways. First, aleatory uncertainty is assumed to be