Reliability Engineering and System Safety 94 (2009) 294–310

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Effect of delayed link failure on probability of loss of assured safety in temperature-dependent systems with multiple weak and strong links

J.C. Helton [a,*], J.D. Johnson [b], W.L. Oberkampf [c]

[a] Department of Mathematics and Statistics, Arizona State University, Tempe, AZ 85287-1804, USA
[b] ProStat, Mesa, AZ 85204-5326, USA
[c] Sandia National Laboratories, Albuquerque, NM 87185-0828, USA

ARTICLE INFO

Article history:
Received 27 July 2007
Accepted 16 March 2008
Available online 18 March 2008

Keywords:
Aleatory uncertainty
Competing failure
Competing risk
Delayed failure
Fire environment
High-consequence system
Probability of loss of assured safety
Reliability
Strong link
Weak link

ABSTRACT

Weak link (WL)/strong link (SL) systems constitute important parts of the overall operational design of high-consequence systems, with the SL system designed to permit operation of the system only under intended conditions and the WL system designed to prevent the unintended operation of the system under accident conditions. Degradation of the system under accident conditions into a state in which the WLs have not deactivated the system and the SLs have failed in the sense that they are in a configuration that could permit operation of the system is referred to as loss of assured safety. The probability of such degradation conditional on a specific set of accident conditions is referred to as probability of loss of assured safety (PLOAS). Previous work has developed computational procedures for the calculation of PLOAS under fire conditions for a system involving multiple WLs and SLs and with the assumption that a link fails instantly when it reaches its failure temperature. Extensions of these procedures are obtained for systems in which there is a temperature-dependent delay between the time at which a link reaches its failure temperature and the time at which that link actually fails.

1. Introduction

Weak link (WL)/strong link (SL) systems constitute important parts of the 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 inoperational 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].

An important property associated with WL/SL systems is the probability of loss of assured safety (PLOAS). Specifically, PLOAS is the probability conditional on a specific accident (e.g., a fire with well-defined properties) that the WL system fails to deactivate the entire system before the SL system fails in a manner that could allow an unintended operation of the entire system. A previous presentation has developed representations for PLOAS for accidents involving fire for a variety of WL/SL configurations [7]. Further, two related presentations consider the verification of calculations to determine PLOAS [8,9].

A fundamental assumption in the representations for PLOAS studied in Refs. [7–10] is that a link fails instantly when it reaches its failure temperature. The purpose of this presentation is to study representations for PLOAS obtained with the assumption that there is a delay between the time when a link reaches its failure temperature and the time at which the link actually fails.

The presentation is organized as follows. First, results obtained in Ref. [7] for PLOAS when there is no delay in link failure are briefly reviewed (Section 2). Then, results with constant delays in link failure are presented for systems with one WL and one SL (Section 3) and more generally for systems with *nWL* WLs and *nSL* SLs (Section 4). Next, the numerical calculation of PLOAS is illustrated with both quadrature-based and sampling-based procedures (Section 5). Then, the representation of PLOAS for systems with temperature-dependent delays in link failure is described for systems with one WL and one SL (Section 6) and also for systems with *nWL* WLs and *nSL* SLs (Section 7), and the numerical calculation of PLOAS for such systems is illustrated (Section 8). Next, the verification of PLOAS calculations is discussed and illustrated (Section 9). Through Section 9, loss of assured safety is assumed to correspond to the failure of all SLs before the failure of any WL. The calculation of PLOAS for other definitions of loss of assured safety is discussed and illustrated in

* Corresponding author at: Department 1544, MS 0776, Sandia National Laboratories, Albuquerque, NM 87185-0776, USA. Tel.: +1 505 284 4808; fax: +1 505 844 2348.
E-mail address: jchelto@sandia.gov (J.C. Helton).

0951-8320/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2008.03.007

Section 10. Finally, the presentation ends with a brief summary (Section 11).

The determination of PLOAS for WL/SL systems falls in the broader area of study for engineered systems known as competing risk analysis or, equivalently, competing failure analysis [11–14].

2. No failure delay

The simplest WL/SL configuration considered in Ref. [7] is one WL and one SL. For this configuration, the value *pF* for PLOAS under fire conditions has several equivalent integral representations (Table 1). The representations for *pF* in Table 1 are based on the assumptions that (i) a single fire giving rise to the time–temperature functions $TMPWL(t)$ and $TMPSL(t)$ is under consideration, (ii) the functions $TMPWL(t)$ and $TMPSL(t)$ are nondecreasing, (iii) the density functions $fWL(T_{SL})$ and $fSL(T_{SL})$ characterize uncertainty (e.g., variability in a population of WL/SL systems) in WL and SL failure temperatures, (iv) a link fails instantly when it reaches its failure temperature, and (v) PLOAS corresponds to the SL failing before the WL.

The representations for *pF* in Table 1 are derived in Section 2.1 of Ref. [7]. Specifically, the first integral in Table 1 represents *pF* with a Stieltjes integral involving time (i.e., an integral of the form $\int_a^b f(t)\,\mathrm{d}g(t)$; see Section 2.9 of Ref. [15]); the second integral represents *pF* with the corresponding Riemann integral on time (i.e., an integral of the form $\int_a^b f(t)g'(t)\,\mathrm{d}t$; see Theorem 29.8, p. 200, of Ref. [15]); the third integral represents *pF* with a Riemann integral on SL failure temperature that is obtained from the second integral through a change of variables; and the final integral involving $G(T_{SL})$ provides a representation for *pF* that facilitates the description and implementation of a quadrature-based approximation to *pF*.

A more complex WL/SL configuration considered in Ref. [7] involves *nWL* WLs and *nSL* SLs with loss of assured safety occurring when all SLs fail before any WL fails. Similarly to the representations for *pF* for the one WL, one SL configuration in Table 1, the value *pF* for PLOAS under fire conditions for this configuration has several equivalent integral representations (Table 2). The representations for *pF* in Table 2 are based on the assumptions that (i) a single fire giving rise to the time–temperature functions $TMPWL_j(t)$ and $TMPSL_k(t)$ is under consideration, (ii) the functions $TMPWL_j(t)$ and $TMPSL_k(t)$ are nondecreasing, (iii) the density functions $fWL_j(T_{WL})$ and $fSL_k(T_{SL})$ characterize uncertainty in WL and SL failure temperatures, (iv) a link fails instantly when it reaches its failure temperature, and (v) PLOAS corresponds to all SLs failing before any WL fails.

Table 1
Representation of value *pF* for PLOAS under fire conditions for a WL/SL system with one WL, one SL, and the assumptions that (i) a link fails instantly when it reaches its failure temperature and (ii) loss of assured safety corresponds to the SL failing before the WL

$$
\begin{aligned}
pF &= \int_{tMIN}^{tMAX} \{fSL[TMPSL(t)]\}\{I[TMPWL(t),\ \infty,\ fWL]\}\,\mathrm{d}TMPSL(t)\\
&= \int_{tMIN}^{tMAX} \{fSL[TMPSL(t)]\}\{\mathrm{d}TMPSL(t)/\mathrm{d}t\}\{I[TMPWL(t),\ \infty,\ fWL]\}\,\mathrm{d}t\\
&= \int_{TMNSL}^{TMXSL} \{fSL[T_{SL}]\}\left\{I\left[TMPWL[TMPSL^{-1}(T_{SL})],\ \infty,\ fWL\right]\right\}\mathrm{d}T_{SL}\\
&= \int_{TMNSL}^{TMXSL} G(T_{SL})\,\mathrm{d}T_{SL},
\end{aligned}
$$

where
$I[a,b,f]=\int_a^b f(T)\,\mathrm{d}T$
$fSL(T_{SL})$ = density function ($^\circ C^{-1}$) for SL failure temperature,
$fWL(T_{WL})$ = density function ($^\circ C^{-1}$) for WL failure temperature,
$TMPSL(t)$ = SL temperature ($^\circ$C) at time t for $tMIN \leqslant t \leqslant tMAX$,
$TMPWL(t)$ = WL temperature ($^\circ$C) at time t for $tMIN \leqslant t \leqslant tMAX$,
$TMNSL = TMPSL\ (tMIN)$,
$TMXSL = TMPSL\ (tMAX)$,
$G(T_{SL}) = fSL(T_{SL})I\left[TMPWL[TMPSL^{-1}(T_{SL})],\infty,fWL\right]$

Table 2
Representation of value *pF* for PLOAS under fire conditions for a WL/SL system with *nWL* WLs, *nSL* SLs, and the assumptions that (i) a link fails instantly when it reaches its failure temperature and (ii) loss of assured safety corresponds to all SLs failing before any WL fails (adapted from Table 2, Ref. [9])

$$
\begin{aligned}
pF &= \sum_{k=1}^{nSL}\left(\int_{tMIN}^{tMAX}\{fSL_k[TMPSL_k(t)]\}\left\{\prod_{\substack{l=1\\ l\neq k}}^{nSL} I[-\infty,\ TMPSL_l(t),\ fSL_l]\right\}\right.\\
&\qquad\left.\times\left\{\prod_{j=1}^{nWL} I[TMPWL_j(t),\ \infty,\ fWL_j]\right\}\mathrm{d}TMPSL_k(t)\right)\\
&= \int_{tMIN}^{tMAX}\left(\sum_{k=1}^{nSL}\{fSL_k[TMPSL_k(t)]\}\left\{\prod_{\substack{l=1\\ l\neq k}}^{nSL} I[-\infty,\ TMPSL_l(t),\ fSL_l]\right\}\{\mathrm{d}TMPSL_k(t)/\mathrm{d}t\}\right)\\
&\qquad\times\left(\prod_{j=1}^{nWL} I\left[TMPWL_j(t),\infty,fWL_j\right]\right)\mathrm{d}t\\
&= \sum_{k=1}^{nSL}\int_{TMNSL_k}^{TMXSL_k}\left(\{fSL_k(T_{SL})\}\left\{\prod_{\substack{l=1\\ l\neq k}}^{nSL} I\left[-\infty,\ TMPSL_l[TMPSL_k^{-1}(T_{SL})],\ fSL_l\right]\right\}\right.\\
&\qquad\left.\times\left\{\prod_{j=1}^{nWL} I\left[TMPWL_j[TMPSL_k^{-1}(T_{SL})],\ \infty,\ fWL_j\right]\right\}\right)\mathrm{d}T_{SL}\\
&= \int_{TMNSL}^{TMXSL} G(T_{SL})\,\mathrm{d}T_{SL},
\end{aligned}
$$

where
$I[a,b,f]=\int_a^b f(T)\,\mathrm{d}T$
$fWL_j(T_{WL})$ = density function ($^\circ C^{-1}$) for failure temperature of WL j,
$fSL_k(T_{SL})$ = density function ($^\circ C^{-1}$) for failure temperature of SL k,
$TMPWL_j(t)$ = temperature ($^\circ$C) of WL j at time t for $tMIN \leqslant t \leqslant tMAX$,
$TMPSL_k(t)$ = temperature ($^\circ$C) of SL k at time t for $tMIN \leqslant t \leqslant tMAX$,
$TMNSL_k = TMPSL_k\ (tMIN)$,
$TMXSL_k = TMPSL_k\ (tMAX)$,
$TMNSL = \min\{TMNSL_k,\ k=1,2,\ldots,nSL\}$,
$TMXSL = \max\{TMXSL_k,\ k=1,2,\ldots,nSL\}$,

$$
\begin{aligned}
G_k(T_{SL}) &= fSL_k(T_{SL})\left\{\prod_{\substack{l=1\\ l\neq k}}^{nSL} I\left[-\infty,\ TMPSL_l[TMPSL_k^{-1}(T_{SL})],\ fSL_l\right]\right\}\\
&\quad\times\left\{\prod_{j=1}^{nWL} I\left[TMPWL_j\left[TMPSL_k^{-1}(T_{SL})\right],\ \infty,\ fWL_j\right]\right\}\quad \text{for } TMNSL_k \leqslant T_{SL} \leqslant TMXSL_k\\
&= 0\quad \text{otherwise}
\end{aligned}
$$

$$G(T_{SL}) = \sum_{k=1}^{nSL} G_k(T_{SL})$$

3. One WL, one SL, constant failure delays

The results for PLOAS in Table 1 for one WL and one SL are derived with the assumption that a link fails instantly when it reaches its failure temperature. These results are now rederived with the assumption that there exists a constant delay time between when a link reaches its failure temperature and when it actually fails. Specifically, the delay times are represented by

$$\Delta WL_0 = \text{difference (min) between time when WL fails and time when WL reaches its failure temperature} \tag{3.1}$$

and

$$\Delta SL_0 = \text{difference (min) between time when SL fails and time when SL reaches its failure temperature.} \tag{3.2}$$