ELSEVIER

Reliability Engineering and System Safety 71 (2001) 179–188

RELIABILITY ENGINEERING & SYSTEM SAFETY

www.elsevier.com/locate/ress

Modelling and quantification of dependent repeatable human errors in system analysis and risk assessment

J.K. Vaurio[1,*]

Fortum Power and Heat Oy, P.O. Box 23, 07901 Loviisa, Finland

Received 6 January 2000; accepted 2 September 2000

Abstract

General equations and numerical tables are developed for quantification of the probabilities of sequentially dependent repeatable human errors. Such errors are typically associated with testing, maintenance or calibration (called "pre-accident" or "pre-initiator" tasks) of redundant safety systems. Guidance is presented for incorporating dependent events in large system fault tree analysis using implicit or explicit methods. Exact relationships between these methods as well as numerical tables and simple approximate methods for system analysis are described. Analytical results are presented for a general human error model while the numerical tables are valid for a specific Handbook (THERP) model. Relationships are pointed out with earlier methods and guides proposed for error probability quantification.

Keywords: Fault tree analysis; Human reliability; Dependent failures; Implicit and explicit methods

1. Introduction

When maintenance is performed by one person or a crew for several identical components consecutively, there is a risk that an error made in one task is repeated in subsequent similar tasks. The conditional probability of repeating an error can be considerably larger than the probability of the first error. Typical errors subject to this kind of dependency are valves or switches left in a wrong position, calibration errors, or use of incorrect fuel, lubricant or additives. These can be detrimental to redundant engineered safety systems that are made of multiple identical parallel trains and periodically tested, maintained or calibrated.

The relevance of testing and calibration errors for system safety has been recognised early in probabilistic safety assessments (PSAs). Although such pre-initiator errors have not been dominating the risk in typical probabilistic safety assessments, closed redundant valves in the auxiliary feedwater system were immediate causes for the Three Mile Island 2 — accident in 1979. Less dramatic but significant events appear in many operating experience reports published by IAEA and WANO. Several suggestions have been made in the past for quantification of the error probabilities for PSA [1–5]. However, a review shows that rarely if ever have they been used in a complete and correct form in a large system analysis. No exact and specific guidance seems to be available for incorporating dependent human errors in real system analysis using large fault trees with hundreds of hardware failure events combined with human errors. The present paper develops general useful equations and numerical data for quantification and shows how the dependent human errors may be correctly handled in fault tree analysis. The focus is on system analysis and on development of numerical values for system model probabilities, rather than on human factors, individual error probabilities or empirical data.

The subject of this paper is a task cycle consisting of a sequence of n tasks. The cycle is isolated from other cycles (if any) so that the first task can be considered an independent task. The probability of errors in the following tasks may depend on the outcome (success or error) of the first task. The strength of this coupling depends on how well the tasks are separated in terms of time and location, personnel, etc.

Assumptions:

1. An error made in performing a task results in a functional failure of a component. The probability of error in the first task is $q_0 = P(H_1)$.
2. Homogeneity when $n > 2$: The tasks are identical,

* Fax: +358-10-4554435.
E-mail address: jussi.vaurio@fortum.com (J.K. Vaurio).
[1] Also with Lappeenranta University of Technology, Lappeenranta, Finland.

0951-8320/01/$ - see front matter
PII: S0951-8320(00)00098-3

Nomenclature

C_j	Boolean (binary) variable; failed sate of component j due to hardware failure
$H_i + H_j$	union $H_i \cup H_j$
H_iH_j	intersection (logical product) $H_i \cap H_j$
$h_{ij...}$	$P(H_iH_j...)$
H_i	Boolean (binary) variable; failed state due to a human error made in task i
$\bar{H}_i$	complement (negation) of event H_i
IAEA	International Atomic Energy Agency
i	task index $i = 1, 2, \ldots, n$, tasks ordered in time
m	minimum number of operational trains needed for system success in an m-out-of-n:G system
n	total number of sequential tasks
P(A)	probability of event A = TRUE
P(A|B)	conditional probability of A = TRUE, given B = TRUE
q_0	$P(H_1)$, probability of human error in the first task of a cycle (independent task error probability)
q_j	conditional probability of the human error being repeated for the $(j + 1)$th time given that it has just occurred for j consecutive times in the current work cycle
r.e.a.	rare-event approximation, sum of the minimal cut-set probabilities
WANO	World Association of Nuclear Operators
x	factor; $P(H_2\|\bar{H}_1) = xq_0$
$Y_{ij...}$	$\bar{Z}_{ij...}$
$y_{ij...}$	$P(Y_{ij...}) = 1 - P(Z_{ij...}) = 1 - z_{ij...}$
$Z_{ij...}$	Boolean variable; simultaneously present (common) error specifically in tasks i, j, …; event s-independent of other events
$z_{ij...}$	$P(Z_{ij...})$
Z_s	Boolean variable, failed state of a system

carried out to identical components, equally separated in space and time, all carried out by the same crew with identical tools (or all by different crews or tools) and all environmental and stress conditions are equal a priori. This external a priori homogeneity does not prevent probabilistic dependencies based on actual outcomes (errors or successes) of the tasks.

3. The probability of an error in the next task depends on the number of consecutive errors immediately preceding the task, but not on any earlier events (errors or successes). This means, for example, that $q_1 = P(H_2|H_1) = P(H_3|H_2\bar{H}_1) = P(H_4|H_3\bar{H}_2H_1) = P(H_4|H_3\bar{H}_2\bar{H}_1)$, and $q_2 = P(H_3|H_2H_1) = P(H_4|H_3H_2\bar{H}_1)$.
4. After any success, the probability of an error in the next task is always the same, xq_0, independent of events before that success. This means that $xq_0 = P(H_2|\bar{H}_1) = P(H_3|\bar{H}_2H_1) = P(H_3|\bar{H}_2\bar{H}_1)$, etc. The importance of the numerical value of x will be demonstrated with examples and by comparisons with earlier models.
5. Standard probability theory (incl. rules of conditional probabilities).

Earlier models are reviewed in Section 1.1. Common to all these models is the assumption that events before the latest successful task have no effect on the error probabilities.

In the present paper explicit equations are derived for all joint probabilities needed in the quantification of large system fault trees, in a general case (arbitrary, x, q_0, q_1, q_2, etc.) for $n = 1, 2, 3$ and 4. Such exact probabilities are derived in Section 2 to facilitate an implicit method for large system fault tree quantification.

System unavailability equations due to human errors are presented in Section 3. Related simplified methods for system analysis are reviewed and recommended.

Expressions for the basic event probabilities of an exact explicit method for large system fault tree modelling and quantification are derived in Section 4. Numerical examples and tables for both implicit and explicit methods are given, thereby facilitating effective use of the Handbook [4] data in system analysis. Summary conclusions are presented in Section 5.

1.1. Relationships with earlier models

In their analytical work on m-out-of-n:G redundant standby systems Apostolakis and Bansal [1] used general probabilities q_j as defined in the Nomenclature, without any specific relationships between them. For the error probability of any task following a success they assumed $P(H_{i+1}|\bar{H}_i...) = P(H_1) = q_0$, independent of events before $\bar{H}_i$. This corresponds to a special case ($x = 1$) of the present paper.

It follows from the total probability theorem that $P(H_2) = P(H_1)P(H_2|H_1) + P(\bar{H}_1)P(H_2|\bar{H}_1) = q_0q_1 + (1 - q_0)q_0$, which is different from $P(H_1) = q_0$ whenever $q_1 \neq q_0$. Thus, the individual unconditional event probabilities are