安全系统工程动态简报

第一号

北京市劳动保护研究所

一九八二年

目录：

一、安全系统工程中使用的危险性辨识和评价方法介绍。

安全系统工程领域中，近年来出现了大量的辨识和评价危险性方法，这些方法散见于各种著作中。

为了使应用者节省时间、查找方便，兹将各种出现于有影响的著作中的方法，加以汇编列表，以向读者。

这些方法可以互相补充并不需要互相取代，由于使用一种方法并不能把危险性分析清楚，事实上也是如此。

本文包括并不全面，由于编制这些方法是没有限制的，有些纯属想象而实用价值不大的内容就没有收录进来。例如“临界路径分析”（Critical Path Analysis），“人为路径分析”（Man Path Analysis）及“人为失误率 预测”（THERP）等。

有些在本文列出的方法，并不是由于它非常有效，而是由于它已很通用，例如在设计或评价一个系统的最初阶段中使用的PHA法。

另外要加以说明的是，辨识或评价一个系统时，并不需将所有的分析方法都用上，而是根据客观需要，选择在实际中可行的方法。

1、变换分析 （Change A.） （10）（12）

2、偶然事件分析（Contingency A.） （1）（8）

3、临界事件分析（Critical Incident Technique）（1）（7）

4、临界分析（Criticality A.） （1）

5、能量分析（Energy A。） （1）

6、事件树分析（ETA） （13）

7、故障模式及影响分析 （1）（8）

8、FTA 事故树分析 (1)(4)(8)(11)（12）（14）

9、 流程分析（Flow A。）(1)

10、 交接面分析（Interface A.）(1)

11、 工作安全分析（Job Safety A.）(2)

12、 管理失误风险分析（MoRT） (5)

13、 事故最大可能性分析/最劣情况 （Max Credible Accident/Worse-case Condition） (1)

14、 暴露的人体分析（Naked Man） (6)

15、 工作逻辑纲络分析（Net Work Logic A.）(1)

16、 操作及支援危险性分析（Operating & Support Hazard A。）(11)

17、 危险性预测分析（PHA）(8) (11)

18、 过程分析（Procedure A.）(1) (8)

19、 样板分析（Prototype A.）(1)

20、 方案分析（Scenario） (8)

21、 单点故障分析（Single Point Failure A.）(10)

22、 潜在性巡查分析（Sneak Circuit A.） (11)

23、 子系统危险性分析（Subsystem Hazard A。）(1) (11)

24、 系统危险性分析（System Hazard A.）(11)

25、 系统性检查分析（Systematic Inspection） (2) (7)

有些方法基本相似。有些是根据同一的逻辑原理。有些则借助于实践和其他技术才能更好地应用。因此把这些方法加以分类是十分有用的。

性质互相有关的。子系统危险性分析、单点故障分析、偶然事件分析、系统危险分析、危险性预测分析、交接面分析、临界分析。

基本相同的方法：

1组：过程分析、工作安全分析、操作及支援危险性分析

2组：交接面分析、系统危险分析

3组：流程分析、能量分析

使用逻辑方法的技术：ETA MORT MET 工作逻辑网络分析、FTA 潜在性巡查分析。

假说…将会法（What-if Method）：事故最大可能性分析、方案分析、临界事件分析。

本文中列的方法中，有一些却是没有一定规律的如：变换分析、系统性检查分析、暴露的人体分析、样板分析。

各种分析方法所在书目如下：

（冯肇瑞）

References

1. Hammer, Willie, "Handbook of System and product Safety", Prentice-Hall, Inc., 1972
2. "Supervisors Safety Manual", National Safety Council, 1976 (Fourth Edition)
3. "Systems Safety", Notes for Course No. 529 The George Washington University, May 1979.
4. Briscoe, G. J., "Risk Management Cuide", EG&G Idaho, Inc., SSDC-11, June 1977.
5. Johnson, William G., Mort Safety Assurance Systems", Marcel Dekker, Inc., 1980.
6. Kije, L. T., "Residual Risk", Russe Press, 1963.
7. McElroy, F. (Editor), "Accident Prevention

Manual for Industrial Operations"; National Safety Council; 1974 (Seventh Edition).

8. Hammer, Willie; "Occupational Safety Management and Engineering"; Prentice-Hall; 1981.

9. Hrzina, J.; "Single-Point Failure Analysis in System Safety Engineering"; Professional Safety; Vol. 25, No. 3, p20, March 1980.

10. Kepner, Charles, H. and Tregoe, Benjiamin B.; "The Rational Manager"; McGraw-hill; 1965.

11. Anonymous; "System Safety program Requirements"; MIL-STD-882A; 28 June 1980.

12. Bullock, M. G.; "Change Control and Analysis"; EG&G Idaho, Inc.; SSDC-2; March 1981.

13. Lewis, H. W.; "The Safety of Fission Reactors"; Scientific American; Vol. 242, No. 3, p 53, March 1980.

14. Vesely, W. E., et al; "Fault-Tree Handbook"; NUREG-0492; U. S. Government Printing Office; January 1981.

二、美国安全工程师协会第21届专业开发年会中关于安全系统工程讲座

今年六月，美国安全工程师协会（ASSE）在密苏里州圣露以斯召开了第21届年会，会后举办了一次安系工程讲座，历时三天。兹将其举办目的和内容摘译如下。

讲座名称："事故管理系统工程入门"

目的：为了了解、评价和控制瞬息变化的事故危险性，在安全系统工程领域中，介绍一种简练的方法，以便在实际工作过程应用。课程的设置将满足下列要求：

1. 所设课程不一定要有学位的人才能听得懂。
2. 根据工厂水平并从管理观点进行讲解
3. 能够在广泛的工作范围内应用
4. 提高参加者的专业能力

为什么安全系统工程如此有用呢？其主要原因就是它能够同时发现各种型式的危险性，并且能够采取传统的方法如管理、价值、效果、措施等加以预防。工厂实践可以保证每一个参加者都能在工作中学会应用。（冯肇瑞）

三、美国工程师学会教育科关于安全系统工程短期训练班课程简介。

1. 题目：安全系统工程概论
2. 内容和目的课程共讲8小时，将介绍几个关键技术，它能够帮助参加者提高工作能力，使学员提高对危险性的分析技巧，并能对危险进行辨识、评价和控制。课程包括最基本的安全系统工程概念、应用课题、示例和与现代工作状况有关的简单应用数字。
3. 课程

A、安全系统工程概论

a、安全系统工程概念

b、几个重要项目

c、安全系统工程的要求

B、安系工程的技术复习

a、典型安全课题实践

b、分析用的基本表格

c、基本逻辑图

d、概率的逻辑效果分析

C、安全分析用矩阵表

a、危险性分类和故障频率

b、功能定向分析

e、由矩阵到逻辑图的逻辑发展

D、安全分析用逻辑图

a、初始暴露分析

b、能量控制策略

c、高级逻辑图

d、逻辑门和概率

E、成功分析，

a、MORT概念介绍

b、MORT的应用

F、决策表和价值工程

a、决策型式

b、决策表结构

c、价值工程

冯肇瑞

四、西德标准：

DIN25424第一部分

事故树分析：方法和符号

1981.9

本标准所说的事故树分析要与事故阶段分析区分开来（见DIN25419 第一部分）。事故阶段分析是寻找因某种原因造成的不希望事件，而事故树分析则是先假设某种不希望事件，寻找造成这一事件的所有原因。有关概念的规定与DIN40042（试行标准）尽可能取得了一致。所用符号也尽可能考虑到DIN40700第一部分和美国IEEE标准352-1975（美国电气电子工程学会发表的）。

目　录

附录A　事故树举例

1. 应用范围

这里。在研究系统故障方面。提出了事故树分析方法的建议。以及符号及其应用的建议。

这种方法对各种系统均可应用。在事故树计值时（不是DIN25424的处理对象）也可考虑时间关系。如以维修、检查计划等形式。

2. 目的

事故树分析的目的是找出导致一种不希望事件的各部分故障或分系统故障的逻辑联系。这种研究有助于在运行和安全方面对系统的评价。

分析的具体目的是：

一求系统确定导致假定不希望事件的所有故障可能的组合（原因）

一求出可靠性参数。如故障组合出现的频率。不希望事件发生的频率。或需用时系统的不可用性。

事故树分析给研究提供一种清晰的可以参照执行的方案。

3. 概念

3.1 考察单元

考察单元是做可靠性说明的对象。

考察单元可以是系统。分系统。部分。基本功能。要区分工程技术考察单元和功能考察单元。

3.2 系统

系统是独立执行某一完整任务的技术手段和组织手段的组合。

要区分技术系统和功能系统。根据一个技术系统的功能将其编成一个或几个功能系统。

3·3 分系统

分系统是各部分的组合体。以便解决一个技术系统内有关联的任务。功能分系统是基本功能的组合。以便解决一个功能系统内有关联的任务。

3·4 部分

部分是一个工程技术系统（3·1节讲的做可靠性说明的系统）的最低级的考察单元。每一个部分都附有一种或几种基本功能。

3·5 基本功能

基本功能是功能系统最基本的考察单元。它只描述一种基本功能如接通。旋转。关闭。打开。供能。

3·6 程序

程序是运行时或紧急状况时的操作手续规定。如维护。修理。使用。信息传递等规定。

3·7 系统分析

本标准所指的系统分析是对一个技术系统进行研究。具体讲就是研究分析：

a）系统的功能。特别是工作效率和关于这种工作效率的允许偏差。

b）二次故障（一个部分不允许使用条件的故障）。

c）指挥故障（不顾部分的功能而由于错误的或有缺点的起动或者是用辅助系统的故障而造成的故障）。

3·9 故障类型（失效类型）

一个部分发生故障的各种可能称为故障类型 。

3·10 事故树输入

事故树输入是基本功能故障。

3·11 不希望事件

不希望事件（事故树输出。TOP 顶端事件）是被研究的功能系统的故障。各故障的组合可以引起这种事件。

3·12 故障组合

故障组合是同时存在导致不希望事件的基本功能。发生不希望事件所必要的所有最起码的故障的组合是最小故障组合。

3·13 事故树

事故树是导致一种假定不希望事件的事故树的输入之间的逻辑关系图。

4、方法论

事故树分析法可以把一个观察系统描绘成一种模式。它可以定量定性地评价系统的故障特性。

4·1 模式和符号

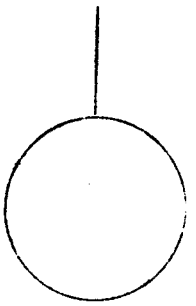
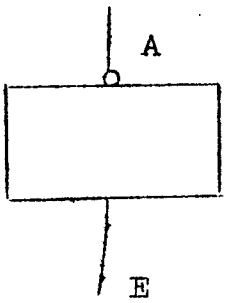
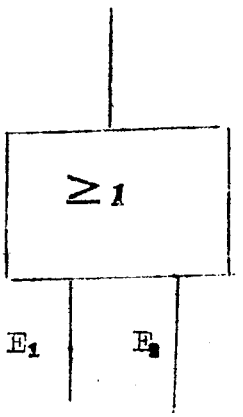
模式，即事故树，是由输入符号和关系符号组成的。关系是事故树内的逻辑联系。它们按照特性规则，由其输入确定输出。这些输入或输出是以二进制表示的。

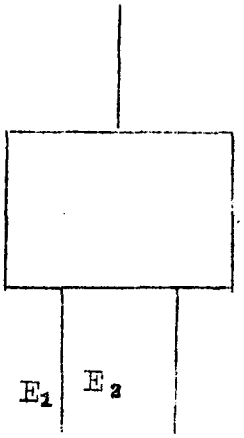
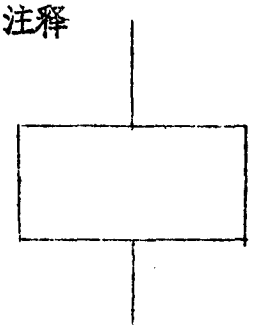
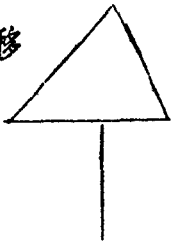
分为“0”，“假的”……有效。

“1”，“真的”……失效。

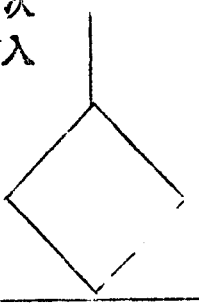
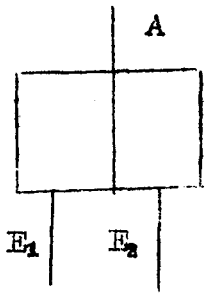
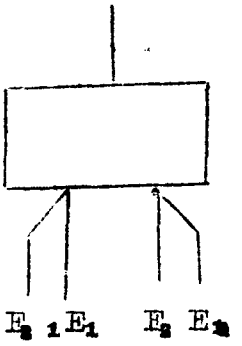
符号表

所有输入和关系都用符号表示。在事故树内都用字母数字标明它们的特性。

编号	名称和符号	说　　明
	标　准　符　号	
1	标准输入 	在可能发生一次故障时。这个符号表示基本功能故障。另外给这个符号标出一次故障的参数和基本功能失效的时间参数。
2	“非”门 	“非”门起否定作用。如果此门的输入E是“0”。则输出A是“1”。或反之。 函数表 E | A 1 | 0 0 | 1
3	“或”门 	“或”门是起逻辑统一的作用。下面的函数表表示此门的两个输入的情况。此门可有任意多个输入。 E1 | E2 | A 1 | 1 | 1 1 | 0 | 1 0 | 1 | 1 0 | 0 | 0

4	“与”门  	“与”门是起逻辑平均的作用。下列函数表适用于此门的两个输入。此门可有任意多个输入。 函数表 E_1 E_2 A 1 1 1 1 0 0 0 1 0 0 0 0
5	注释 	在方块内注明关于输入、输出、门的说明
6	输入转移  输出转移 	用一个转移符号中断事故树或在别的地方继续开始

专 门 符 号

7	二次输入 	用这种符号做为二次门的输入。给这个符号注上一个基本功能或一个功能分系统出现二次故障的参数。及二次故障后故障时间的参数。
8	“二次”门 	“二次”门表示因一次故障产生二次故障。如果E_1由“0”变成“1”。那么就随二次输入E_2的概率和持续时间。门的输出从“0”变成“1”。此门总是有一个一次输入和一个二次输入。
9	“储备”门 	这种门表示储备线路。E_1和E_2是门的输入。而且负责冗余的基本功能或功能分系统。E_1运行。E_2备用。如果E_1由“0”变成“1”。则通过换向机构$E_{2\,2}$接通E_2。在E_1修复后。可以通过换向机构$E_{2\,1}$再回接E_1。另外。可以按一定的控制方法进行换向（这种控制方法不在事故树中说明。而要另行说明）。如果运行单元和备用单元是“1”。或者如果运行单元和附属换向机构是“1”。则输出A是“1”。

4·2 分析步骤

要将一个技术系统转化成尽可能接近实际的模式和计值。下列步骤已证明是恰当的。

a）按4·3节。用系统分析的方法对系统进行详细研究。

b）规定不希望事件和衡量故障的标准。

c）规定重要的可靠性参数和观察时间间隔。

d）考察各部分的故障类型。

e）提出事故树。

f）将输入参数写进事故树。如故障率。故障时间和非可用性。

g）事故树计值。

h）结果评价。

4·3 关于系统分析的提示

关于事故树分析。要对所考察的系统有一个明确的认识。一般通过系统分析得到这种认识。分析的具体步骤在下面各节中做了说明。

4·3·1 系统功能

把技术系统看成一个“黑箱”。它支配着输入和输出。这样就可对系统的功能进行满意的分析。这个黑箱必须完成一种或几种功能。而这些功能以其总体决定着黑箱的输出。

要研究系统的输入和输出。以及系统功能要达到的工作效能和与这些效能的允许偏差。有时还要考虑各运行阶段。

4·3·2 环境条件

系统必定在一定环境条件影响下实现其功能。而技术系统本身不可能影响这些条件。

这些环境条件在系统运行阶段中是要进行研究的。

4·3·3 辅助系统