安全系統工程论文集

（日）佐山隼敏来华讲义

目　　录

一、安全系统工程名词术语……（1）
二、化工装置的危险评价—可操作性研究……（6）
三、化工装置的危险度评价—事故树分析……（16）
四、过程系统F T 编制方法研究之（一）—基本算法及其应用……（29）
五、过程系统F T 编制方法研究之（二）—有两个离散值的变量……（39）
六、过程系统F T 编制方法研究之（三）—反馈和前馈控制回路结合系统……（47）
七、过程系统F T 编制方法研究之（四）—控制回路和保护仪表控制回路（切断回路安全网）的结合系统……（59）
八、过程系统F T 编制方法研究之（五）—编制复杂构造系统……（70）
九、附件
附1.美国P R A 活动……（81）
附2.P R A 方法……（87）
附3.P R A 管理……（90）

一、安全系统工程名词术语

有关安全系统工程的名词术语很多，但这类术语多从系统工程、可靠性工程和人机工程等方面转用过来，还没有从安全系统工程的角度讨论过，以下仅就一些重要的名词术语，加以阐述

系统（System）

目前"系统"这个词很流行，常常听到说"系统"，这个词的意义说清楚是很难的，虽然可以给系统下一个严密的定义，但比较抽象，难以理解　今提出"系统"的主要定义如下：

1）由两个以上的组件所构成，

2）组件之间存在着连系，

3）组件受环境的影响，

4）有一定的目标和任务。

所有系统都应满足上述条件　举例来说，家庭用的小型灭火器就是一个很好的"系统"灭火器的压杆、粉末充填容器、蛇管等都是组件，其目标是消灭初期火灾。因为灭火器是在各个家庭中使用，所以其环境范围随所用的地点决定　考虑系统和环境的情况时，应明确其使用界限范围

街道上配备有多台灭火器时，"系统"就指的是全部灭火器，单个灭火器就成为"一个系统"，环境则指街道环境

再如建筑物内的消火栓又是一个组件，它并不具备系统的全部性能。此处的系统则是由消火栓—配管—加压装置　水源构成的　消火栓虽然比小型灭火器大得多，但其性能仅起组件的作用

可靠性（Reliability）

日本的家用电器如电视机等和汽车大量向国外输出，已经构成国际矛盾。为什么日本产品这样畅销？其原因就是日本产品很少故障，也就是说可靠性高。

有关可靠性工程的名词术语，在本文后半部再作介绍，先把可靠性和安全性的不同点先说清楚，所谓可靠性系表示系统、机器、另件（组件）等的性能在时间上的安定程度。日产电视机和汽车较之其他国家的产品能够正常运转的时间长。

然而可靠性高的产品不一定就是安全性高，如电视机过热会发生火灾，由于汽车故障发生了人身事故，则属于安全问题

安全性　Safety

有关安全性的定义很多，此处所说的安全性系指人没有受伤或死亡，财产未受到损失的状态

拿新干线和飞机为例，如果新干线由于某些故障停止运行，社会上就认为属于可靠性的

问题，但如飞机发生故障，如若陆架收不进去，返回出发地点时便成为安全性的问题了。

因此某些相类似的故障发生后，要看其对系统、目标和性能的影响如何，可靠性和安全性在某些情况下是同义语，某些情况下则不是如此。

再看，以前只是认为机器、另部件等硬件（Hardware）才会出现可靠性问题，而现在对软件(Software)的可靠性逐渐重视起来了。大型计算机几乎不发生故障，但由于输入程序有错误就可能发生重大事故。1980年由于计算机程序错误在神户市造成电话中断，成为重大的社会问题

保安（Security）

当前“警备保障”这个词已经常用了，保安这个词是和它相对应的。所谓保安就是防止危险和灾难，可是在系统的范围内，有计算机的保安问题，其内容是多方面的，包括下述内容：

自然或人为灾害（计算机及其数据的破坏），

犯罪行为(盗用数据，改变程序，改变数据)

保密问题（擅自转用数据库或将其用于别的目的）。

使用银行的计算机，用假输入盗窃现金，盗用现金卡暗号等犯罪案件在国内逐步增加。关于计算机保安问题，很多情况是未知的，所以难以预测发生那些重大事情。

风险（Risk）

买一件珍宝是否选得好是不确定的，既或选坏了，人们考虑所冒风险损失的数额也不会很大。但买一万件珍宝的情况则不同了，是否会选上二等三等货色也不能确定。万一选错则损失金额会很大，这就是所说的冒风险。所谓风险系指包括不确实性和各种损失两个方面的含义，因此可以用下式表示

$$\text{风险} = \text{不确实性} + \text{损失}$$

在美国原子能委员会发表的拉氏姆逊报告中，为了对核电站的风险进行定量比较，风险用下式定义：

$$\text{风险}\left\{\frac{\text{损失水平}}{\text{单位时间}}\right\} = \text{发生频率}\left\{\frac{\text{事　件}}{\text{单位时间}}\right\} \times \text{损失数量}\left\{\frac{\text{损失水平}}{\text{事　件}}\right\}$$

现在日本交通事故的死亡风险约为10^{-4}（死亡/年·人），这个定义存在的问题是，某一种情况下发生的事故，高频率低损失和低频率高损失的风险一样。所以要明确风险的概念还是一个重要的课题，有待进一步确定。

危险性（Hazard）

高尔夫球场的洞穴是典型危险性的例子。冰冻的道路，浩瀚的太平洋都算作危险性，其定义就是危险之源（Source of danger）。此处的危险(Danger)一词，常表示广义的危险。至于危险品则是用大写字母DANGER来表示的。

乘快艇横越太平洋要冒很大的风险，但乘大型客轮则风险非常小。所以说采用了安全装置和防护措施，风险就会变化，可以下式表示：

$$\text{风险} = \frac{\text{危　险　性}}{\text{安全装置和防护措施}}$$

从上式可以看出，如果加强安全装置和防护措施，则风险会变小，但不会变成零。在日本，Risk，Hazard，和Danger都译成危险，容易产生误解。（译者注：我国也有同样情况，应予注意）。

风险评价（Risk Assessment）

进行风险评价的手续和内容如图1所示

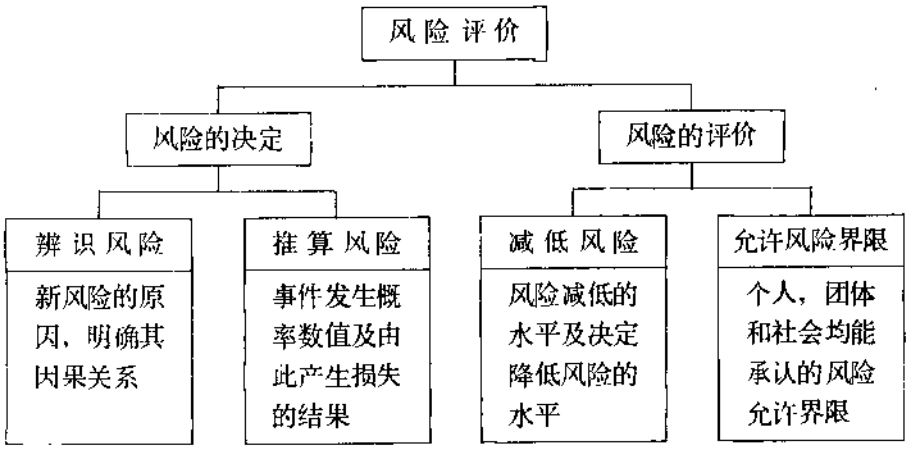


图1　风险评价的结构

首先从风险的辨识开始，其意义就是识别危险性，就象一个新产品问世，要由试验看看它会不会致癌一样。

预测风险需要算出不希望事件（事故）发生概率的数值，确定人和设施的损失大小。为进行此项工作可使用事故树分析法。这种推算叫作风险评价，它是一种狭义的评价。

各种危险性的项目很多，为减少风险，最好是加强安全装置和防护措施，但是它们的有效性、费用等含有很多不确定的因素。

关于风险的允许水平，在日本还是完全没有解决的问题，这是留给今后的重要课题。目前风险评价在原子能发电、天然气基地、化工联合企业 大量危险品输送等问题上都有应用，但在实施上还存在不少问题，今后有必要进一步研究开发。

可靠性工程有关名词术语已在日本标准J1S Z 8115发表了，以下对其中主要术语加以说明

故障（Failure）

所谓故障就是指系统、机器、零部件等丧失了所规定的性能，例如灯炮不亮、电动机不转动都叫故障。

可靠度与不可靠度（Reliability和Unreliability）

可靠度有下述定义：

1）系统、机器和零部件等，

2）在规定的条件下，　　3）在使用期间中，

4）实现规定性能，

5）的概率。

可靠度4）的内容如果变成丧失了规定的性能则叫作不可靠性，也就是所谓不可靠度，它是指在规定的条件下，在使用期间中发生故障的概率。

可靠度和不可靠度之间有下列关系：

$$\text{可靠度} + \text{不可靠度} = 1$$

如果电灯炮发生故障，再修理已不可能，只能用新的替换。另一方面如果电动机发生故障，则能通过修或更换其一部分零件使之恢复正常状态。对可靠度来说，自然是不包含其修理性能的。但广义的可靠度定义则应包括修理，如下所示。

维修（Maintenance）

所谓维修是为了维持系统、机器、零部件的可靠性而进行的修理处理

有效性和非有效性（Availability and Unavailability）

所谓有效性系指可以修理的系统、机器或零件在特定瞬间能够维持性能的概率。表示有效性的定义有很多种，其中最好以所用的时间来表示。

$$A = \frac{\text{运行时间}}{\text{运行时间} + \text{不能运行时间}}$$

有效性通常接近于1，如0.999，但一般使用非有效性的情况居多

$$\bar{A} = 1 - A = \frac{\text{不能运行时间}}{\text{运行时间} + \text{不能运行时间}}$$

$$= 1 - 0.999 = 0.001 = 10^{-3}$$

缺陷（Fault）

如打网球失误一分不算丢分，连续失误两次才算丢分，这就叫作缺陷。它在JIS中没有定义，而在系统工程中则常见到这个词。所谓缺陷，系指对系统、机器、零部件的可靠性能够造成不良的影响。所以说缺陷不是故障而是很有可能发展成为故障的事件。

电动机转动部分声音和振动变大，轴承温度升高等都是缺陷的例子。所以说缺陷是故障的前兆应及早发现。因此为了进行设备维修，所谓异常检测（Fault Detection），异常诊断（Fault Diagnosis）是越来越重要了。

失误（Error）

失误最少有下述三个含义，使用时应予注意：

1）人犯错误、失误、遗漏或疏忽，

2）自动控制或计算机输出误差，

3）计算时舍位误差或其他数学上的误差

其中1）系指实际进行工作时产生的误差，例如开错阀门。所谓遗漏就是该作的事未作，如忘记开关阀门等。

第3）是用计算机求近似值时发生的，以及求园度造成的误差等。

故障保险（Fail Safe）

大规模生产系统或家用电器都采用故障保险方式，其代表性的例子如电气切断器和保险丝等。系统达到危险状态或回路发生短路时，切断器或保险丝打开，因此而保护了电气回路和机器。另外，如洗濯机甩干机转动的时候，打开盖子时转动立即停止，这些都是故障保险方式。

因此，所谓故障保险系指机器故障、操作失误或系统一部分发生故障时，同时能防止故障的扩大并能确保安全的动作方式。最常见的如保险丝将电流切断，叫作故障停止(Fail Passive)方式，又如飞机飞行时发动机发生故障，此时飞机不能停顿，因而就需要开动备用发动机，这就叫作故障激活(Fail Active)方式。

故障保险第一是保护人，第二是保护人周围的环境，第三是防止机器损伤，第四是防止设备性能损失。

确保安全（Fool Proof）

确保安全方式，照字面的意思是指傻瓜也能使用，就是说外行也容易使用的机器。其中有代表性的如傻瓜照象机，只要装进胶卷就可以进行各种摄影，这就是确保安全方式。其他的例子如洗濯机甩干机的盖子，必须盖好后机器才能转动。其它家用电器、汽车等确保安全的设置是很多的。

因此，确保安全方式是在机器发生故障，人员发生误操作时，可以预先防止事故发生的动作方式。

最近各企业发动的综合生产保全运动，为了消灭操作失误，就采用确保安全方式，在这个运动中要找出故障是怎样产生的问题。三浬岛事件应引以为戒。

二、化工装置的危险度评价

——可操作性研究——

可操作性研究（Operability Study）是一种以系统工程为基础的危险度评价方法。它是在化工装置设计、运转时，为了探明装置的危险性，寻求必要措施时甚为实用的方法。本文在说明该方法的原理和分析程序的同时，并举出了各种实际问题的应用事例。并指出该方法存在的问题和特点。

一、绪　　言

化工装置是一个由热交换器、蒸馏塔、反应器等多种设备组成的系统、有既定的设计目标并进行运转的各种装置。但对于发生异常情况时如何处理从工程学角度来看至今还处于未开发阶段。“装置的弱点在哪里?”“现在可能有哪种事故？”“需要采取何种措施？”这种措施适应否？”……对于这些问题不容易确切地作出解答。

就正在运行的装置来说，对其预防事故措施、故障保险回路、紧急停车回路等设备其标准的设计思路、性能和作用的情报是很难收集、存储、传送的。上述问题均属于化工装置危险度评价问题，并迫切期望开发、建立实用危险度评价方法。本文从系统工程学角度介绍化工装置危险度评价方法。

1975年冈山县保安防灾研究会成立，1976年3月发表了“关于保安防灾典型事例的调查研究报告书”，作为第2期的研究课题，选定了“化工装置危险度评价”其调查研究的结果已经于1978年8月发表。现在第3期工作正处于继续进行阶段。本文引用了第2期报告书的一部分。

二、危险度评价方法

已经发表的危险度评价方法如下：

（1）检查表（Check list）方法　　（2）预想灾害评价法

（3）道公司方式、冈山方式等

（4）可操作性研究（Operability Study）

（5）故障类型影响及致命度分析FMECA（Failure Mode, Effects and Criticality Analysis）

（6）事件树分析ETA（Event TreeAnalysis）

（7）事故树分析FTA（Fault Tree Analysis）

关于道公司方式（Dow）。冈山方式，广岛大学河村教授已在《安全工学》第4、5期

(1980年)作过介绍，故本文着重阐述可操作性研究 (Operability Study) 与事故树分析(FTA)两种方法。Operability Study (可操作性研究) 与Operations Research尚无确切的译法。其他方法的研究情况仅列于参考书中。

三、可操作性研究 (Operability Study)

可操作性研究是由英国帝国化学工业公司(ICI)开发的方法，该公司在建设或增建新工厂时自愿使用这种方法，对工厂进行危险度评价。其后，该方法的实用性得到了承认，英国化学工业协会所属的化工安全卫生协会(Chemical Industry Safety aud Health Council of the Chemical Industries Association) 出版了以一般产业为对象的技术手册。

帝国化学工业公司(ICI)最初的可操作性研究主要对象为连续工艺过程，应用实例亦仅限于连续过程。随后亦制定了适用于间歇过程的指南用语。进一步将二者合并、针对一般产业公开发表了通用的指南用语。关于最初阶段的方法已经大概地介绍了，因此这里论述一下对于一般产业可以适用的可操作性研究。

3.1方法的基础

本方法的基础原理，就是着眼于偏离标准和设计及运转条件的“偏差”(deviation)。使用该法的程序是：第一准备好能反映工艺过程的图纸和说明书以便充分理解工艺过程，第二对工艺过程的各个部分进行讨论看能引起何种偏差；最后，判断这种偏差是否会发生危险。为了系统地讨论标准状态的偏差，要使表1的指南用语适用于各个部分。这种用语不仅能适用于化学工厂，而且也适用于其他一般工业。

3.2简单应用实例

为了简单明瞭地说明这种方法，兹举一套简单装置为例。图1所示，用泵将原料A与B送入反应器，经过反应生成制品C。现在假定，若原料B的浓度大于原料A的浓度，即进行爆炸性反应。在图1的流程图中，取以原料A的泵吸入口到反应器的入口这一部分来进行观察。这部分的设计、运转标准就是要按规定的流量输送原料A。

那么，若将表1的指南用语NOT、DON′T或NO用于该标准，则成为“未加原料A”。根据流成图讨论，则未加原料A的原因有四种：

1）原料A贮槽是空的；

2）泵未开动（机械故障、电气故障、泵开关拉开）；

3）管道破裂；

4）阀门关闭，

其后果怎样呢？如果未加原料A，反应器内B的数量立即比A增大，因而将产生爆炸危险性，并将导致灾害。这个问题有必要进一步加以研究。

其次，若将MORE用语用于该标准，则意为“反应器内流入过量的原料A”的偏差。其原因是由于泵的送入量过大。这种原因可能引起下列二种后果。

（1）反应生成物C中含有过剩的A，这在后续过程中仍将继续存在；

（2）若进入反应器内的流量过大，则反应器将会溢出。是否会导致危险尚须进一步讨论。

若将LESS用于该标准，此时的偏差就变为“进入反应器的原料A流入量减少”。这种原因与A完全不流入的情况不同，即（1）阀门部分关闭，（2）管道部分堵塞，（3）泵不按规

定流量运转等。其后果与完全停止流动的情况相同，有引起爆炸的可能性。

上述三个用语应用比较简单，用起来不会发生什么问题。但对其余四个用语则有必要稍加说明。

AS WELL AS 的意思是：虽可按设计、运转标准完成但同时也有发生某种事件的意思。若使用该用语，则变为“在输送原料A的同时”发生的偏差。这包含三个方面：①除了输送原料A还输送其它成分。如图1所示，在泵的吸入口还有来自原料贮槽A以外的配管，其阀门没有关闭时就会发生这种偏差。例如，混入A的稀释材料；②是将原料A输送到反应器以外的地方。从流程图上可以看出，泵吸入口的配管是连通的，可以把原料A输送到别的地方，③在输送原料A的同时发生其它事件。例如，在配管、泵中原料A由液态变为气态，或发生A的分解反应等。

PART OF用语系指只能完成设计和运转标准的一部分。如果使用该用语，则成为“输送原料A的一部分”这一偏差。它包含两个意思：①原料A的某种成分消失了，对消失成分的影响作出评价；

②若由泵对一个以上的反应器供料，则有一个或一个以上的反应器没有获得原料供应。

其余两个用语：REVERSE和OTHER THAN是指因发生完不成设计和运转标准的情况。

表1　指南用语一览表

指南用语	意义	说明
NO或者NOT	完全实现不了设计和运转规定的标准。	完全不能实现设计和运转的标准，也不会发生什么事件(例如：无有流动)
MORE LESS	比标准值数量有所增加或减少	与物理量和特性值有关（例如：由于流量、温度或加温等是否会发生反应）
AS WELL AS	质量提高	虽然可以全部完成设计和运转的标准、但另外还会发生某种事件（例如：存在过量的组分或相的变化）
PART OF	质量降低	仅可以部分不能全部完成设计和运转标准，(例如：组成与标准值有差异)
REVERSE	出现与设计和运转标准相反的事物	主要适用于发生某些事件的场合（发生逆流、逆反应），对于物质亦可适用，使用解毒药，同时出现了中毒；使用光学异构体L同时出现了异构体D
OTHER THAN	出现了完全不同的事物	一点也完成不了设计和和运转标准，发生完全不同的事件

表 2　反应容器系统的可操作性研究（从贮槽出口开始，至反应器入口为止）

指南用语 Guide Word	偏　差 Dtviation	可能原因 Possible Causes	对系统的影响及后果 Conseguence
NO或NOT	未输送原料A	1．贮槽是空的；2．泵发生故障；3.配管断裂 4、阀门关闭。	1、容器内B的浓度较大，引起爆炸
MORE	输送A过多	1、泵的流量过大；2、门开得过大；3、贮槽内压力高。	1、反应器内A过剩，要调查对工艺的影响，2、从反应器向外溢流，要调查是否会引起灾害
LESS	输送A过少	1、阀门部分关闭；2、配管部分堵塞；3、泵的性能降低	1、与NO,NOT情况相同
AS Well AS	输送A的同时	1、从泵吸入口处阀门流入；2、从泵吸入口处阀门输送到别处；3、管、泵内发生相变化	1、可能生成危险混合物，发生火灾、静电、腐蚀等。
PART OF	输送A的一部分	1、A的成份消失；2、向别的反应器进行供料	1、对消失成分的影响进行评价；2、对别的反应器内的影响进行评价。
REVERSE	反向输送原料A	1、反应器满了，压力上升，向管、泵逆流	1、原料A向外部泄漏，调查A的危险性。
OTHER THAN	发生了输送A以外的事件	1、输送与A不同的原料；2、向别的地方输送A；3、管内A凝固	1、调查A有无发生反应；2、予测别的地方可能发生的结果

如果使用REVERSE，则成为“反向输送原料A”的偏差。这意味着：反应器中原料A加满，使压力上升，而产生由反应器向泵的配管系统逆流。

最后，OTHER THAN系指发生了与设计和运转标准完全不同的情况。如果使用这种用语，则成为“发生了输送原料A以外的事件”，这一偏差包含三种意思：（1）输送与A不同的原料。如流程图所示，例如，由泵吸入口的T形管流入别的原料。还要调查有那些物质混入A贮槽的可能性，都要判明它们的影响；（2）变更了原来设计、运转目的。例如，将原料A输送到反应器以外的地方。由流程图可知，通过泵吸入口的T形管可以引起这种现象；（3）发生异常事件。例如输送原料A时发生了A凝固的现象。

将以上讨论的结果汇总列于表2，至于其措施则在下面的应用实例中加以说明。根据英国的经验，分析如图1这样的简单事例约需1.5小时。其细目为：入口管2根、出口管2根、

排气口1个，和容器各部分，各需15分钟。

四、分析步骤

应用这种方法处理实际问题的步骤有以下6个阶段：

1）明确问题的目的及其范围；

2）组织作业小组；

3）进行分析准备；

4）实施分析；

5）重新复核；

6）记录结果。

现将上述各项简述如下，细节请参考手册。

1）明确目的　这种方法可用于设计审查、决定建设场地、决定购置装置、审查操作规程、改善现有装置的安全性等；还要明确发生危险时的对象，如工厂职工、设备装置、居民、环境等。

2）小组的组成　为了实行分析，必须组成两个不同的小组，一个是技术组，一个是"后勤"组。技术组要对装置有广泛而又详细的知识，可以从设计与运转两方面来选人，由机械工程和化学工程的技术人员、研究开发工作的化学家、制造和设计负责人员、以及仪表和电气专业人员组成。人数以3～5人为宜；还要组织实施分析的支援小组。该小组由分析领导人领导，领导人的职责就是：组织技术组、管理教育、收集和整理数据、分析等工作。如设置秘书负责记录、整理已判明存在的危险性，可以提高效率。对于技术组、分析领导人、秘书的教育培养也已经系列化了。

3）分析的准备，准备工作由下列四个阶段组成：

（1）收集数据；

（2）将数据变换成适当的形式；

（3）决定分析程序；

（4）决定分析所需的时间。

在连续式过程中，取得数据并开始进行分析是比较简单的，在间歇式过程中要了解装置的操作程序则十分费事。对于复杂而又属于专利的设备，准备工作比分析需要更多的人数和天数。如果取了数据，领导人就可以确定分析工作所需的时间。图1中，设一处分析为15分钟，全部分析完毕需1个半小时，一次分析时间假设在3小时之内。

4）进行分析　分析原理及其程序在前一节已经用实例作了说明。此处仅提出实际应用的意见，首先，领导人应选定某种配管部分，并要求小组成员明确该部分的目的。在小组各成员未理解其内容之前，不使用指南用语。如果判明存在某种危险，领导人应当弄清全体小组成员是否理解它；假设判明存在危险性，通常有下列两个解决办法：一是寻求每个危险性的各自解决办法，另一个是在判明所有危险性之前，不提解决办法。在实际中需要根据不同的问题来探讨不同的解决方法。

5）重新复核　如果从分析结果发现有应进一步解决的问题时，可将其编制成表，供小组成员传阅。然后，进行所谓"评价与措施"的工作。如果措施方案很多，则选择最有效的措

施。一般有下列四种：

（1）改变流程。　（2）改变流程条件，

（3）修正部分设计，

（4）改变运转方法。

若存在若干措施的情况下，为便于理解，则将其分成下列二类：

（1）消除主要危险因素的措施

（2）减少对系统的影响的措施，评价措施时可用事故树分析。

6）记录　小组的重要活动之一是记录分析结果。其中一个方法是编成"危险性档案"，该档案（file）的内容包括：

（1）供分析使用的所有数据的复制件（流程、操作规程等）；

（2）小组编制的报告书、质疑、建议、再设计等所有资料的复制件。这类档案应按装置分别加以保存，作为将来进行技术改造时的情报源。再者，如果将来充分实施这类分析，那么保险费用亦将由此而受到影响。

五、可操作性研究的实例

水岛地区联合企业中各企业的7套装置曾采用这种方法，并弄清了存在的问题，这些在第2期报告书中进行了总结。作为与下一讲要说明事故树分析相同的例题，本文着重讲述一下加热炉。该过程是将原料气体（H_2 100%）加热到400℃的管式加热炉。用CH_4气作燃料，为使原料气出口温度保持一定，用温度指示控制阀（TIC）进行控制流量，燃烧器有4个，为了简便起见没安装辅助燃烧器，加热炉及其周围的流程为图2所示。

作为安全装置，在燃料气体压力降低时设置了为切断燃料气体的紧急切断装置；其它还设置有燃烧气体警报器（高低位），原料气体出口温度警报器（高低位）。各种计量仪表的动作特性如下：

调节阀—TICV—1供气故障时关闭，XCV—1供气故障时关闭；

电磁阀—平常在励磁情况下断开，异常时在非励磁情况向大气排放（断开系统为平时通电方式）；

压力开关—压力降低时接点断开（正常情况接点关闭）；发信器—全部为正动作形。

该过程的可操作性研究的实施结果如表3所示。表3是以从燃料气体供给部分到燃烧器这一区间为对象的。表2缺少措施一项，而表3最后一项添加有必要的措施。在讨论由于标准状态的偏差是否会发生危险时，尽管未能记入措施一项，但在重视防止发生危险的情况下要检查措施。关于表3的原因B、C、I可以考虑若干措施，象措施1、12、18所表示的那样，由于不确定的因素很多，因而最好用事故树分析来进一步研究。可操作性研究对选定事故树分析的顶上事件是极为有用的。同时表3也是编制事故树的基础资料。表3下部的OTHER THAN处的Maintenance，它是与ICI公司最初的指南用语OTHER相对应。OTHER是指与正常运转[illegible]能引起的一切异常事件，例如，起动、停止、维修等。然而，该OTHER用语应用范围很广，其内容也很笼统，与其它用语不相平衡。也是从这一点出发明确地规定了表1所制定的用语及其意义。对于装置起动、停止、保全的情况还应该以其它形式进行探讨。

表3、加热炉可操作性研究（从燃料气供给部分起，到燃烧器止）

指南用语	偏差	可能的原因	可能产生的影响和后果	必要的措施
NOT NO	NO flow 无流动	1）由于V_1，TICV1 V_2误操作而关闭；2）由于TICV1的指示系统、调节系统、CV故障而关闭；3）由于XCV1的CV故障和联锁误动作等而关闭；④由于V_{4A}～V_{4D}误操作而关闭	A．熄火，原料气体出口气体温度降低。 B．熄火，燃料气若流入炉内，则发生爆炸。	1．设置原料气体警报（TICAL）及燃料气体警报（PIAL）。 2．XCV1不能自动返回 3．检查断流阀门和FCV的联锁装置。 4．就B来说，用FTA分析。 5．研讨检测熄火的方法
MORE	More Press 压力较大	5）燃烧器堵塞⑥提高TICV开度1，TICA温度降低。 2．原料气体流量增加，温度降低等 3．TICV1的指示系统调节系统、CV故障。 4．误操作⑦TICV副线阀门开。 8）由于V_4A～V_4D误操作而开度增大。	C．若超过燃烧器气压上限，则产生熄火，流入未燃气体，爆炸 D．在⑥的3．4和7、8的情况下原料气体温度升。 E．在同上情况下，超过了盘管设计温度，由于火灾异常，盘管破损爆炸 F．由于燃料压力过大，造成燃烧不完全，在炉内二次燃烧。	6．研讨PIAH的断流阀与联锁化。 7．加强温度计的检查 8．温度计用双份或双重检测 9．熟悉燃烧器能力及确立燃烧器检查规则。 10．讨论燃烧器的定期清洗。 11．讨论设置废气分析仪（O_2，CO） 12．就C来说，用FTA分析。 13．设置燃料气警报（高位）（PIAH）及原料气警报（TIAL）（低位）
	More flow 流量较大	（9）燃烧器喷咀破损（6），（7），（8）（同前）	同上	14．掌握炉内燃烧状态。其他同上。

指南用语	偏差	可能的原因	可能产生的影响和后果	必要的措施
LESS	Less Press 压力过低	(10)阀门、法兰、配管外漏 (11) 燃烧器喷咀破损 (12) TICV开度减小，1．TICA温度上升。 2.原料气体流量下降、温度上升等。 3．TICVI的指示系统、调节系统、CV故障	G(10)、(12) 3、4 (13) 的情况下原料气体温度降低 H、(IC) 的情况下在炉外遇明火发生爆炸， I．若超过燃烧器气压下限则造成熄火、流入未燃气体、爆炸。	15．设置可燃气体检测器。 16．讨论设炉内压力计。 17．设置原料气体警报(TIAL)及燃料气体警报 (PIAL) 18．用FTA分析I项
OTHER THAN	Maintenance 维修	4．误操作(13)由于$V_4A \sim V_4D$误操作而关闭(14)燃烧气源压力降低。 (15)燃烧器点火时由于点火失败而使炉内滞留可燃气体。 (16)燃烧器空气量不足，风门误操作。 (17)气流调节器因故障关闭。 (18)燃烧器风门或喷咀误操作。 (19)燃烧器、风门或喷咀故障	再次点火，爆炸、火灾 J．炉内气压上升。 K、由于燃烧室空气不足而燃烧不完全或进而熄灭。 L、喷出炉外、爆炸。 M、原料气体温度降低。	19．炉内设气体检测器。 20．风门的操作标准化。

可操作性能研究的开发工作已有数年，但主要是应用于化工装置，作为危险度评价方法尚未确定。从以前的实施结果所探明存在的问题及其特点综述如下：

1）必要的措施存在下述的一些问题，有必要明确措施的目的和机能：

①对应于原因或结果中的哪一项？

②出现异常的发现和预防以及事后措施中的哪一项？

③异常情况的回避、减轻、分散、组合和转移中的哪一项？

④设计或运转阶段中的哪一项？

⑤是否有必要根据采取的措施再次检查原因和结果？

2）该方法主要适用于配管部分，但对容器的分析程序不明确；

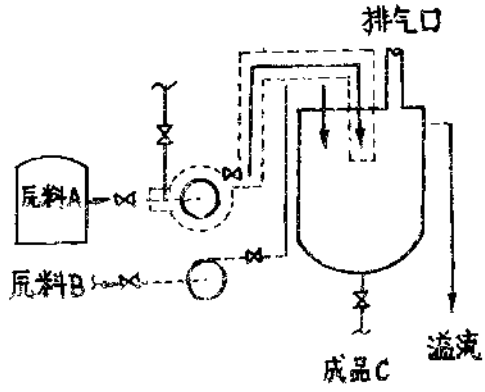
3）在控制系统错误动作及所设置的安全措施不动作的情况下，没有关于对措施有效性的检讨。

该方法的特点如下：

1）因为从中间事件出发，所以兼有事故树分析与FMECA两种方法的特长，它是一种在工作量和经费方面较事故树分析都要少的实用方法；

2）这种方法可适用于设计及运转两方面的问题，对于解决运转人员方面的实际问题和新成员的培养教育均有作用。

3）保存了为编制工厂安全设计和操作规程所需的基础资料，为情报的收集和传送提供了可能



反应：A＋B→C，B的浓度高于A则会发生爆炸。检查部份为虚线圈起部分

图1　反应器供料系统

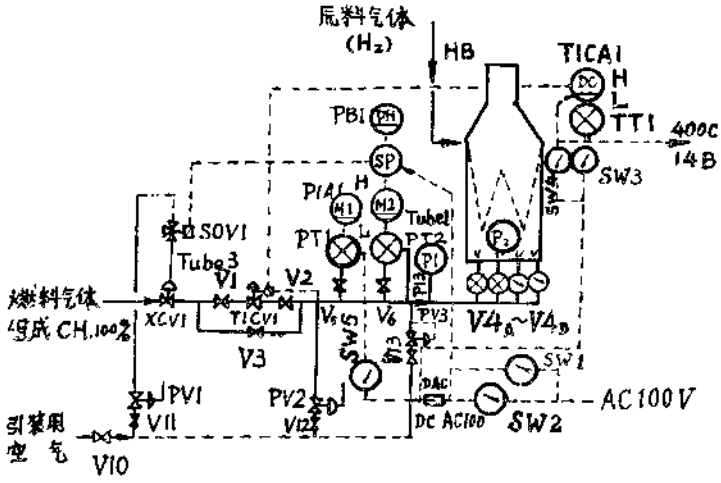


图 2　加热炉及其周围部分的流程图