

Principles of Safety

安全原理

◎ 赵廷弟 焦健 鲍晓红 等编著

◎ 屠庆慈 主审



国防工业出版社
National Defense Industry Press

安全原理

Principles of Safety

赵廷弟 焦 健 鲍晓红 编著
孙有朝 陈 露 魏钱铤
屠庆慈 主审

国防工业出版社

· 北京 ·

内 容 简 介

本书面向高校安全工程专业,突出针对现代复杂社会技术系统,以系统思维和系统工程方法,从安全的本质内涵与属性,专业基础科学和技术科学两个方面,系统性介绍安全原理理论与方法,同时结合时代特征和航空航天特色,介绍软件安全性和航空安全。

本书可使读者较为全面地了解掌握安全原理的基本概念、原理与技术体系。主要供高等院校相关专业高年级本科生及研究生教学使用,也可供相关工程技术人员学习参考。

图书在版编目 (CIP) 数据

安全原理/赵廷弟等编著. —北京:国防工业出版社,2018. 10

ISBN 978-7-118-11744-8

I. ①安… II. ①赵… III. ①安全科学 IV. ①X9

中国版本图书馆 CIP 数据核字 (2018) 第 251210 号

※

国防工业出版社出版
(北京市海淀区紫竹院南路 23 号 邮政编码 100048)
三河市腾飞印务有限公司印刷
新华书店经售



*

开本 710×1000 1/16 印张 25¼ 字数 458 千字
2018 年 11 月第 1 版第 1 次印刷 印数 1—3000 册 定价 65.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777

发行邮购:(010)88540776

发行传真:(010)88540755

发行业务:(010)88540717

前 言

安全性是产品的固有属性。安全科学与工程就是研究装备寿命周期中危险的发生、发展规律,达到预防危险、避免事故,提高装备效能的一门工程学科。

安全问题由来已久,在工业 4.0 的 CPS 时代尤其重要并受社会高度关注。如现代化的武器装备系统、航空运输与卫星发射、高速铁路系统、复杂网络及云系统、通信系统、电力系统等都面临高安全高效能的需求与问题。确保安全和追求高效能是社会技术系统全寿命周期的目标之一。

我国在安全科学与工程领域的研究与应用一直在不断的发展,为国民经济和国家安全发展做出了应有的贡献。进入 20 世纪 90 年代以后,我国颁布了一系列安全性工程技术标准和管理规定,并逐步在飞机、导弹、火箭等大型武器系统的研制中推行,推进了系统安全工程的发展,推动了我国工程型号安全性工作的迅速发展。特别是进入 21 世纪以来,随着复杂社会技术大系统的不断发展和应用,系统科学与工程思维为主线的安全性工程得到了各级领导和工程技术人员普遍重视,并在理论研究和工程应用上积累了丰富的经验。

本书作为安全工程专业的基础课程教材,面向高等院校的安全工程专业本科生及其他专业高年级本科生和研究生等。内容依据安全原理的理论体系,结合航空航天特色,形成基础性、体系性和较为完整的安全原理。本书包括四大部分:第一部分由第 1、2 章组成,讲述安全的概念、属性与范畴,基本概念与安全性度量,是关于安全的最为基本和普适的内容,是学习和掌握安全原理的基础和出发点。第二部分由第 3、4、5 章组成,讲述危险因素与本质、事故致因理论,安全工程原理与技术方法;本部分是安全原理的核心内容,即事故的客观规律和预防事故、保障安全的基本工程事理与技术方法体系。第三部分即第 6 章,讲述安全生产管理原理,是生产阶段如何保障安全的管理手段。第四部分由第 7、8 章组成,面向 21 世纪信息化时代,软件作为系统的重要组成部分,结合航空特色,讲述软件安全性和航空安全。

参与本书编写工作的有:赵廷弟(第 1、2、5、6 章),焦健(第 3、4 章),鲍晓红(第 7 章),孙有朝(第 8 章),陈露、魏钱铎(第 2、6 章)。全书由赵廷弟教授统稿,屠庆慈教授主审。吴居宜、任福纯、王红力、陈磊、江泽泳参与了初期的书稿

提纲研讨;朱一鹏、德新林、褚嘉运、陈志伟、董洁、夏宏青、马宁、姜春阳、李少君、王望、忻昱、郭媛媛参与了校稿、统稿工作等,对他们的工作表示感谢。

编写过程中,参考了大量国内外文献,已在参考文献中列出,在此一并表示感谢。

由于水平有限,错误之处在所难免,望读者指正。

目 录

第 1 章 绪论	1
1.1 什么是安全	1
1.2 安全问题的范畴	6
1.3 什么是安全原理	7
1.4 本书的构成	7
第 2 章 基本概念与度量	9
2.1 基本概念	9
2.2 概念的相关性	12
2.3 安全性评价与度量	14
第 3 章 危险因素及其机理	20
3.1 危险概述	20
3.2 危险基本原理	23
3.3 环境危害	37
3.4 技术危害	43
3.5 人为因素	54
第 4 章 事故致因理论	76
4.1 事故致因理论概述	76
4.2 事故因果连锁理论	83
4.3 能量意外转移理论	95
4.4 动态变化理论	101
4.5 以人为核心的事故致因理论	110
第 5 章 安全工程原理与技术体系	115
5.1 概述	115
5.2 系统与系统工程原理	115
5.3 安全工程原理	120
5.4 安全工程技术方法	141

第 6 章	安全生产管理	212
6.1	安全管理概述	212
6.2	安全管理理论	223
6.3	安全管理文化与法规	231
第 7 章	软件安全性	245
7.1	软件安全性概述	245
7.2	软件安全性相关基本概念与度量	250
7.3	软件系统事故致因理论	260
7.4	软件安全性工程	276
7.5	软件安全性技术	298
第 8 章	航空安全	322
8.1	航空安全概述	322
8.2	民用航空器适航管理	323
8.3	飞行安全	361
8.4	地面安全	374
8.5	航空运营安全管理	382
参考文献		393

第 1 章 绪 论

1.1 什么是安全

论安全、安全原理及安全工程等,首要问题就是:什么是安全?

所谓“无危则安、无损则全”:无危,即没有危险(事故之前);无损,即没有损伤(事故之后)。与“安全”定义相关的词在英文中有 Safety、Safe,以及 Security、Secure。Safety 一般翻译成安全或安全性,Security 翻译成安全、安全性或保密性。Safety 和 Security 在英文中的解释也很相似,甚至相同。本书所谈的安全/安全性,若无特别说明,一般指 Safety。

众多词典中对安全都给出了解释,如:

(1) 安全[safe;secure]:不受威胁,没有危险、危害、损失[新华字典,<http://zidian.00cha.com/show.asp?zhi=10004649>];

(2) 安全:没有危险;不受威胁;不出事故[现代汉语词典,2016年9月第七版,2016年9月北京第561次印刷];

(3) Safety:The condition of being protected from or unlikely to cause danger, risk, or injury [牛津词典, <http://www.oxforddictionaries.com/definition/english/safety>];

(4) Safe:Not likely to cause or lead to harm or injury;not involving danger or risk;Protected from or not exposed to danger or risk;not likely to be harmed or lost [牛津词典, <http://www.oxforddictionaries.com/definition/english/safe>];

(5) Safety:the quality of being safe;freedom from danger or risk of injury;a contrivance or device designed to prevent injury. [柯林斯词典, <http://www.collinsdictionary.com/dictionary/english/safety>];

(6) Safe:affording security or protection from harm;free from danger;unable to do harm;not dangerous[柯林斯词典, <http://www.collinsdictionary.com/dictionary/english/safe>]。

在行业中对安全的定义如下:

(1) 安全(Safety):“免除了不可接受的损害风险的状态”[国家标准(GB/T

28001—2001)];

(2) 安全性(Safety):产品所具有的不导致人员伤亡、系统毁坏、重大财产损失或不危及人员健康和环境的能力[国军标(GJB 451A—2005《可靠性维修性保障性术语》)];

(3) 安全:安全是一种状态,即通过持续的危险识别和风险管理过程,将人员伤亡或财产损失的风险降低并保持在可接受的水平或其以下[国际民航组织];

(4) Safety:The state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management.

(5) Safety:Freedom from risk which is not tolerable[ISO/IEC GUIDE 51:2014 (E), Safety aspects— Guidelines for their inclusion in standards];

(6) Safety: Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. [MIL-STD 882E, 2012, DEPARTMENT OF DEFENSE STANDARD PRACTICE SYSTEM SAFETY; NASA/SP - 2010 - 580 NASA System Safety Handbook]。NASA 扩充 882E 的概念,将不可返回的航天系统的任务失败也归结为安全问题;

(7) Safety:State where an acceptable level of risk is not exceeded [ECSS-S-ST-00-01, ECSS system glossary of terms];

(8) Safety: Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. [FAA System Safety Handbook];

(9) Safety: The state in which risk is lower than the boundary risk. The boundary risk is the upper limit of the acceptable risk. It is specific for a technical process or state; SAFETY: The state in which risk is acceptable. RISK is the combination of the frequency (probability) of an occurrence and its associated level of severity[SAE ARP 4754-2010, Guidelines for Development of Civil Aircraft and Systems];

(10) Safety:The attribute of dependability with regard to the non-occurrence of or recovery from failures and other conditions that could cause unacceptable operational events of an aircraft, engine or component there of[RTCA DO - 297, 2005, Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations]。

如以上的词典与行业定义,安全是一种状态,即无危无损的状态,也就是说安全是指没有威胁或危险、危害或损失。Safety 的定义中有两种定义:其一定义为状态/条件,指产品在某一时刻安全与否的状态,其意为“安全”;其二定义为属性/能力,是各类产品的一种共性的固有属性,是各种系统必须满足的首要设计要求,是通过设计赋予的属性,其意为“安全性”。

安全定义为情况或状态,表征产品的瞬时特性和使用特性,如在某一时刻产品是否处于安全状态,安全作为一种状态或情况是不可度量与比较的,类似于产品在使用过程中的某一时刻是否可靠。安全性作为产品的固有属性,是保障使用安全的能力体现,是可度量与比较的。安全性是保障其使用过程中安全的基础,在很多领域也被称为“本质安全”,本书称之为“固有安全性”。

针对技术系统而言,就是系统正常运行,没有对生命、财产、环境可能产生损害的状态或抗风险能力(英文中常用 Safety),通常是指技术系统的客观状态。对于社会系统而言,就是没有战争、被攻击、抢劫/盗窃等社会危害行为的状态(英文中常用 Security),通常是人的主观行为。

在本书中,如无特殊说明,安全一般指技术系统的安全。

1.1.1 安全问题的由来

安全问题可以说同人类与生俱来,安全无时不在、无处不在,是人类生存与繁衍的本能需求,对于自然界而言,无所谓安全与否,仅是物质的不同形态而已。

在远古时代,人类如同一般动物,受到来自于大自然的危害和人类内部的危害,主要是人身安全的生存需求。随着人类社会的进步,特别是技术进步,在给人类带来极大好处与利益的同时,也带来众多的安全问题,无论是技术系统本身还是利用技术手段的人类自身。

人类追求的范围与层次日益增强,安全问题也日益增多,危险与危害的形式与机理也日益复杂,危害来自于各个领域和层次。同时,人类对安全的意识和要求日益增强,抵御危害的能力也不断进步。

1.1.2 安全问题的本质与特征

安全是针对事故而言,危险是事故的根源,没有危险即安全,但有危险不一定不安全,就像高压电是危险,人不靠近,则不可能有事故,事故是安全与否的分界线。安全问题无论对于人、财产或环境而言,其本质是能量的意外释放。没有事故、即便有危险也无所谓安全,没出事故我们可能无法知道某些危险,危险只有在触发下才会发生事故。因此,危险是安全的本质属性、事故是安全的客观属性。

1. 危险的客观性

危险是可能造成人员伤亡、财产损失或环境破坏事故的根源,即必要条件,是自然界、技术系统和社会系统固有的,虽然不同的人对危险可能有不同的主观感受,但它是不以人的意志为转移的客观存在,在某种触发下导致事故。

绝对没有危险或彻底消除所有的危险是不现实的,因为人类的生存必须依赖于能源,而能量的失控恰恰是事故的根本,危险普遍存在于人类活动的一切领域与时空域,只是不同的场合或时间与空间,危险的固有程度不同。

2. 事故的随机性

安全是一种状态,其对立面就是事故,存在危险,并有触发条件的特定的时间、地点出现,事故才发生。触发事故发生的原因主要是系统/产品的故障、行为的意外失控等,事故的发生是人-机-环等综合因素导致。这些触发因素是随着系统的运行/产品的使用而动态变化的,其状态,特别是其异常状态具有随机性,体现出事故具有偶然性。一方面是事故发生的时间、地点和规模具有随机性,另一方面是事故后果的严重性也是不确定的,对何时、何地发生事故,其后果如何,都不可能确定性地准确预测。

3. 事故的必然性

危险是客观存在的,由于某种触发而导致事故发生是安全的本质,没有危险或消除所有危险是不可能的,人-机-环系统完美无缺也是不可能的,必然潜在着触发危险而导致事故。在系统使用过程中,存在危险与触发的可能,必然导致着事故的发生。

事故的偶然性并非无章可循,偶然之中必有必然性,事故发生于意料之外、但必然发生于其机理之中。通过大量事故资料统计,可以找出事故发生的规律,预测事故发生的概率和可能的严重程度。通过危险/事故机理分析,管理与设计、生产、使用的改进,可以消除某些危险或其触发条件,或降低事故发生的概率,或减少事故的损失。

4. 安全的相对性

危险的客观存在,事故的必然性与随机性,说明绝对的安全是不存在的,安全是相对的,与事故是辩证统一的。随着科技的发展,通过持续的设计、生产、管理与使用的改进,可以不断提高抵御事故风险的固有能力和安全性,同时不断提高使用安全、降低事故风险,但不可能绝对杜绝事故的发生,只能降低事故发生概率和减少事故损失。

5. 安全的系统性

安全问题是系统或产品整体层面的问题。事故是在特定的时间、空间与环境下,危险在受到触发时导致的,是人-机-环多因素综合的结果。特别是随着

技术的不断发展,复杂社会技术系统的安全问题,不仅与系统/产品的系统性、复杂性相关,而且与运行管理模式,甚至法规及文化相关。

6. 安全的事理性

在技术系统中,能量的利用是必然的,事故是能量的意外释放。事故的发生或如何科学、安全地利用能量并避免事故的发生,都与我们利用能量的手段或方法,以及运行管理的模式相关。所有技术系统都是按照人们的功用目的而设计的,表征系统/产品抵御事故风险能力的安全性,是产品的固有属性,是设计出来的,即设计性和可控性。系统/产品是以主观功用为目标,依据客观物理规律,以设计的逻辑为载体,依靠信息而控制运行的,产品研制也是系统工程事理的应用。因此,系统/产品研制与使用的科学性、事理性直接影响其安全性和运行使用的安全。

1.1.3 安全问题的认识与理念

对安全问题的认识与理念是人类的主观心理问题,会因人而异。了解安全的本质与属性,对安全问题应有正确的认识和树立正确的安全理念。

1. 安全第一、预防为主

安全关乎生命,生命对于每一个人都是最为宝贵的,在人们的日常生活与工作中,毋庸置疑:安全第一,可以说是第一准则。从安全的本质与特征出发,对待安全问题要预防为主,防患于未然、将危险或事故消灭在萌芽时期,或尽可能降低事故发生的可能性与严重程度。

2. 要有风险意识、不能有侥幸心理

安全的基本特征告诉我们:没有绝对的安全,安全是相对的,既有必然性、也有随机性,对待安全问题要有风险意识,不能因存在安全风险而固步自封、无所作为,或者无限责任,祈求绝对的安全;同时,不能有侥幸心理,觉得事故是极小概率事件,缺乏防范意识,安全意识淡漠。客观上讲,极小概率事件也是要发生的,要用辩证的思想看待安全问题,尊重客观规律,既不能对安全问题无限扩大责任,更不能安全意识淡漠、侥幸回避。

客观评价安全风险、科学管理安全问题、理性对待安全事故。

3. ALARP 的工程原则

没有绝对的安全,体现在工程中,就是 ALARP 原则,即“合理可行的最低”原则(ALARP:as low as reasonably practicable)。绝对安全的飞机是不飞的、绝对安全的汽车是不开的、绝对安全的高铁是不运行的。人们追求幸福、改造自然,尊重事理,应用物理研制与运行社会技术系统,就必然存在安全隐患与事故。

社会技术系统是以“效能”为目标、“安全”为底线。系统/产品的研制与应

用,根据科学技术的发展水平和工业能力,以及人们的期望,追求科学合理的安全目标,正如航空器的适航要求,遵循 ALARP 的原则,并不断进步,逐步提高安全水平。

1.2 安全问题的范畴

如前所述,安全是人类与生俱来的本能需求。安全的范畴与外延,随着社会的发展不断地演化与扩展,如国家安全、信息安全、食品安全、交通安全等,几乎涉及人类生活的各个方面。

按照所涉及的层次与领域划分安全,安全的范畴可划分为:国家安全、公共安全、生产安全与职业健康、社会技术系统安全。

1. 国家安全

国家安全是指国家政权、主权统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态,以及保障持续安全状态的能力。

国家安全是最高层次的安全,包括:国民安全、领土安全、主权安全、政治安全、军事安全、经济安全、文化安全、科技安全、生态安全、信息安全等。

2. 公共安全

公共安全,是指社会和公民个人日常的生活、工作、学习、娱乐和交往中的生命、健康和公私财产的安全。

公共安全概念涉及到 5 个方面:

- (1) 自然灾害,包括地震、台风、滑坡、泥石流、森林火灾等;
- (2) 事故灾难,环境生态的灾难,安全生产在各个领域的事故;
- (3) 公共卫生事件,包括食品安全,群体不明原因的疾病,以及动物的疾病;
- (4) 个人信息安全,个人相关信息在网络、通信和智能终端等方面的安全保障;
- (5) 社会安全事件,既包括刑事案件、恐怖袭击,也包括了大规模的群体事件和经济安全事件。

3. 社会技术系统安全

社会技术系统安全是层次最低、范围最小和最为具体的安全问题,是以我们研制与使用的技术系统/产品为对象,基于人-机-环的具体系统/产品的安全问题,部分涉及法规、管理体制机制等方面。

社会技术系统安全主要是针对航空、航天、船舶、核能、化工、高铁、汽车和电梯,以及家用电器等系统或产品的事故机理,在全寿命周期解决安全性水平提升

和安全保障的问题。

如无特殊说明,本书主要针对社会技术系统的安全问题。

1.3 什么是安全原理

安全原理是以事故为对象、以危险为核心,阐述安全的本质与属性,事故为何发生和如何发生的基本规律,以及如何预防、控制事故和救援的一般原理与方法论。

安全的本质与属性是安全的基本问题,是开展安全科学和工程研究及应用的根本与基本出发点,否则无从谈起安全问题。

安全原理是安全工程的基础理论,是专业基础科学与技术科学的综合体,如图 1-1 所示。既阐述事故发生的客观规律,如“事故致因理论”,同时论述如何避免事故的科学与方法论,如“系统安全工程”原理,即应用系统科学与工程原理,在系统/产品全寿命周期,开展预防、控制事故及救援的工程过程与技术。

事故致因理论是阐述危险本质与属性、事故的机理,揭示事故发生的客观规律、形成描述事故规律的理论模型。为事故原因的定性、定量分析,为事故的预防,为改进安全管理工作,从理论上提供科学的依据。

安全工程原理是阐述研制、建设及使用社会技术系统的全寿命周期,如何开展危险分析、事故预防、控制与救援的基础工程过程模型和一般技术方法。

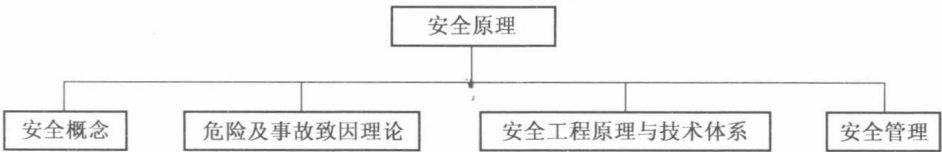


图 1-1 安全原理构成

1.4 本书的构成

本书作为安全工程专业的基础课程教材,依据安全原理的理论体系,并结合航空航天特色,内容包括五大部分:第一部分由第 1、2 章组成,讲述安全的概念、属性与范畴,基本概念与安全度量,是关于安全的最为基本和普适的内容,是学习和掌握安全原理的基础和出发点。第二部分由第 3、4 章组成,讲述危险因素与本质、事故致因理论。第三部分由第 5 章组成,讲述安全工程原理与技术方

法。第二、三部分是安全原理的核心内容,即事故的客观规律和预防事故、保障安全的基本工程事理与技术方法体系。第四部分,即第6章,讲述安全生产管理原理,是生产阶段如何保障安全的管理手段。第五部分由第7、8章组成,是面向21世纪信息化时代,软件作为系统的重要组成部分,结合航空特色,讲述软件安全性和航空安全。

总之,本书试图从安全的本质内涵与属性,专业基础科学和技术科学两个方面,系统性介绍安全原理理论与方法,同时结合时代特征和航空航天特色,介绍软件安全性和航空安全。

第2章 基本概念与度量

2.1 基本概念

根据国军标(GJB 451A、GJB 900A、GJB/Z 99—97等),参考美军标(MIL-STD-882E、GEIA-STD-0010等),结合工程应用情况,在本节给出安全性工程中的基本概念定义。其他概念会在相关的章节中结合其内容给出。

1. 安全

一些经典的定义如下:

(1) 免除不可接受的损害风险的状态。(GB/T 28001—2001《职业健康安全管理体系—规范》)

(2) 不发生可能造成人员伤亡、职业病、设备损坏、财产损失或环境损害的状态。(GJB/Z 99—97《系统安全工程手册》)

(3) 不导致严重的或灾难性的后果的状态。(ISO 14620—1《空间系统—安全性要求—第1部分》)

(4) 没有引起死亡、伤害、职业病或者财产、设备的损坏或损失或环境危害的条件。(MIL-STD882C《系统安全大纲要求》)

综上所述,安全是不发生可能造成人员伤亡、职业病、设备损坏、财产损失或环境损害的状态。该定义是指产品在寿命周期所处的状态,包括试验、生产和使用等,指产品在某一时刻安全与否的状态,表征产品的瞬态安全特性。

2. 安全性

一些经典的定义如下:

(1) 产品所具有的不导致人员伤亡、装备毁坏、财产损失或不危及人员健康和环境的能力。(GJB 900A—2012《装备安全性工作通用要求》)

(2) 产品所具有的不导致人员伤亡、系统毁坏、重大财产损失或不危及人员健康和环境的能力。(GJB 451A《可靠性维修性保障性术语》)

(3) 不导致人员伤亡,危害健康及环境,不给设备或财产造成破坏或损伤的能力。(GJB 1405—92《质量管理术语》)

安全性是各类产品的一种共性的固有属性,与可靠性、维修性和保障性等密

切相关,是各种产品必须满足的首要设计要求,是通过设计赋予的产品属性。

3. 危险

一些经典的定义如下:

(1) 可能导致伤害或疾病、财产损失、工作环境破坏或这些情况组合的根源或状态。(GB/T 28001—2001)

(2) 可能导致事故的状态。(GJB 900A—2012,GJB/Z 99—97)

(3) 可能导致事故的产品现有或潜在的情况。(ISO 14620—1)

(4) 发生事故的必要条件。(MIL-STD-882C)

综上所述,危险是可能导致事故的状态或情况。危险是与安全相对的概念,是指系统中存在导致不期望后果的可能性超过了人们的承受程度,从危险的概念可以看出,危险是人们对事物的具体认识,必须指明具体研究对象,如危险环境、危险条件、危险状态、危险物质、危险场所、危险人员和危险因素等。

4. 危险源

危险源不是一个严格意义上的术语,它被用来进一步说明危险的来源。

危险源是指系统中具有潜在能量和物质释放危险的,可造成人员伤亡、财产损失或环境破坏的,在一定触发因素作用下可转化为事故的部位、区域、场所、空间、岗位、设备和其他位置。危险源的实质是具有潜在危险的源点或部位,是爆发事故的源头,是能量、危险物质集中的核心。

危险源由3个要素构成:潜在危险性、存在条件和触发因素。潜在危险性是指一旦触发事故,可能带来的危害程度或损失大小,或者说危险源可能释放的能量强度或危险物质量的大小;存在条件是指危险源所处的物理、化学状态和约束条件状态;触发因素不属于危险源的固有属性,是危险源转化为事故的外因。

危险源是引发危险的根本原因,它们通常来源于(GJB/Z 99—97):

(1) 物质或产品固有的危险特性(如能量或毒性);

(2) 有害的环境;

(3) 产品(硬件或软件)的故障或失效;

(4) 人员行为失误(包括由心理、生理等因素所引起的行为失误)。

5. 事故

事故是造成人员伤亡、职业病、设备损坏或财产损失的一个或一系列意外事件。事故描述已经发生的事件,也是危险导致的结果。(GJB 900A—2012)

人们对事故下了种种定义,其中伯克霍夫(Berckhoff)的定义较为著名。按伯克霍夫的定义,事故是人在为实现某种意图而进行的活动过程中,突然发生的、违反人的意志的、迫使活动暂时或永久停止的事件。该定义对事故做了全面的描述。