异常环境下要害系统确信安全评估方法

谢朝阳，刘平，何倩云，蒋华兵，李明海

（中国工程物理研究院总体工程研究所，四川 绵阳 621900）

摘要：目的 获得异常环境下的要害系统确信安全评估（PLOAS）建立评估方法和技术框架，为要害系统安全性设计和安全防护决策提供科学支撑。**方法** 基于要害系统在异常环境条件下结构响应行为机制，以表征安全性的响应特征参数为对象，融合试验、数值仿真等技术手段以及代理模型构建等不确定性分析方法，通过定量计算安全特征参数未达到失效阈值的概率，建立通用的确信安全评估方法和技术流程。**结果** 针对单特征参数系统、隔离-失能系统以及多特征参数系统，分别提出了 PLOAS 的定义。并以高压容器作为工程案例，实现了火烧环境下高压容器的确信安全评估。**结论** 建立的确信安全评估方法技术流程兼顾了系统安全物理特性与统计特点，对于高安全性要求的要害系统安全风险评估具有较好的适用性和推广性。

关键词：要害系统；异常环境；不确定性分析；确信安全失效概率

中图分类号：TL76 **文献标识码：**A **文章编号：**1672-9242(2021)05-0006-05

DOI：10.7643/ issn.1672-9242.2021.05.002

Assured Safety Assessment Method of High Consequence System with Abnormal Environment

XIE Chao-yang, LIU Ping, HE Qian-yun, JIANG Hua-bing, LI Ming-hai

(Institute of Systems Engineering, China Academy of Engineering Physics, Mianyang 621000, China)

ABSTRACT: An assessment method of assured safety and technical frameworks for high consequence system with abnormal environment were obtained, which provided scientific support for safety design and protective decision-making of high consequence system. Based on structural responses behavior mechanism of high consequence system under abnormal environmental conditions, the response characteristic parameters representing safety are used as the object, and the technical methods such as testing, numerical simulation as well as the uncertainty analysis methods such as surrogate model construction are combined, and through quantitative computation of the probability of characteristic parameters not-reaching failure threshold, a general assured safety assessment method and technical processes are established. For single characteristic parameter system, strong and weak system and multiple characteristic parameter system, the definitions of PLOAS were proposed respectively. The high-pressure vessel was used as an engineering case, to realize the assured safety assessment of the high-pressure vessel in the fire environment. Through theoretical analysis and case calculations, it is shown that the technical process of the assured security assessment method established takes both physical and statistical characteristics of system security into account, and has good

收稿日期：2021-04-01；**修订日期：**2021-04-16

Received：2021-04-01；**Revised：**2021-04-16

基金项目：中物院创新发展基金项目（2019YCX04002）

Fund：Innovation and Development Foundation of CAEP (2019YCX04002)

作者简介：谢朝阳（1981—），男，博士，副研究员，主要研究方向为系统可靠性与安全性。

Biography：XIE Chao-yang (1981—), Male, Doctor, Associate researcher, Research focus: system reliability and safety.

引文格式：谢朝阳，刘平，何倩云，等. 异常环境下要害系统确信安全评估方法[J]. 装备环境工程, 2021, 18(5): 006-010.

XIE Chao-yang, LIU Ping, HE Qian-yun, et al. Assured safety assessment method of high consequence system with abnormal environment[J]. Equipment environmental engineering, 2021, 18(5): 006-010.

applicability and generalization for the security risk assessment of high consequence systems with high security requirements.

KEY WORDS: high consequence system; abnormal environment; uncertainty analysis; probability of loss of assured safety (PLOAS)

要害系统（High Consequence System）来源于美国 Sandia 国家实验室对战略武器以及重大基础设施的安全性研究实践[1-2]，是指由于意外事故或人为破坏，可能导致重大灾难性后果的系统，如核电站反应堆、战略武器等。要害系统广义安全（Surety）涵盖正常环境的可靠性、异常环境的安全性以及故意或敌对环境下的安保控制[3-4]。其中异常环境（火烧、冲击、雷击等）下的安全性是产品的固有特性，表征系统在可容许的事故后果范围内，能够抵抗外界异常载荷刺激的能力。

安全性是要害系统的重要属性之一，从历史数据看，尽管各国都高度重视反应堆等要害系统的安全性，但是仍不能完全避免发生事故的风险。比如 1986 年的切尔诺贝利核电站发电组爆炸事故，2002 年美国戴维斯-贝斯核电厂反应堆压力容器的顶盖降级事件，2011 年日本福岛核电站放射性物质泄露事故等[5]。因此准确地认识评估系统安全性对于要害系统的工程活动管理与决策具有极其重要的意义。

由于设计制造和服役环境的不确定因素，要害系统的实际运行风险往往高于预期，传统的确定性方法在评估安全性时存在较大偏差。1992 年和 1994 年，国际原子能机构和美国核管理委员会分别发布指导方针，要求全面实施核电站的概率安全评估（PSA）[6]。概率安全评估理论立足于风险视角，关注事故的可能性和严重性，难以定量反映要害系统安全设计特征对异常刺激的抵御能力。在安全性设计方面，美国 Sandia 实验室针对要害系统提出了隔离-失能安全设计措施[7]，其核心在系统中设置专门的隔离部件和失能部件。其中，失能部件是系统正常功能链路的关键环节，其失效阈值低于隔离部件。在异常环境下，失能部件可以在隔离部件失效前可靠地失效，使要害系统丧失爆发灾难性事故的能力。如果隔离部件先于失能部件失效，其失效概率被称为确信安全失效率（Probability of Loss of Assured Safety，PLOAS），定量表征系统安全性的丧失情况。如果要害系统在异常环境下确信安全失效率 $\eta_{\mathrm{PLOAS}}<10^{-6}$，则称为确信安全[8]。

现有相关文献主要针对隔离-失能设计系统 PLOAS 评估开展了方法、模型以及不确定性研究[9-10]，对于更一般的要害系统，缺乏比较通用的确信安全评估方法和技术流程。为此，文中基于系统确信安全的基本概念，结合传统可靠性的统计理论，探讨提出异常环境下要害系统确信安全评估方法，可为反应堆等涉核要害系统安全性评估提供参考。

1　确信安全评估基础理论与方法

1.1　概念与定义

1）确信安全：针对涉核等高危险要害系统中安全性关键部件，在规定的异常环境下丧失安全功能或造成不可接受事故的概率小于 10^{-6}，则称系统确信安全。其主要意义在于能够明确地表征系统对异常环境的容忍能力，对安全功能关键部件的设计以及要害系统使用管理限制决策具有实际工程价值。

2）确信安全评估：基于系统安全功能与外界环境之间的响应机制，计算 PLOAS 的大小，并判断其是否满足确信安全要求。

3）安全特征参数：表征安全性关键部件响应行为特征及程度的参数，通过该参数可以判断系统是否处于安全状态。比如撞击场景下结构的应力、爆炸品内部温升、火烧条件下的功能部件温度等。

4）安全失效阈值：基于安全特征参数，当该参数值超过某一边界值，则表示系统处于事故状态，该边界值定义为失效阈值。

1.2　确信安全评估理论基础

1.2.1　单特征参数系统

对于要害系统中的一般安全性设计部件，比如反应堆中的管道或压力容器，其确信安全的状态就是结构不发生破坏失效。因此，可用结构强度裕量表征系统的安全性，异常环境下要害系统承受的应力可作为反映其安全性状态的特征参数。设 T 为安全功能部件的安全状态特征参数，其失效阈值为 T_0，异常环境刺激下安全特征参数的实际值记为 T_1。当 $T_1>T_0$ 时，认为安全功能失效系统处于事故状态，如图 1 所示。考虑到各种不确定性的存在，PLOAS 的计算表达式为：

$$\eta_{\mathrm{PLOAS}} = P(T_1 - T_0 > 0)\int_{T_0}^{+\infty} f_{\mathrm{T}}(t)\mathrm{d}t \tag{1}$$

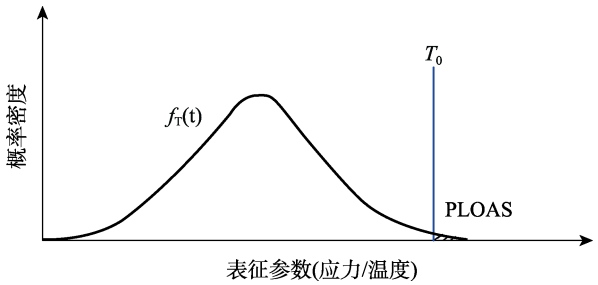

图 1　单特征参数系统确信安全系统

Fig.1 PLOAS of single feature parameter

1.2.2　隔离–失能竞争系统

要害系统中，隔离失能系统的功能关系如图 2 所示。正常情况下，失能开关闭合、隔离开关断开，整个系统处于断路状态，系统安全。异常环境下，如果失能开关未按预期可靠失效（未断开），隔离开关失效闭合，则系统处于不安全状态；如果失能开关按预期可靠失效，隔离开关断开或闭合，系统均处于安全状态。考虑到材料、制造等各种不确定性，用 T_w 和 T_s 分别表示失能和隔离开关失效阈值的随机变量。假设两者相互独立，其概率密度分布函数分别为 $f_w(t)$ 和 $f_s(t)$，两者均服从正态分布，PLOAS 则为图 3 中阴影部分的面积，可通过式(2)表达。

$$\eta_{\mathrm{PLOAS}} = P(T_w > T_s)\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f_w(t_w) f_s(t_s)\mathrm{d}t_w\mathrm{d}t_s \tag{2}$$

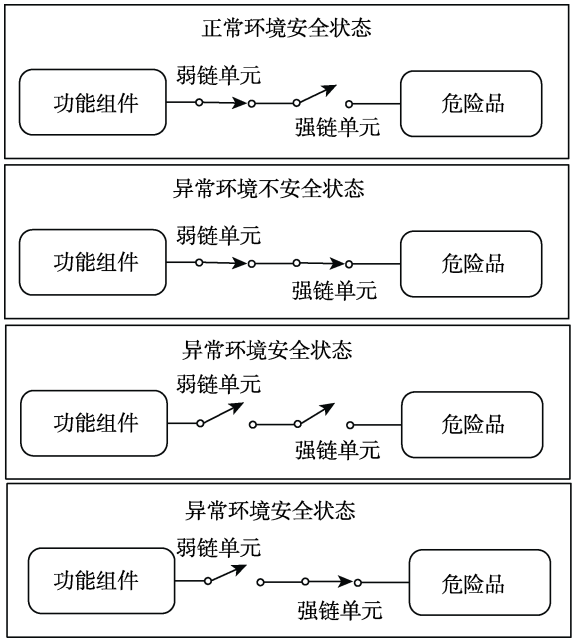

图 2　隔离（强链）/失能（弱链）系统功能示意[11]

Fig.2 Function diagram of isolation-inoperability system[11]

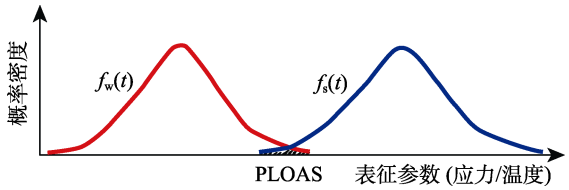

图 3　PLOAS 与失效阈值概率密度分布

Fig.3 PLOAS and distribution of failure threshold

1.2.3　多特征参数系统

对于要害系统中的安全部件，有多个特征参数反映其安全状态时，假设每个特征参数相互独立，如果某一个参数值到达失效阈值时，系统安全状态将发生改变，则系统的 PLOAS 定义为：

$$\eta_{\mathrm{PLOAS}}=\max(P_1,P_2,\cdots,P_n) \tag{3}$$

式中：$P_1,P_2,\cdots,P_n$ 分别表示每个安全特征参数基于相应的失效阈值计算得到的 PLOAS 结果，系统的 PLOAS 则取其中的最大值。

2　评估流程与框架

基于 PLOAS 的相关概念和理论基础，在实际的确信安全评估中，面临安全特征参数分布难以获取的困难。为此，需要开展以安全特征参数为中心的试验测试和数值模拟仿真工作，量化安全特征参数的不确定性。基于上述考虑，文中提出了确信安全评估总体技术框架，如图 4 所示。

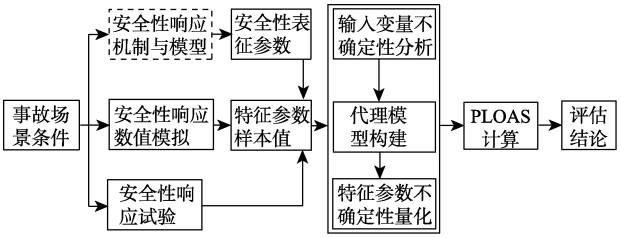

图 4　确信安全评估流程与技术框架

Fig.4 Process and technical framework of assessment of PLOAS

评估过程如下：

1）首先根据评估对象——要害系统特点和事故场景条件，明确异常环境下系统发生不可接受事故后果的主要演化机制。

2）根据事故演化机制，识别并确定表征系统安全性行为的特征参数，形成安全性特征参数集。

3）基于确定的安全性特征参数集，开展系统或分解试验，测试安全性特征参数集中的相关参数。

4）通过试验测试获得的特征参数试验数据，校验数值模拟模型，通过校验后的数值模拟模型，计算获得安全性特征参数集中的不可直接测试量。

5）基于试验和数值模拟获得的数据样本，视情建立安全性响应特征参数集与试验条件以及产品状态因素之间的代理模型[12-13]。常见的包括响应面法[14]、Kriging 法[15]、多项式插值方法等[16-17]。

6）利用试验、数值模拟获得的结果，结合代理模型，进行不确定性传播分析，给出安全性特征参数集中各参数的概率密度分布。

7）基于各参数概率密度分布，根据确信安全失效概率的定义计算系统 PLOAS。

8）根据 PLOAS 定量计算结果，评估要害系统在给出的异常环境条件下是否满足确信安全的结论。

3　工程算例

高压容器常用于贮存有毒有害危险性气体，除了在正常工况下要保证其结构可靠外，在运输过程中如果遭遇运输工具发生火烧等意外事故，容器内的气体

由于高温的作用将使得压力变大，造成结构破裂，有发生有毒有害气体泄漏的风险[18]。为了控制和减小放射性气体因为运输工具产生的异常环境而导致的有毒有害气体泄漏事故，高压容器在运输过程中可采用抗事故包装箱对运输工具产生的火烧和冲击环境刺激进行衰减控制。通常运输事故将产生冲击和高温这两类异常环境刺激。由于运输汽车自身的吸能缓冲以及包装固定等防护措施，冲击环境对高压容器结构破坏影响不大。如果运输工具意外燃烧，据统计，汽车燃油火烧的温度一般为 800~1000 ℃[19-20]，若不采取隔热防护措施，高压容器内气体压力将增大到 3~4 倍，且不锈钢在高温环境下的极限强度将下降，高压容器必然发生破坏，因此需采用抗事故包装箱进行隔热设计。

针对高压容器在运输过程中的火烧事故场景，根据机械结构失效机制，以高压容器结构应力作为安全性特征参数，考虑的不确定性源参数见表 1。根据高压容器的几何结构开展有限元建模仿真，单次有限元计算结果如图 5 所示。考虑到随机不确定性，以有限元计算结果作为训练样本，建立高压容器在异常高温条件下最大应力响应的 Kriging 代理模型。根据代理模型，采用蒙特卡洛抽样可获得最大应力响应的不确定性分布。高压容器应力与强度的概率密度分布如图 6 所示。考虑到高压容器长期腐蚀以及高温导致的强度损减，以强度作为失效阈值。根据图 6 所示的分布情况，可计算得到 PLOAS 为 3.47×10^{-7}，满足确信安全要求。

表 1　高压容器参数及不确定性源分析

Tab.1 The source of uncertainties for pressure vessel

序号	特征参数	不确定性源	类型	表征	参考值	说明
1	材料性能参数(X_1)	U_1	正态分布	均值 均方差	735 MP 15 MPa	极限强度
2	腐蚀损伤参数(X_2)	U_2	均匀分布	—	[5%,18%]	腐蚀导致极限强度的损减比例
3	高压容器厚度(X_3)	U_3	正态分布	均值 均方差	10 mm 1 mm	贮气罐壳体的内外尺寸
4	工作压力(X_4)	U_4	均匀分布	—	[40,50] MPa	加注气体精度
5	材料强度高温性能损减	U_5	正态分布	—	[0%,2%]	高温时高压容器强度损减比例区间
6	隔热防护后高压容器内气体温度	U_6	正态分布	均值 均方差	120 ℃ 6 ℃	高压容器内温度变化

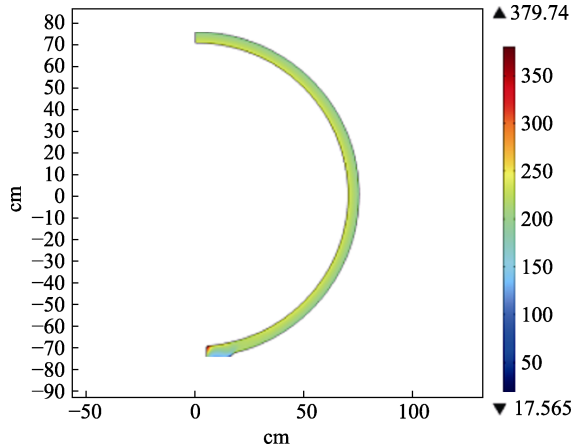

图 5　高压容器最大应力有限元计算

Fig.5 The maximum stress of pressure vessel

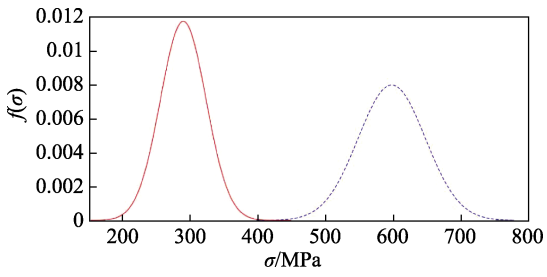

图 6　结构应力与失效强度阈值的概率密度分布

Fig.6 Distribution of structural stress and failure strength threshold

4　结论

1）针对异常环境下要害系统的安全性评估问题，基于系统安全性物理特性和统计理论，提出了确信安全评估方法和技术框架，并给出了具体的实施方案和评估实例，该方法可应用于要害系统确信安全量化评估。

2）针对单安全特征参数、隔离失能竞争系统、多安全特征参数 3 种情况，定义了 PLOAS 的内涵和计算理论基础。

3）文中的评估方法，以安全特征参数为中心，具有一定的通用性，对试验与数值模拟仿真具有较高精度要求。

参考文献：

[1]　郭历伦，罗景润，谢朝阳. 保证性概念及内涵研究[J]，中国安全科学学报，2007，17(11)：21-25.
GUO Li-lun, LUO Jing-run, XIE Chao-yang. Research on the conception and connotation of surety[J]. China safety science journal, 2007, 17(11): 21-25.

[2]　WINTER W L, COVAN J M, DALTON L J. Passive safety in high-consequence systems[J]. Computer, 1998, 31(4): 35-47.

[3] COVAN J M, COOPER J A. Predictable safety in the control of high consequence systems[C]// Proceedings of Third IEEE international, high-assurance systems engineering symposium. [s. l.]: IEEE, 1998.

[4] ROCANA J, SHARON F, RON H, et al. Risk-based assessment of the surety of information system[R]. Washington, DC: Sandia National Labs, 1995.

[5] NNSA. Fiscal year 2014 stockpile stewardship and management plan report to congress[R]. United States: NNSA, 2013

[6] SALLABERRY C J, HELTON J C. CPLOAS_2 user-manual[R]. Albuquerque, NM: Sandia National Laboratories, 2013.

[7] 赵建强, 熊彦铭, 张佑建. 隔离-失能竞争失效机制下安全系统多目标优化设计[J]. 中国安全科学学报, 2020, 30(6): 1-7.
ZHAO Jian-qiang, XIONG Yan-ming, ZHANG You-jian. Multi-objective optimization design for safety system based on isolation-inoperability competing failure mechanism[J]. China safety science journal, 2020, 30(6): 1-7

[8] HELTON J C, PILCH M, CEDRIC J. Probability of loss of assured safety in systems with multiple time-dependent failure modes: Incorporation of delayed link failure in the presence of aleatory uncertainty[R]. Albuquerque: Sandia National Laboratories, 2018.

[9] HELTON J C, PILCH M, CEDRIC J. Probability of loss of assured safety in systems with multiple time-dependent failure modes: Representations with aleatory and epistemic uncertainty[J]. Reliability engineering and system safety, 2014, 124: 171-200.

[10] 王飞, 张方晓. 机械热弱链设计及其安全性评估方法研究[J]. 兵工学报, 2011, 32(5): 632-635.
WANG Fei, ZHANG Fang-xiao. Research on design and safety evaluation method of the mechanical-thermal weak-link[J]. Acta Armamentarii, 2011, 32(5): 632-635.

[11] DENNING R S, BUDNITZ R J. Impact of probabilistic risk assessment and severe accident research in reducing reactor risk[J]. Progress in nuclear energy. 2018; 102: 90-102.

[12] HELTON J C, JOHNSON J D, OBERKAMPF W L. Probability of loss of assured safety in temperature dependent systems with multiple weak and strong links[R]. Albuquerque: Sandia National Laboratories, 2004.

[13] XIE C, LI G, WEI F. An integrated QMU approach to structural reliability assessment based on evidence theory and kriging model with adaptive sampling[J]. Reliability engineering & system safety, 2018, 171: 112-122.

[14] ZHAO L, CHOI K K, LEE I. Metamodeling method using dynamic kriging for design optimization[J]. AIAA Journal, 2011, 49(9): 2034-2046.

[15] RAJASHEKHAR M R, ELLINGWOOD B R. A new look at the response surface approach for reliability analysis[J]. Structural safety, 1993, 12(3): 205-220.

[16] GAVIN H P, YAU S C. High-order limit state functions in the response surface method for structural reliability analysis[J]. Structural safety, 2008, 30(2): 162-179.

[17] HURTADO J E, ALVAREZ D A. Neural network-based reliability analysis: A comparative study[J]. Computer methods in applied mechanics and engineering, 2001, 191(1-2): 113-132.

[18] 郑津洋, 欧可升, 花争立. 车用高压储氢气瓶局部火烧试验方法研究[J]. 太阳能学报, 2014, 35(1): 58-63.
ZHENG Jin-yang, OU Ke-sheng, HUA Zheng-li. Investigation on localized fire test method for on-board high-pressure hydrogen storage tanks[J]. Acta energiae solaris sinica. 2014, 35(1): 58-63.

[19] 史光梅, 李明海, 胡绍全. 油池火灾环境下包装容器的热响应特性模拟[J]. 包装工程, 2011, 32(23): 130-132.
SHI Guang-mei, LI Ming-hai, HU Shao-quan. Simulation of Thermal Response of Package under Fire Condition[J]. Packaging engineering, 2011, 32(23): 132-134.

[20] 史光梅, 李明海, 胡绍全. 横向风对油池火烧试验的影响[J]. 装备环境工程, 2010, 7(6): 86-90.
SHI Guang-mei, LI Ming-hai, HU Shao-quan. Effects of cross wind on kerosene pool fir test[J]. Equipment environmental engineering, 2010, 07(006): 86-90.