在轨可修复单机可靠性分析方法

李 杰[1]，杨 宏[2]，乔军卿[1]，赵国清[1]
（1. 山东航天电子技术研究所，烟台 264003；
2. 中国空间技术研究院 载人航天总体部，北京 100094）

摘 要：在深空探测中，单机具有在轨修复能力有助于提高飞行器系统的可靠性。目前对在轨可修复单机的可靠性问题鲜有研究。建立和分析了在轨可修复单机的可用度模型，推导出可修复单机的瞬态可用度计算公式，通过模拟仿真，计算了不同修复率下的单机可用度变化趋势，与非可修复单机的可用度仿真结果进行了比较。并利用可修复单机的稳态可用度给出了对任务末期修复率和失效率关系的快速估计方法。研究结果表明，在轨修复率越高，在任务周期内可修复单机的可靠性越高；单机具有较高的修复率还可缓解研制阶段对单机可靠性的需求压力。

关键词：可靠性分析；可修复单机；在轨修复；可用度；修复率

中图分类号：TP302.7　　**文献标识码：**A　　**文章编号：**2095-7777（2019）06-0603-06

DOI:10.15982/j.issn.2095-7777.2019.06.012

引用格式：李杰，杨宏，乔军卿，等. 在轨可修复单机可靠性分析方法[J]. 深空探测学报，2019，6（6）：603-608.

Reference format: LI J，YANG H，QIAO J Q，et al. A reliability analysis method for on-orbit repairable single-unit[J]. Journal of Deep Space Exploration，2019，6（6）：603-608.

引 言

以往空间任务中，当电子设备如数管计算机、远置单元、热控管理单元等在轨发生故障时，受技术水平限制，是无法派送人员和装备到现场进行修复的。国内传统单机设备研制阶段，在进行可靠性评估时，一般不考虑修复因素对单机和系统可靠性影响，一般通过软硬件资源的冗余容错设计，来提高设备和系统的可靠性，确保空间任务的完成[1-3]，如采用双机冷备[4]、双机热备[5]、三模冗余容错[6]、多机复合容错[7]等措施。这就不可避免地导致了设备和系统设计复杂度、体积及重量的增加[8]。

对于载人空间任务而言，任务期间有人值守，能够对单机设备进行一定程度的在轨维修和维护[9]。在通用化程度较高的前提下，可以大幅减少备件数量、减轻整器重量，降低航天器研发成本。随着航天电子故障诊断技术及健康预测与管理技术的不断发展，包括深空探测在内的无人飞行器的电子设备与系统的远程维护与在轨自主保障修复也具有了可行性[10]。具有在轨可修复能力可大大提高软硬件资源的利用效率，提高设备与系统可靠性。

地面可修复系统已有一些研究成果，如Rao等[11]结合马可夫过程及系统动态仿真研究了一个含备份的可修复系统，Moghaddass等[12]根据维修人员及工作的串并组合对系统可用度进行了分析，孔德良等[13]将系统分解为若干小模块，先分别计算再综合为系统可用度。而在航天领域，单机在轨可修复是近年来才面对的一个新课题，目前的研究也主要集中在修复方法上[14-15]，对可修复单机的可靠性问题鲜有研究。如不加区别地直接使用非可修复单机可靠性分析方法，就不能准确把握在轨可修复单机的可靠性特点，分析结果也难以对研制工作起到指导作用。因此，有必要开展在轨可修复单机可靠性分析方法研究。

1 单机可靠性模型

1.1 相关概念

1）可靠度（Reliability）与可用度（Availability）

在可靠性分析理论中[16]，可靠性是指产品在规定的条件下和规定时间内，完成规定功能的能力。可靠性的概率度量叫可靠度，它是指在规定时间段内设备无故障运行的概率。可用度是在某种维修条件下、在规定时间内维持系统正常功能的概率。可用度又分为

收稿日期：2019-5-7　修回日期：2019-6-13
基金项目：国家重大科技专项工程

2类：①系统在某一时刻处于正常状态的概率，称为瞬态可用度；②当时间趋于无穷时，系统瞬态可用度的极限，称为稳态可用度。

可用度是可修复单机的一个重要的可靠性指标。对可修复单机，任务末期可用度趋于一个稳定值，可用稳态可用度来衡量。可靠度适合作为非可修复设备的可靠性指标，也可引申为可修复单机在修复率为0时的可用度。本文采用可用度作为可修复单机和非可修复单机可靠性比较的基准。

2）修复过程

修复是指当一个设备或一个系统发生故障时，通过技术手段使之重新恢复到能够行使正常功能状态的过程[17]。

本文假设修复后单机完好如初。修复可采用多种方法，既可以是对故障部件进行软硬件维修，也可以是更换故障部组件。完整的单机修复过程一般包括以下几个步骤：①检测到故障发生，诊断故障原因，隔离故障位置，确定单机修复方案（如：软件在线更新，冷热复位、断电更换硬件等）；②通过软件在线更新、复位、断电更换硬件等，恢复单机正常功能，包括为更新或更换而进行的拆除、取备件、替换等各项工作，以及更新或更换后的软硬件测试及校准；③再次加入系统，行使正常功能。

本文所涉及的单机修复，既可以是维修单机的软件、硬件或部组件，也可以是整机更换。在备件充足的情况下，修复工作可多次重复进行。一般修复过程都含有拆除、测试校准、再接入等步骤。但一些特殊情况，如在线软件更新，就不一定需要单机拆除和接入操作。

3）修复率

修复率μ按单机平均修复时间的倒数计[18]，$\mu=\frac{1}{MTTR}$。平均修复时间越短，修复率越高。此处的修复时间涵盖了从检测到故障发生，到消除故障、系统恢复正常功能的时刻为止，包括了故障检测、诊断与隔离的时间t_1，软硬件获取、维修及测试校准时间t_2，以及再次加入系统的时间t_3，即：$MTTR=t_1+t_2+t_3$。

假设单机通用化程度高，软硬件一致性较好，所采用的故障检测、诊断与隔离算法是一样的，则t_1可视为是不变的。忽略单机位置给替换操作带来的差异，t_3也可视为是不变的。随着故障类型及备件储备情况的不同，t_2则会发生比较大的变化，尤其是受到备件补充能力的影响。在$MTTR$中，t_2所占比例较大，一般情况下远超t_1和t_3。本文主要以t_2来估计$MTTR$及μ。

1.2 可靠性模型

假设单机工作寿命分布与修复时间分布是相互独立的，经过修复的故障单机其工作寿命分布如新的单机一样。单机失效率λ不随时间变化而变化，且单机可靠度R（t）呈指数分布，即R（t）$=\mathrm{e}^{-\lambda t}$。

单机状态S共有2种状态：正常状态和故障状态，即

$$S=\begin{cases}0 & \text{正常状态}\\ 1 & \text{故障状态}\end{cases}$$

非可修复单机可靠性模型如图1所示，表示单机在t时刻，有$\lambda\mathrm{d}t$的概率从正常状态转移到故障状态。当转移到故障状态（$S=1$）后，由于没有修复，只能停留在故障状态（$S=1$），单机失效。

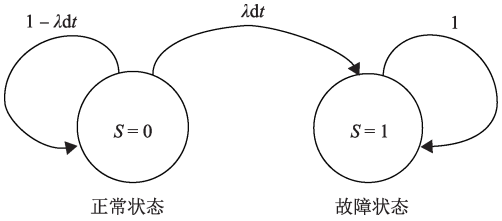

图1 非可修复单机可靠性模型

Fig. 1 Reliability model of none-repairable single-unit

可修复单机可靠性模型如图2所示。由于具有修复能力，故障单机有一定的概率$\mu\mathrm{d}t$从故障状态中恢复到正常状态。

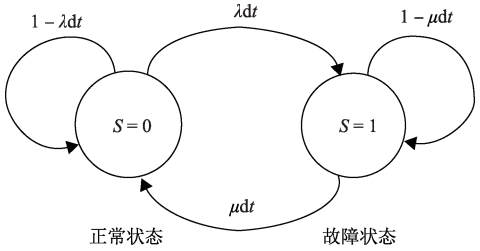

图2 可修复单机可靠性模型

Fig. 2 Reliability model of repairable single-unit

1.3 可修复单机可用度估计公式推导

假设初始加电后，单机处于正常工作状态。对图2的可修复单机可靠性模型建立状态方程为

$$\begin{cases}P_0(t+\mathrm{d}t)=(1-\lambda\mathrm{d}t)P_0(t)+\mu\mathrm{d}tP_1(t)\\ P_1(t+\mathrm{d}t)=(1-\mu\mathrm{d}t)P_1(t)+\lambda\mathrm{d}tP_0(t)\end{cases}\tag{1}$$

其中：P_i（t）为t时刻$S=i$（$i=0,1$）状态下单机正常工作概率。

整理式（1），得

$$\begin{cases}\dfrac{\mathrm{d}P_0(t)}{\mathrm{d}t}=-\lambda P_0(t)+\mu P_1(t)\\ \dfrac{\mathrm{d}P_1(t)}{\mathrm{d}t}=\lambda P_0(t)-\mu P_1(t)\end{cases}\tag{2}$$

对式（2）使用 Laplace 变换，得到

$$\begin{cases}sP_0(s)-P_0(0)=-\lambda P_0(s)+\mu P_1(s)\\ sP_1(s)-P_1(0)=\lambda P_0(s)-\mu P_1(s)\end{cases}\tag{3}$$

根据前文假设，单机初始处于正常状态，故 P_0（0）= 1，P_1（0）= 0。代入式（3），并解方程可得

$$\begin{cases}P_0(s)=\dfrac{\mu}{\lambda+\mu}\times\dfrac{1}{s}+\dfrac{\lambda}{\lambda+\mu}\times\dfrac{1}{s+\lambda+\mu}\\ P_1(s)=\dfrac{\lambda}{\lambda+\mu}\times\dfrac{1}{s}-\dfrac{\lambda}{\lambda+\mu}\times\dfrac{1}{s+\lambda+\mu}\end{cases}\tag{4}$$

对式（4）使用 Laplace 反变换，可得

$$\begin{cases}P_0(t)=\dfrac{\mu}{\lambda+\mu}+\dfrac{\lambda}{\lambda+\mu}\mathrm{e}^{-(\lambda+\mu)t}\\ P_1(t)=\dfrac{\lambda}{\lambda+\mu}-\dfrac{\lambda}{\lambda+\mu}\mathrm{e}^{-(\lambda+\mu)t}\end{cases}\tag{5}$$

其中：P_0（t）为 t 时刻单机处于正常工作状态的概率；P_1（t）为 t 时刻单机处于故障状态的概率。

根据可修复单机可用度的定义，在 t 时刻单机正常工作状态的概率即为单机瞬态可用度为

$$A(t)=P_0(t)=\frac{\mu}{\lambda+\mu}+\frac{\lambda}{\lambda+\mu}\mathrm{e}^{-(\lambda+\mu)t}\tag{6}$$

根据式（6），在确定任务周期、单机的失效率，以及不同备件状态下的修复率后，就可以得到可修复单机在整个任务周期的可用度变化趋势。

对于非可修复单机，可视其修复率 μ= 0，代入式（6），可得：$A(t)=\mathrm{e}^{-\lambda t}=R(t)$，即对非可修复单机，其可靠度与可用度是等效的。

2　可修复单机可用度分析

本文以某信息系统通用计算机作为在轨可修复单机进行可用度仿真分析。

2.1　参数设置

设任务周期为 15 年（共 131 400 h），假定单机失效率 $\lambda=10^{-4}$/h。根据表 1 所列维修类型和备件储备状态估算不同情况下的修复率。

表 1　不同维修类型和备件状态下的修复率估计

Table1　Repair rate estimation for different maintaining and backup states

序号	维修类型	备件状态	MTTR/h	修复率/h	备注
1	在线软件更新	无需拆除和更换备件	0.5	2.0	
2	在线软件更新	无需拆除和更换备件	1.0	1.0	
3	在线软件更新	无需拆除和更换备件	1.5	0.666 7	超过 1.5 h 按第 4 项算
4	更换软硬件	有备件	3.0	0.333 3	
5	更换软硬件	无现成备件	6.0	0.166 7	需从其它单机拆除借用
6	更换软硬件	无现成备件	24	0.041 67	待其它单机用完后借用，1 天
7	更换软硬件	无现成备件	730	0.001 369 9	待其它单机用完后借用，1 个月
8	更换软硬件	无现成备件	4 380	2.283×10^{-4}	待地面补给，间隔半年
9	更换软硬件	无现成备件	8 760	1.142×10^{-4}	待地面补给，间隔 1 年

表 1 中，第 1～3 项在线软件更新是在轨维修项目之一，但这 3 项不涉及故障的检测、诊断与隔离过程，也没有设备的拆除和再接入过程，更新软件是地面经过检验和测试后上传至飞行器，因此其平均修复时间是按照从系统注入单机，并经过在轨测试后正式投入使用这段时间。

2.2　计算与分析

将上述参数（任务周期、单机失效率、修复率）带入式（6），得到可修复单机在 15 年任务周期内，不同维修类型和备件状态下的可用度变化曲线。

因表 1 中第 1～6 项可用度值比较大且分布密集，将第 1～6 项的可用度曲线用图 3 表示，其余的可用度

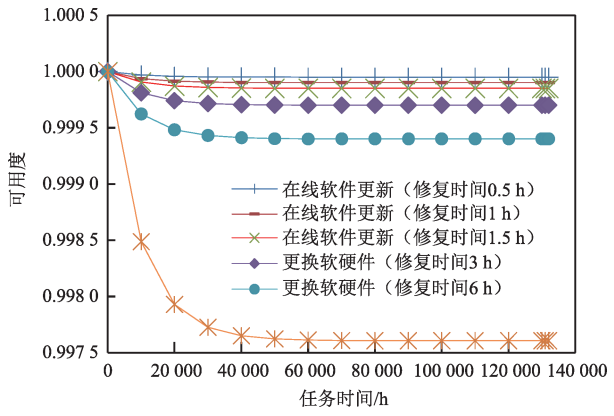

图 3　第 1～6 项的可用度曲线

Fig. 3　Availability curves of No. 1～6 in table 1

用图4表示。表1中的各项在第15年末的可用度值如表2所示。

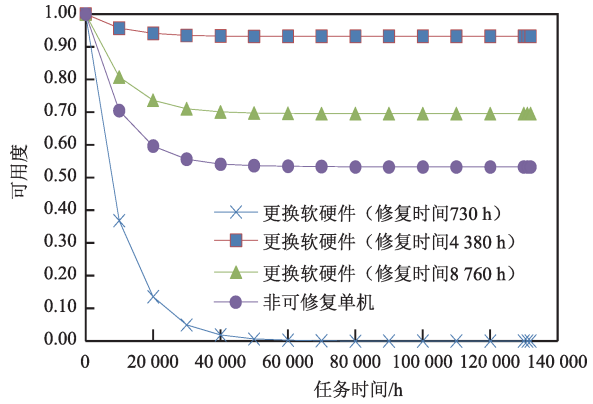

图4 第7～9项及非可修复单机的可用度曲线

Fig. 4 Availability curves of No. 7～no. 9 in table 1, and none-repairable single-unit

表2 表1中各项及非可修复单机在15年末的可用度值

Table2 Table1 availability values at the end of 15-year mission of No.1～no.9 in, and none-repairable single-unit

表1中序号	第15年末的可用度值
1	0.999 95
2	0.999 90
3	0.999 85
4	0.999 70
5	0.999 40
6	0.997 61
7	0.931 97
8	0.695 40
9	0.533 14
非可修复单机	1.85×10^{-6}

仿真计算中使用的单机失效率相对较高，非可修复单机在1 000 h可用度就跌至0.905。表1中的第1～7项因具有较高的修复率，在任务周期中始终保持比较高的可用度，在任务末期单机可用度仍高于0.9。表1中的第8、9项因修复率相对较低，任务末期可用度也相对较低，但远高于非可修复单机。这表明，具有可修复能力，同时具有较高的修复率，可以使失效率相对大的单机也能在任务周期内保持较高的可用度，从而使得飞行器具有较高的可靠性。

3 修复率与失效率关系快速估计

当t趋于无穷时，由（6）式可得到单机稳态可用度[19]为

$$A(\infty)=\lim_{t\to 0}\left(\frac{\mu}{\lambda+\mu}+\frac{\lambda}{\lambda+\mu}\mathrm{e}^{-(\lambda+\mu)t}\right)=\frac{\mu}{\lambda+\mu} \quad (7)$$

由图3和图4可见，随着时间的推移，可用度曲线分别趋近并各自收敛于某一个稳定数值，区别在于不同失效率和修复率下这个数值是不一样的。

当（7）式中修复率μ分别趋于0和∞两个极端值时，得到以下两种极端情况：当$\mu\to0$时，$MTTR\to\infty$，A（∞）$\to0$，即在没有修复力的情况下，稳态可用度最终趋于0。当$\mu\to\infty$时，$MTTR\to0$，A（∞）$\to1$，相当于具有瞬间修复能力，单机在任务周期内几乎全程可用。

按照文献[17]的方法将式（7）作泰勒展开，有

$$A(\infty)=\frac{\mu}{\lambda+\mu}=1-\frac{\lambda}{\mu}+\frac{\lambda^2}{\mu^2}-\cdots\approx1-\frac{\lambda}{\mu} \quad (8)$$

略去高次项后，得到一个近似估计公式（8），可作为设计初期，在期望的稳态可用度下，对单机修复率和失效率的关系进行快速估计。如：当期望任务末期的稳态可用度不低于0.9时，$1-\frac{\lambda}{\mu}\geqslant0.9$，就需要满足$\mu\geqslant10\lambda$的条件。

此处的关系估计只与μ和λ的比例有关，与它们的绝对数值无关。实际应用中，可根据当前单机失效率水平确定合适的维修策略，以更有效地调动资源；或可根据现有的维修能力预计所需的单机失效率，在备件充足、通用程度高、操作便捷、平均修复时间短的场景下，可适当降低对单机失效率的要求，这有利于系统成本控制。

4 结 论

深空探测任务周期长，要求电子设备具有较高的可靠性。通过采用新的技术和新的设计方法等让设备具有可修复能力，是提高其可靠性的一种有效途径。本文研究了在轨可修复单机的可靠性分析方法，推导了单机瞬态可用度计算公式，给出了修复率和失效率关系快速估计方法。研究结果表明，具有可修复能力对提高单机有效工作时间、提升单机可用度起着非常大的作用，修复时间越短，修复率越高，单机可用度提升幅度就越大，可靠性越高。通过对修复率与失效率关系快速估计，可在设计初期阶段为维修策略和可靠性规划提供决策依据。

参 考 文 献

[1] EICKHOFF J. On board computers, on board software and satellite operations: an introduction[M]. Heidelberg, Berlin: Springer-Verlag, 2012.

[2] 杨孟飞，华更新. 航天器控制计算机容错技术[M]. 北京：国防工业出版社，2014.

[3] KIM D, LEE S, JUNG J. Reliability and availability analysis for an on board computer in a satellite system using standby redundancy

and rejuvenation[J]. Journal of Mechanical Science and Technology，2012，26(7)：2059-2063.

[4] 朱明俊，周宇杰. 一种低成本纳卫星星载计算机容错方法[J]. 航天器工程，2016，25(2)：52-57.
ZHU M J，ZHOU Y J. Method of Fault-tolerant on-board computer for low-cost nano-satellte[J]. Spacecraft Engineering，2016，25(2)：52-57.

[5] 李鹏，来新泉. 基于双机热备的航天发动机控制器设计[J]. 火箭推进，2010，36(3)：58-62.
LI P，LAI X Q. Design of dual-processor hot standby aerospace engine controller[J]. Journal of Rocket Propulsion，2010，36(3)：58-62.

[6] 张伟功，辛明瑞，邱庆林，等. 标准化嵌入式三模冗余容错计算机技术研究[C]//第十三届全国容错计算学术会议. 海拉尔：中国计算机学会容错计算专业委员会，2009.
ZHANG W G，XIN M R，QIU Q L，et al. Research on standard embedded TMR computer technology[C]//13th Conference of China Fault-Tolerant Computing. Hailaer：TCFTC，2009.

[7] 黄波，曹帮林，张福鑫，等. 一种三模混合冗余总线控制系统设计研究[J]. 航天控制，2015，33(6)：76-80.
HUANG B，CAO B L，ZHANG F X，et al. Research on triple modular hybrid redundant bus control system[J]. 2015，33(6)：76-80.

[8] 张海军，崔利荣. 空间站的维修性[J]. 质量与可靠性，2013(4)：9-12.
ZHANG H J，CUI L R. Maintainability of space station[J]. Quality and Reliability，2013(4)：9-12.

[9] 王大鹏，谭春林，张柏南. 载人航天器在轨维修性系统设计[J]. 中国空间科学技术，2010，30(5)：16-22.
WANG D P，TAN C L，ZHANG B N. On-orbit maintainability system design for manned spacecraft[J]. Chinese Space Science and Technology，2010，30(5)：16-22.

[10] 罗荣蒸，孙波，张雷，等. 航天器预测与健康管理技术研究[J]. 航天器工程，2013，22(4)：97-102.
LUO R Z，SUN B，ZHANG L，et al. Analysis of PHM technology for spacecraft[J]. Spacecraft Engineering，2013，22(4)：97-102.

[11] RAO M S，NAIKAN V N A. Reliability analysis of repairable systems using system dynamics modeling and simulation[J]. Journal of Industrial Engineering International，2014，10(3)：10-69.

[12] MOGHADDASS R，ZUO M，QU J. Reliability and availability analysis of a repairable k-out-of-n：G system with R repairmen subject to shut-off-rules[J]. IEEE Transactions on Reliability，2011，60(3)：658-666.

[13] 孔德良，王少萍. 可修系统的可用度分析方法研究[J]. 北京航空航天大学学报，2002，28(2)：129-132.
KONG D L，WANG S P. Study on availability for repairable system [J]. Journal of Beijing University of Aeronautics and Astronautics，2002，28(2)：129-132.

[14] 顾毅，张明华，李仁，等. 载人航天电子单机在轨维修技术[J]. 中国空间科学技术，2018，38(6)：73-81.
GU Y，ZHANG M H，LI R，et al. On orbit maintaining technology for electronics single-machine in manned spaceflight[J]. Chinese Space Science and Technology，2018，38(6)：73-81.

[15] 李振松，李光旭，李晓峰，等. 面向航天器嵌入式软件的在轨修复方法[J]. 空间控制技术与应用，2019，45(1)：66-70.
LI Z S，LI G X，LI X F，et al. On orbit repair method of spacecraft embedded software[J]. Aerospace Control and Application，2019，45(1)：66-70.

[16] 曹晋华，程侃. 可靠性数学引论[M]. 北京：高等教育出版社，2006.

[17] SHOOMAN M L. Reliability of computer systems and networks[M]. New York：John Wiley & Sons，INC.，2002.

[18] CASTANO V，SCHAGAEV I. Resilient computer system design [M]. Switzerland：Springer International Publishing，2015.

[19] ZHENG Z，CUI L，HAWKES A G. A Study on a single-unit Markov repairable system with repair time omission[J]. IEEE Transactions on Reliability，2006，55(2)：182-188

作者简介：
李杰(1969–)，男，研究员，博士，主要研究方向：演化硬件、空间计算机系统架构。
通讯地址：山东航天电子技术研究所(264003)
电话：(0535)6928110
E-mail：l.jie.ehw@outlook.com

A Reliability Analysis Method for On-Orbit Repairable Single-Unit

LI Jie [1]，YANG Hong[2]，QIAO Junqing[1]，ZHAO Guoqing[1]

（1. Shandong Institute of Space Electronic Technology，Yantai 264003，China；
2. Beijing Insititute of Spacecraft System Engineering，Beijing 100094，China）

Abstract：During deep space exploration，the ability of being able to be repaired for an on-orbit unit can greatly improve the reliability of spacecraft system. However，researches on single-unit reliability with the influence caused by the on-orbit repair are really scarce. An availability model and its state equations of on-orbit repairable single-units are studied，and its transient availability formula is proposed. The availability with different repair rates of a repairable single-unit is calculated，and compared with a non-repairable one. A method for quick estimating the expected reliability at the end of mission by applying the relationship between repair rate and failure rate is presented. It is shown that the higher on-orbit repair rate，the higher reliability of a single-unit. The high on-orbit repair ability can also reduce the requirement on the reliability of a developing single-unit.

Keywords：reliability analysis；repairable single-unit；on-orbit repair；availability；repair rate

Highlights：

- The reliability estimating method for on-orbit repairable single-units by using the repairable unit's availability is presented.
- The calculation formula of the availability of repairable units is provided, which can be applied for estimating the repairable unit availability in engineering design.
- A method for quick estimating the expected reliability at the end of mission by applying the relationship between repair rate and failure rate is presented, supporting the decision making in the early stage of project.
- The study conclusions can support the balance and control of the system reliability and cost in the on-orbit repairable application scenario.

[责任编辑：高莎，英文审校：朱恬]