

Therac - 25医疗事故的安全性分析

黄国秀, 马平都, 陶慧娥

中图分类号: TL73 文献标识码: B 文章编号: 1004 - 714X(2007)02 - 0210 - 02

【摘要】 Therac - 25事件到今已有 20年的历史, 针对事故的复杂性, 笔者利用系统工程的观点和现代软件工程的基本原理, 对事故的复杂性未重视、系统工程被漠视、软件工程被忽视、用户界面被藐视和软件测试被轻视等五个方面进行了分析, 并对医疗设备的安全性作了分析。

【关键词】 Therac - 25 医院事故; 软件工程; 系统工程; 系统安全

1 问题的提出

Therac - 25是由加拿大原子能公司制造的放射性治疗仪, 设备在 1985年 6月至 1987年 1月使用期间共发生了 6个剂量辐射事件, 结果造成 4位病人死亡、2人重伤的特大医疗事故。Therac - 25事件至今已有 20年的历史, 事故表面现象是由超剂量辐射造成, 但实际上, 深层的原因是系统和软件的安全性设计方面存在严重问题。假如在开发 Therac - 25设备时, 运用现代软件工程技术对系统进行设计, Therac - 25灾难事故也许就不会发生。

2 Therac - 25事故重现

放射线治疗肿瘤技术起源于 20世纪 60年代, Therac - 6和 Therac - 20是 Therac - 25的前身, Therac - 25属于第三代医用高能电子线性加速器, 采用双通概念, 使仪器的空间更加紧凑和易于使用。Therac - 25具有更高的能量, 能够对深部的病变进行治疗, 降低了治疗费用, 缩短了治疗时间。Therac - 25在使用不到二年的时间里, 却出现六次灾难事件, 回放如下^[3]:

(1) 1985年 6月, 一名 61岁的妇女, 到 Marietta 的 Kenne stone 肿瘤中心接受锁骨部位的 10MeV 电子射线照射, 治疗中病人感到炙热和疼痛, 大声喊叫, 医生 Tim Stull无法解释, 怀疑与过量辐射有关, 并与 AECL 电话联系。AECL 工程师答复称设备没有发生超剂量的可能。

(2) 1985年 7月, 一个 40岁女性子宫颈癌患者, 在加拿大安大略 Hamilton 接受 Therac - 25 治疗, 治疗剂量为 2Gy (200rad), 治疗过程中机器停机, 显示出现‘HTILT’错误。同时控制台显示‘No dose’(无剂量)和治疗暂停, 于是操作人员按键盘恢复继续运行, 同样错误再次发生, 在发生 5次之后, 机器进入悬挂状态, 进行了重启的操作。病人当时反应有强烈烧灼感和电击麻刺感。该病人在 5个月后死亡。据以后的分析, 该病人在治疗过程中实际受到 150Gy (15 000rad) 的辐射, 对人体而言, 辐射剂量达到 10Gy (1 000rad) 就已经是致命的了。

(3) 1985年 12月, 一名妇女经过 X射线治疗后, 对准 Therac - 25 光束发射槽的肤色褪色。幸运的是她虽然受伤但幸免于难。

(4) 1986年 3月, 一个男性背部肿瘤患者, 在美国东得克萨斯 ETCC 泰勒医院接受 Therac - 25 治疗, 治疗模式为电子射线, 剂量为 180拉德, 面积为 10cm × 17cm, 操作人员对设备操作十分熟悉, 迅速敲击键盘, 输入相关数据, 发现模式显示为 X

(X射线), 于是更改为 E(电子射线), 启动机器, 机器很快停机, 显示‘Malfunction 54’, 这个信息的含义在说明书中没有明确定义, 其解释是能量已发射, 可能过低或过高。控制台显示为剂量过低, 操作人员于是进行了恢复和重启的操作, 这时治疗舱内的病人已无法忍受, 跳下床敲门, 治疗被迫终止。5个月后该病人死亡, 据分析该病人接受了 160 ~ 250Gy (16 000 ~ 25 000rad) 拉德的辐射。

(5) 1986年 4月在上述事件发生三周之后, 美国东得克萨斯 ETCC 为一个男性面部皮肤癌患者作 Therac - 25 电子射线治疗, 剂量为 1.8Gy (180rad), 仍然由相同的操作人员操作, 事件发生过程几乎与上例完全相同, 病人剧痛大声叫喊。由于脑部受损, 20d后死亡, 据分析该病人接受了 250Gy (25 000rad) 的辐射。

(6) Therac - 25 废除前的最后一次过剂量辐射发生在 1987年 1月。由于另外一种软件错误, 导致病人遭到强电子束照射, 结果病人于 4月份死亡。

3 软件工程基本原理

软件工程主要是针对 20世纪 60年代“软件危机”而提出的, 它是一门研究用工程化方法构建和维护有效的、实用的和高质量的软件的学科。软件工程的目的是提高软件的质量与生产率, 最终实现软件的工业化生产。软件工程的基本原理有七条: ①用分阶段的生命周期计划严格管理。②坚持进行阶段评审。③实行严格的产品控制。④采用现代程序设计技术。⑤结果应能清楚地审查。⑥开发小组的人员应该少而精。⑦承认不断改进软件工程实践的必要性。

4 Therac - 25医疗事故的安全性分析

到了今天事故原因早已查明: Therac - 25故障不仅是由于一般的软件错误造成, 故障的根本原因是系统总体安全设计问题。现运用现代工程技术, 对 Therac - 25事故作如下分析。

4.1 事故的复杂性未重视 任何事故的发生, 很少是单纯的, 通常包含在诸多相互关联事件构成的一个复杂网络中, 涉及诸如技术、人文、组织等因素。这次导致 Therac - 25 多次事故发生的重要原因在于没有非常明确的证据的条件下, 就确信事故的原因已经查明, 例如将 Hamilton 事故中的微型开关作为事故的主要原因, 并且忽略了对其他各种可能的相关因素的分析。另外一个错误的假定是认为, 改正了一个软件错误, 就会预防事故今后发生, 实际上软件故障总是一个接一个地不断暴露。

4.2 系统工程被漠视 现用系统工程的观点, 从复杂系统事故的角度来分析 Therac - 25 事故, 涉及的因素有: ①管理缺位, 缺乏确定的程序跟踪所有报告的事故。②对软件过分信任, 已至删除了所有的硬件互锁装置, 使软件成为可引发事故的单点

失效。③低水平的软件工程实践。④不实际的风险评估和过分信赖评估的结果。

在本案例中和其他工程发生的事故中,一个共同的错误在于对软件过分信任。非软件的专业人士似乎认为软件是不会失效的,从而过分依赖计算机控制功能。其实软件虽然不会发生如同硬件一样的损耗失效,但是软件的设计错误更难于发现和消除。硬件的失效模式一般是有限的,所以构建保护机构比较容易,从 Therac - 25得到的教训是在实施计算机控制时不要删除标准的硬件互锁装置。

硬件备份、互锁和其他的安全保护器件,在许多不同的系统中现在已经被软件置换,其中包括商用飞机、核电站和武器系统。在硬件互锁装置存在的地方,他们也常被软件控制。在设计危险系统时,如果认为一个故障就足以导致严重事故,那就违反了系统工程的基本原理。软件需要作为一个单独的元件来处理,软件不应该单独承担安全的职能。在系统设计中,必须避免单个软件错误或软件工程错误就足以造成灾难性后果。

当前工程界的另外一个趋势是忽略软件, Therac - 25的第一次安全分析,没有包括软件,当问题出现后,分析者又将注意力完全集中在硬件上。调查软件可能的影响不应成为事故分析的最后一个环节,事实上软件错误可以导致硬件的瞬时故障,因为软件给被控制的硬件发布指令。

在 Therac - 25中,病人的反应成为衡量辐射程度的唯一实际指示。Therac - 25完全依赖操作人员,没有独立的机构检查操作是否正确,而机器本身也不能检测大剂量辐射是否发生。Therac - 25的离子室不能掌握高密度的电子束,在它们饱和的时候,显示的是低辐射剂量。

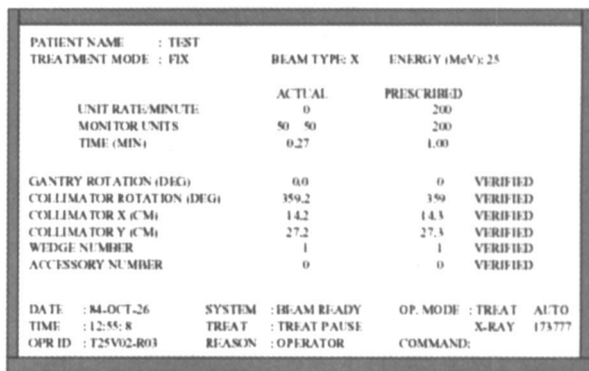
任何一家公司在建造安全关键系统的时,应该进行核查实验,一旦发现问题的任何线索,应该有既定的事故分析程序,医生 Tim Still的第一个电话就应该促使 Kennesbome 和 AECL 进行广泛调查,第一件诉讼就应该立即启动应急响应程序。每一个使用危险设备的企业都应该有危险记录和跟踪,同时使事故的报告和分析成为其质量控制过程的一部分,这不仅有助于事故的预防,而且可以降低保险费率,并在诉讼发生后提供背景资料。

最后,过分依赖安全性分析的数字结果是不明智的,在 Han ilon 事故发生、微开关故障改进后宣称安全性提高了 5 个数量级是无法验证的。

4.3 软件工程被忽视 Therac - 25 中包括了软件编码错误,这个问题在其他与计算机相关的一般事故中是少见的。一般计算机错误主要涉及需求、环境条件和系统状态等。虽然实施软件工程不能完全消除软件中的错误,但是可以极大地减少错误。许多公司在他们的系统中使用软件,但是并不象软件工程师那样严肃对待,下述软件工程的基本原则在 Therac - 25 中受到明显的破坏:①编制软件文档不应是一种事后行为。②应该建立软件质量保证体系和标准。③应保持设计简单性。④如何得到错误信息,例如软件核查试验,应该从软件设计开始时就制订出方案。⑤软件应该在模块级和软件级进行广泛的测试和分析,仅进行系统测试是不正确的。⑥安全性必须构造入软件系统,任何安全关键软件项目必须包括特殊的安全性分析和设计程序,此外不管软件错误是否存在,系统级安全性必须得到确切的保证。Therac - 20 包含有导致泰勒事件的同样软件错误,但是硬件的互锁消除了故障的后果。

4.4 用户界面被藐视 用户界面在 Therac - 25 事件中受到了某种程度的关注,实际上它在这次事件中只有部分影响,虽然软件的界面和这个软件的其他部分一样,存在改进的余地。软件工程师需要接受更多的界面设计培训,从人 - 机工程的角度需要更多的数据输入。不过在当时 Therac - 25 是由小型机软

件控制,因此该机器曾被吹捧为特别“用户友好的”^[3]。但实际上 Therac - 25 控制台屏幕显示图 1 所示,从窗口可发现操作界面并不友好。



PATIENT NAME : TEST		TREATMENT MODE : FIX		BEAM TYPE: X		ENERGY (MeV): 25	
				ACTUAL		PRESCRIBED	
UNIT RATE/MINUTE:				0		200	
MONITOR UNITS:				50 50		200	
TIME (MIN):				0.27		1.00	
GANTRY ROTATION (DEG):				0.0		0 VERIFIED	
COLLIMATOR ROTATION (DEG):				359.2		359 VERIFIED	
COLLIMATOR X (CM):				14.2		14.3 VERIFIED	
COLLIMATOR Y (CM):				27.2		27.3 VERIFIED	
WEDGE NUMBER:				1		1 VERIFIED	
ACCESSORY NUMBER:				0		0 VERIFIED	
DATE : 14-OCT-26		SYSTEM : BEAM READY		OP. MODE : TREAT		AUTO	
TIME : 12:55:8		TREAT : TREAT PAUSE		X-RAY		173777	
OPR ID : T25V02-R03		REASON : OPERATOR		COMMAND:			

图 1 控制台屏幕显示图

必须着重指出在用户友好界面和安全性方面存在着潜在冲突。用户界面设计的一个目的是尽可能方便操作者使用,但是在 Therac - 25 软件中,操作的简单性是以牺牲系统安全性为代价的。最后不仅在初始设计中必须考虑软件和软件界面的安全性,而且需要记录决策理由,使得以后的变更有依据可查。

4.5 软件测试被轻视 事实上,对于软件来讲,不论采用什么技术和什么方法,软件中仍然会有错。测试的目的是发现程序中的错误,是为了证明程序有错。软件测试在产品开发中占据相当重要的一部分,统计表明,在典型的软件开发项目中,软件测试工作量往往占软件开发总工作量的 40% 以上。而在软件开发的总成本中,用在测试上的开销要占 30% ~ 50%。如今微软的软件测试人员是开发人员的 1.5 ~ 2.5 倍。正是由于清晰地认识到了软件测试的重要性,微软的产品质量才有了明显的提高。

ETCC 泰勒医院 1986 年 4 月 Therac - 25 事故发生后,ETCC 立即停止 Therac - 25 工作,并通知 AECL。ETCC 的医生立即对事故进行了仔细的调查。由于机器的女操作员能够确切记忆事故发生时设备实际操作过程,经过一段时间的努力,终于使错误信息“Malfunction 54”信息得以重现。他们发现,在机器的编辑阶段,数据的输入速度是该错误出现的关键因素,也就是说,对于一个熟练的操作人员,在重复同样的操作千百次之后,编辑速度越来越快,最终将使“Malfunction 54”信息出现,即超剂量辐射事故发生。参加实验的医生是在经过了相当长的实践后达到了临界的编辑速度。次日对结果感到迷惑的 AECL 工程师来到现场,直到他在医生和操作人员的训练下使“Malfunction 54”信息再次出现时,才接受了医院的看法,并测量这时的辐射剂量已经达到饱和的 250Gy (25 000rad)。

得到这个消息的美国芝加哥大学联合辐射中心的医生在他们的教学设备 Therac - 20 上进行了实验,两个月后医生们观察到在学生实验中经常出现保险丝烧毁和继电器断路的事件^[3],经分析其实质与 Therac - 25 故障完全相同,但是由于有硬件电路的保护,没有造成任何严重的影响。

现在我们可以设想一下,假如当时测试能更加全面一点、彻底一些, Therac - 25 灾难事故也许可以避免。

5 结论

随着现代科技的发展,计算机在医疗中应用越来越广泛,软件产品的功能复杂性和结构复杂性越来越高,因软件系统失效造成事故将不可避免,如何利用现代工程技术,减少或者避免 Therac - 25 类似医疗事故的发生,是医疗单位及医疗软件开发部门必须要面对课题。

辐射危险评价方法探讨

侯长松, 孙全富, 苏 旭

中图分类号: TL71 文献标识码: B 文章编号: 1004-714X(2007)02-0212-03

【摘要】目的 通过对辐射危险评价的内容和模式的探讨, 为辐射危险评价提供参考依据。方法 对目前评价的基础性问题进行探讨。结果 在辐射危险评价中应选择合适的模式和参数。结论 辐射危险评价是一项系统复杂的过程, 在评价前应做好一系列的准备工作。

【关键词】辐射; 危险评价; 探讨

辐射危险评价是对某一系统(放射照射或污染的厂矿或其他场所的从业人员、居民等)发生辐射伤害的危险性进行定性或定量分析, 评价该系统发生危险的可能性及其严重程度, 最终目的是寻求最低的事故概率、最小的损失和最优的安全效益。辐射危害评价以辐射剂量学、放射生物学、放射毒理学、放射流行病学、放射损伤临床研究等为基础, 收集主要来自人类实际观察获得的辐射效应研究资料, 对不同照射剂量与照射方式的各种辐射照射, 在不同个体与群体中引起的不同类别与程度的健康危害进行分析, 建立辐射剂量效应相关的定量估计模式; 对单位剂量照射引起的危险即危险系数; 对单位剂量照射引起的危险群体已经发生的和将会发生的危险进行评价和预测; 对受照个人发生的健康影响(随机性效应)进行判断; 在对辐射可能引起的各种危险进行单一分析的基础上, 还需对各种后果进行多属性的综合分析, 即危害分析、危险比较分析与危险感知等社会判断, 为建立辐射防护剂量限值提供医学判断的基础。辐射危险评价的主要研究领域包括: 概率性能评价与危险分析, 敏感度与不确定度分析以及综合安全评价。20世纪80年代初期, 1991年国家“八五”科技攻关课题中, 危险评价方法研究列为重点攻关项目, 劳动部劳动保护研究院等单位组织了专题研究“易燃、易爆、有毒重大危害源辨识、评价技术研究”。近30年来, 大多数工业发达国家已经将危险评价作为工厂设计和选址、系统设计以及制定事故应急计划和预防措施的重要依据。我国的阳江高本底研究^[1]和医用X射线工作者恶性肿瘤研究^[2]以及核爆下风向落下灰研究^[3]为我国开展辐射危险研究提供了宝贵的经验, 国内一些专家编著的有关书籍^[4-7]也可作为相应的参考资料。总体来说, 我国辐射危险评价刚起步, 许多问题尚需规范化, 距离工业发达国家还有相当大的距离。随着《中华人民共和国职业病防治法》的颁布实施, 我国的卫生(危险)评价工作进入了一个崭新的发展阶段。

作者单位: 中国疾病预防控制中心辐射防护与核安全医学所, 北京 100088

作者简介: 侯长松(1972~), 男, 辽宁海城人, 助理研究员, 从事医用诊断设备及职业病危害评价工作

1 辐射危险评价的剂量学与生物学基础

电离辐射致癌效应的线性无阈假设是辐射危险评价的重要科学基础^[8], 由此, 才可以在剂量评价的基础上, 依据剂量-响应关系, 进行危险评价。目前认为, 对剂量-响应关系的主要影响是旁路效应、染色体不稳定和适应性响应^[9], 对这些因素的研究日渐深入, 正在逐步提出辐射致癌机制的基于剂量-响应模型。有研究证实, 在低剂量($< 0.2\text{ Gy}$)时, 旁路效应对危险分析起着重要的作用^[10]。

1.1 辐射危险评价的剂量学基础 在辐射危险评价中, 更重要的是按传能线密度(LET)进行化分, 例如低LET外照射(可再进一步分为高剂量率($> 0.1\text{ mGy/min}$)和低剂量率照射)、低LET内照射以及高LET内照射(可进一步分为氦照射和其他内照射)。按剂量分, 可分为大剂量照射和小剂量照射(剂量小于 0.5 或 0.2 Gy)。一般说来, 均匀照射比非均匀照射容易处理, 外照射比内照射容易评价, 急性比慢性照射容易处理。另外, 还可能出现混合照射的情况。为了危险评价, 需要将照射剂量进行归一化计算。对于放射性核素辐射危险评价而言, 不需要对核素进行分组, 因为辐射剂量及其健康危险同每种核素的特定性状高度相关。对涉及大量放射性核素的系统, 危险评价应着重于剂量学的主要贡献者和与健康危险关系最密切的核素。对剂量学数据的评价主要包括以下几个方面: ①对分析方法的评价; ②对探测下限的评价; ③对测量和监测的QA/QC的评价; ④将样本数据与空白对照数据进行比较; ⑤环境样品的比较; ⑥建立危险评价用的剂量学数据库。

1.2 辐射危险评价的生物学基础 电离辐射慢性照射可能产生的严重的非致癌效应危险包括遗传和致畸效应。在人类中尚未观察到辐射诱发的遗传效应, 从动物资料外推得到的单位照射的危险低于或相当于辐射致癌危险。另外, 遗传效应通过数代扩散开来, 就致畸效应而言, 单位照射的危险大于致癌危险。但是, 致畸效应可能存在阈值, 并且只有发生在孕期特定时期(如在怀孕的第9个月)的照射才能产生致畸效应。遗传效应可以在30a的生育期间内发生, 致癌效应则可发生在一生的任何时期。如果对辐射源没有适当控制, 致癌的累积危险要

参考文献:

- [1] Evelyn Stiller Cathie LeBlanc著, 基于项目的软件工程面向对象研究方法[M], 贵可荣等译. 北京: 机械工业出版社, 2002. 6
- [2] Evelyn Stiller Cathie LeBlanc Project-Based Software Engineering An Object-Oriented Approach[Z]. Pearson Addison Wesley, 2004

- [3] Peterson I Fatal Defect Chasing Killer Computer Bugs[M]. New York: Random House, 1995
- [4] Grady Booch Object Solutions Managing the Object-Oriented Project[P]. Addison-Wesley Pub Co, 2002
- [5] Scott W Ambler 面向对象软件开发教程[M]. 车皓阳, 刘悦译. 第2版. 北京: 机械工业出版社, 2003

(收稿日期: 2006-11-28)