FMEA在危险分析中的使用和误用

孟杰雄[1] 刘沫[2]
1 首都医科大学 （北京 100069）
2 福禄克测量技术研究所 （北京 100089）

The Use and Misuse of FMEA in Risk Analysis

MENG Jie-xong[1] LIU Muo[2]
1 Capital University of Medical Scienses (Beijing 100069)
2 Fuluke Metrid Technology Institute (Beijing 100089)

文章编号：1006-6586(2006)07-0052-04 中图分类号：F203 文献标识码：E

失效模式和效应分析（FMEA）是对医疗器械产品进行风险管理的一个有力工具，但是这种方法自身存在一定的局限性或缺点，在使用当中应尽量注意并加以避免。

ISO（国际标准化组织）于2000年颁布了关于医疗器械风险管理方面的标准：ISO 14971:2000，该标准为识别、评价和降低医疗器械的风险提出了明确的方法。该标准是医疗器械风险管理领域唯一一份国际化标准。与之前其他的风险管理标准（例如EN 1441）不同，ISO 14971:2000不仅明确规定了对医疗器械进行危害识别、风险分析和控制方法，还针对这些过程增加了很多重要的细节性说明，并将风险管理扩展到医疗器械产品的整个寿命周期。也就是说，ISO 14971:2000提出了一整套将医疗器械风险降低到最低的可接受水平的方法。

在美国，FDA已经认可了ISO 14971:2000；在欧洲，该标准于2004年4月代替了EN 1441《医疗器械：风险分析》（同年，撤销了EN 1441）；我国也于2003年6月20日发布了其等同采用标准YY/T 0316/ISO 14971：2000《医疗器械 风险管理对医疗器械的应用》，并于2004年1月1日开始实施（同时代替了YY 0316-2000）。因此，符合ISO 14971:2000不但对于保证医疗器械产品的安全至关重要，同时也是满足法规要求的关键。

新标准覆盖面更广，基本内容包括对产品的每一个风险进行分析、评价和控制。到目前为止，国外医疗器械生产企业对以上这些过程进行记录所最常用采用的工具，就是失效模式和效应分析（FMEA）或是其的扩展形式——失效模式、效果及危害度分析（FMECA）。在本文中，除了特别指定，将FMEA和FMECA统称为“FMEA”。

据估计，国外大概80%的医疗器械生产企业使用FMEA对产品的风险进行分析、评价和控制。虽然这种方法效果明显，但其自身所存在的缺陷也会降低风险管理的效果。本文就是要对这些缺陷进行说明并提出解决的方法。

风险管理的要素

在讨论FMEA的特性之前，我们有必要简短回顾一下风险管理中各个阶段的风险分析。

进行风险分析，第一步是根据医疗器械产品自身的特性及其预期用途识别所有相关的危害和损害。那么危害和损害有什么区别呢？危害是指损害的潜在源，损害是危害造成的影响，许多危害（诸如电能、机械能及热能）会造成多种形式的损害。事实上在风险分析过程中，我们所真正关注的就是损害。当然，有时特定的危害可能引起单一的损害。在这情况，两个名词可以相互代替。

当所有的危害和损害都已被识别后，分析过程就只剩下评估每个损害发生的概率及其发生时所造成危害的严重度。概率和严重度相结合（可以采用图表法或数值方法）就可以表示出该危害的风险。

风险分析后，就要对每种风险进行评价了。风险评价就是要决定某一风险是否有必要降低，或其本身是否可接受。当该风险不可接受时，制定措施对其进行降低或控制。

在适当地控制之后，要对危害或损害的风险值进行重新评价，并且要评价这些降低措施是否又产生新

收稿日期：2006-04-21
作者简介：孟杰雄，首都医科大学生物医学工程研究生

的危害或损害。以此类推，不断重复进行这种评价以及必要的控制，直到认为风险是可接受的。

上面的描述只是对风险管理过程的简要回顾，旨在为下面将要讨论的FMEA建立一些概念。

FMEA与产品风险

在哪能够找到使用FMEA和FMECA对医疗器械进行风险分析的指南呢？首先应该考虑的就是ISO和IEC标准。在大多数国家，严格执行这些标准就可以保证产品符合安全性要求。

在ISO和IEC目录中，只有一个标准是关于这一主题的：IEC 60812-1985 “Analysis techniques for system reliability Procedure for failure modes and effects analysis (FMEA)”（我国于1997年等同采用为GB/T 7826-87/IEC 812-1985《系统可靠性分析技术 失效模式和效应分析(FMEA)程序》）。正如其标题所示，该标准并非直接阐述FMEA作为工具在风险管理过程中是如何使用的，但是也提出了对于FMEA一般使用的理解。

传统FMEA的第一个特性就是其标题中的“失效模式”，并且在风险管理中定义“失效模式”是相当复杂的。的确有许多医疗器械产品的风险是由失效产生的（就像IEC 60601-1中所定义的“单一故障”），但是医疗器械的许多风险却来自于设计时的预期用途和正常条件下的使用。

大多数医疗器械是通过有效地控制损害来获得临床受益的。例如一把无法切割人体组织的解剖刀，固然是相当安全的，但是使用这样解剖刀是无法进行外科手术的。这是问题的症结，ISO 14971和EN 1441都明确要求对这些固有风险进行分析和评价，并尽可能地将其减少到合理可接受范围。但是以FMEA为基础的风险管理过程通常不会注意到这种事实，而只把重心集中于设备失效或其使用失效上。如此地实施风险管理既不全面，也不符合任何标准。

FMEA的局限性和缺点可以参看IEC 60812的2.2.4条：“FMEA用于由部件导致整个系统失效的分析时是非常有效的。然而，对于具有多功能和由大量元器件组成的复杂系统，实施FMEA可能感到很困难和很繁琐。这是由于对于来自系统而必须考虑的详细资料为数太多。这些困难还会随系统可能存在的工作模式以及修理和维修方针的考虑而增加。

另一个局限性是通常不包括人为差错的后果，人机关系的研究是一个专门问题。通常，人为差错按时间顺序在系统工作期间显现出来，对其影响的研究必须通过一定的方法，例如因果分析法进行。尽管如此，FMEA还是能够用来识别对人为因素很敏感的部件。当环境的影响很重要时，FMEA表现出更多的局限性。在考虑这些影响时，要求对系统的不同部件的特征和性能有非常全面的了解。”

由于医疗器械行业的特殊性，不只是器械本身很复杂，其所使用的环境也十分复杂。此外，使用的环境中还有存在大量的不确定因素。为了根据ISO 14971：2000正确地进行风险管理，所有这些不确定因素也都要被评价。完全按照IEC所定义的FMEA对产品进行分析风险有时是相当困难的，甚至最后无法取得任何效果。

故障树分析法

克服以上问题的一种途径就是使用故障树分析法，重点使用FMEA分析那些实际导致危害的部件和配件。如果严格按照FMEA操作，就要对每个部件的失效模式进行评估，以决定它们是否会造成危害。

与此相反，故障树分析法首先对器械及其预期操作环境的接口进行分析，寻找所有发生的损害作为顶事件，然后追溯这些损害发生的所有原因和原因的组合，包括由于器械使用或环境影响造成的部件或子系统的失效或损害。最后可以用FMEA只分析可以造成危害的那些设计元素。

以上两种技术最理想的使用方法是：使用FMEA从下到上分析所有部件的失效模式及其影响，同时用故障树分析法从上到下追溯每种损害（顶事件）的所有原因和原因的组合，最后对比验证这两种独立进行的分析结果。但这样操作需要花费大量的时间和金钱，而使用故障树分析法的结果直接进行FMEA分析，就可以大大节省资源、提高效率了。

探测性与产品风险

在应用FMEA进行风险管理时，有些生产企业使用“探测度”这个概念得到一个基本的风险顺序数(RPN)。在IEC 60812中并没有涉及这一概念的使用。它并非产生于开发设计中的FMEA技术，而是来自于使用FMEA评价生产过程。

依据ISO14971的说明，涉及到用数值来估计风险的相对严重程度。风险是损害的严重度和损害发生的概率的结合。实际上，这也是IEC 60812中对于失效效应危害度的估计的描述。

除此之外，在FMEA的计算过程中还需要定义第三3个参数，就是探测度。针对分析找出的每一个失效模式，分析其失效检测方法，以便为系统的维修性、测试性设计以及系统的维修工作提供依据。例如在生产制造过程中，当检测到某个可能造成损害的缺陷时，要么马上采取行动进行维修，要么将该产品滞留等待修理。在这种情况下，就需要根据探测度推算RPN值了。损害可能实际发生于从器械生产到应用于临床的每个阶段，在此期间这种延时是真实存在的。故障检测方法一般包括目力检测、离机检查、原位测试等手段，如BIT(机内测试)、自动传感装置、传感仪器、音响报警装置、显示报警装置等。

但是在使用过程中，检测出产品的某一危害并不能保证避免其损害的发生。下面的例子就说明检测与预防损害无关：手榴弹在击针被拔出10s后，就会发生爆炸；当击针被拔出8s后，手榴弹被扔进了一间屋子内。虽然它能被检测到，但是屋内的每个人都死了。这说明检测和损害的预防是没有关系的。

这个例子有些极端，但是它表明在使用过程中，探测度是不能完全替代严重度和概率来决定基本RPN值的。

事实上检测就是对风险的降低，它可以降低损害会发生的可能性。因此，在制定探测度预防损害时，必须考虑危害被检测到后的以下几个方面是否能满足：首先是在场人员有多少时间可以用于采取行动；其次是在场人员是否清楚发生了什么，和应采取哪些措施；最后是在场人员的知识和所接受的训练能否保证他们是否知道必须采取什么行动来避免受到损害。

在决定探测度时应该考虑以上这些重要因素，当然也要考虑其它可能影响探测度的因素。但是，并没有有关的特殊说明，指导人们怎样评估这些因素来决定探测度。而在评估的过程中，一定要保持前后执行标准一致。

除此之外，我们必须为每一危害记录其中每种因素的评价和基本假设。如若不然，在评审风险分析，以及在产品的寿命周期更新风险分析(ISO 14971：2000所定义的风险管理的关键要素)时就没有任何意义。然而，怎样在风险评价中建立探测度的分析呢？

理想情况是，探测度就是一种降低，它降低了RPN值(通常是由严重度和概率决定)，正如固有的安全设计、防护设计或警告标识等都可以作为探测度。其实判别检测结果并采取必要的措施来避免损害本身就是一种降低风险的措施。实施这一措施的过程包括评估反应时间、在场人员情况和人员人知情况。

这种理想的方法可以确保评估过程的一致性，并记录评价结果和确认信息。然后在设计变更过程中查看这些记录文档，就可以保证做变更时不会无意识地忽视这种探测的作用。这种方法也可应用于对假设的评审，保证现场资料符合风险分析的最初结果。不幸地是，实际情况并不总是那么理想。对于已经开始使用探测度计算风险的RPN数值的组织而言，他们可能已经能够明显感觉到进行探测度分析的巨大阻力。

例如一家器械医疗器械生产企业要建立、健全并实施完全符合ISO 14971：2000规定的风险管理体系。这家企业的工程设计人员已使用严重度、发生概率和探测度来计算每一风险的RPN值。但这种方法的最大问题是：他们时常遇到事实上无法检测的危害。

下面就来举个例子对以上情况进行说明：我们看一台接入危险电压的电气设备，由于设备内部有保护接地线，所以其金属外壳不会引起未接地所带来的电击危害。我们将危害的严重度的等级分为1到10，10代表死亡。发生概率的等级同样分10级，10代表一定发生(概率=1)。最后将可检测度的等级分为1到4，1代表完全可检测到，4代表无法检测。

在这个例子中电击的潜在严重度是10，因为漏电流可以引起房颤。但是由于使用了IEC 60601-1中定义的双重绝缘方法加强了设备的绝缘，这种危害的发生概率就相当的低，因此，我们将其发生概率的等级定为1。但是如果绝缘被击穿，那么未接地的金属外壳就携带了危险电压。在此情况下，除非有人触碰了设备外壳并被击伤，否则这种危害是不会被检测到的。我们将其可检测度的等级定为4。由此计算出RPN值为40($10\times1\times4$)。

不幸地是，风险可接受的临界值规定为30。这就意味着，尽管我们已经进行了防护设计，使得危害的发生概率降低到无需任何措施的等级，但我们还得采取措施降低风险。而在计算中如果不考虑探测度因素，

(下转第86页)

艺卓(EIZO)宣布为更可靠的成像解决方案推出全新3兆液晶显示器

RadiForce®GS310 拥有艺卓为软件拷贝诊断成像设计的“数字均匀均衡器”

近日，Eizo Nanao Corporation（“EIZO”）发布出新型号的 Radiforce 300 万像素单色液晶显示器 GS310。GS310 可以帮助 PACS、胸透、CT（电脑断层摄影）以及 MRI（磁共振成像）等医疗成像应用实现精确的诊断。

GS310 的创新特点包括数字均匀度均衡器（Digital Uniformity Equalizer–DUE），用来实现对亮度不均匀进行补偿。为了对这种不均匀进行补偿，艺卓在位于日本的工厂中对每台显示器都进行了测量，然后根据测量获得数据使用 DUE 队显示器进行调节。另外，DUE 也有助于降低总所有权成本（TCO）和延长显示器的寿命。显示屏上的最高量度和亮度分布会随时间的推移而状况恶化。GS310 同时还配备了 CAL Switch 切换功能，可以使用前面板上的按钮针对具体的图像，如 CR 和 CT，来选择校准模式。

艺卓为 RadiForce GS310 配备了 MED3mp-PPP 和 VREngineSMD5-PCI 显示卡，这两种显示卡都拥有双 DVI-I 输出接口，并且无需使用软件即可实现肖像和风景显示模式。

（上接第 54 页）

我们就无需采取任何措施了。也就是说如果在计算过程中不涉及探测度的因素，设计师的任务就轻松多了。

对于一个对探测度方法有抵触心理的组织来说，在计算器械风险的 RPN 值时，也可以采用以下替代方法来表示探测度。第一种方法是记录对探测度的假设，当然这个假设值是与探测度的真值相关的。为了节省时间，我们可以对情况进行选择性记录：记录的探测度是为了降低或消除进一步降低风险的需求。

第二种方法是将探测度和发生概率合并成一个数值。对风险来说，探测度的作用是降低损害发生的可能性。因此，将这两个数合二为一也是有意义的。

我在前面提到的那家医疗器械生产企业最终采用了第二种方法。我们在定义可能性等级时引入了“探测度”的观念，并将前面那个例子的概率等级分为 1 到 40。

为了牢记“探测度”的作用，我们就应该把可能性数值视为探测度的函数。就是说如果一种故障发生的概率非常之小，就无需在其可能性数值中引入探测度；只有当其发生概率大到一定程度时，可能性数值才受探测度的影响。简而言之，小概率事件无需检测。同时用户不会熟悉很少发生的事情，因此就不太可能记住这种情况下该采取什么措施。而且面对突发情况时人们往往比较惊慌，即使知道该怎样做，也很少有人能够从容应对。而事件发生的概率越大，探测度对事件发生可能性的影响也就越大。也就是说，对于经常发生的事件来说，探测度是一个非常重要的因素。在对产品进行风险分析时，使用这种探测度随发生概率变化而变化的方法是十分有效的。

结论

在估计危害的风险时，引入损害发生的探测度是很有必要的。在实际运用时，如果下面几个问题的答案都是肯定的，那么在估计危害的风险时就应该引入探测度数值：

- 是否有必要经常对损害的发生进行检测？
- 当危害被发现后，人们是否有充足的时间做出反应？
- 是否提供给使用者足够的信息，来说明能够避免损害发生的特殊措施以及这些措施的顺序？
- 使用者是否清楚可能发生的情况，以及遇到这些情况时所该采取的措施？

如果能够保证每次涉及“探测度”时都考虑到以上这些因素，并将结论记录在案，那么就能够保证整个风险分析过程符合 ISO 14971：2000 的要求。有了这些证据，当医疗器械产品因其风险引发官司时，参与风险分析的人员也就无需尴尬地站在证人席上进行解释了。