雷电灾害风险评估技术

吴孟恒 ◆ 等 编著

气象出版社
China Meteorological Press

雷电灾害风险评估技术

吴孟恒　等 编著

气象出版社
China Meteorological Press

图书在版编目(CIP)数据

雷电灾害风险评估技术/吴孟恒等编著. —北京:气象出版社,2009.11

ISBN 978-7-5029-4862-7

Ⅰ.雷… Ⅱ.吴… Ⅲ.雷击火-气象灾害-风险分析 Ⅳ.P427.32

中国版本图书馆 CIP 数据核字(2009)第 205320 号

出版发行:气象出版社
地　　址:北京市海淀区中关村南大街 46 号　　邮政编码:100081
总 编 室:010-68407112　　发 行 部:010-68409198
网　　址:http://www.cmp.cma.gov.cn　　E-mail:qxcbs@263.net
责任编辑:刘　畅　吴晓鹏　　终　　审:纪乃晋
封面设计:博雅思企划　　责任技编:吴庭芳
印　　刷:北京中新伟业印刷有限公司
开　　本:700 mm×1000 mm　1/16　　印　　张:10.75
字　　数:205 千字
版　　次:2009 年 11 月第 1 版　　印　　次:2009 年 11 月第 1 次印刷
印　　数:1—5000　　定　　价:36.00 元

前　言

依据中国气象局令第8号《防雷减灾管理办法》，大型工程、重点工程、爆炸危险环境等建设项目需要进行雷击风险评估，以确保公共安全。

雷电灾害风险评估是指导与统筹各种建设项目防雷工程设计的需要，也是防雷减灾工作科学、规范发展的重要内容。气象部门有责任指导和规范雷电灾害风险评估实施工作。

2008年，我国颁布了国家标准GB/T 21714.2—2008《雷电防护　第二部分：风险管理》，给出了一套完整实用的雷电灾害风险评估方法，对雷电灾害风险评估和雷电防护提供了技术依据。

本书依照GB/T 21714.2—2008，系统整理了上述标准条文，阐述了风险评估的理论原理，介绍了风险评估计算程序使用方法，结合我们的实际工作情况编写而成。对从事雷电灾害风险评估工作的技术人员具有指导意义，也可用于大专院校教学参考。

本书由河北省防雷中心组织编写，由吴孟恒统稿，孟德东编写了第一至四章，付国振编写了第五、第六章，顾东艳、高文平、冯鹤、崔海华编写了部分章节并绘制了全书插图。

由于在防雷基础理论、应用理论研究等方面的不足，加之编者的理论水平和实践经验的限制，书中错误在所难免，恳请读者给予批评指正。

吴孟恒

2009年10月

目　录

第1章　风险管理基本知识

§1.1　风险模型

1.1.1　什么是风险

危险是可能造成伤害或破坏的根源，或可能导致伤害或破坏的某种状态。

风险是某种特定危险事件（事故或意外事件）发生的可能性和后果的组合。风险包括两种因素：① 危险发生的可能性；② 危险事件（发生）的后果。

过去，人们往往依靠经验和直观推断来做出决策。随着技术的发展，风险评估（risk assessment）和风险管理（risk management）技术作为复杂或重大事项决策的必要辅助手段，近年来在决策分析、管理科学、运营研究和系统安全等领域得到了广泛的认知和应用。

风险（risk）的定义通常为：能够对研究对象产生影响的事件发生的机会，它通过可能性和后果这两个方面来具体体现出来。

“风险”用 ISO/IEC TR 13335—1:1996 中的定义可以解释为：特定威胁诱发某个（些）资产的弱点，造成资产损失或破坏的潜在可能性。

风险概念中包括三个因素：

（1）对可能发生的事件的认知；

（2）该事件发生的可能性；

（3）发生的后果。

比如火灾风险（fire risk）包含火灾危险性（发生火灾的可能性）和火灾危害性（一旦发生火灾可能造成的后果）双重含义。

火灾风险评估是指：在火灾风险分析的基础上对火灾风险进行估算，通过对所选择的风险抵御措施进行评估，把所收集和估算的数据转化为准确的结论的过程。火灾风险评估与火灾模拟、火灾风险管理和消防工程之间有密切关系，为其提供定性和定量的分析方法。简单的如消防安全设施检查表，复杂的就会涉及概率分析。在具体应用中针对不同的风险目标的性质和分析人员的经验不同

会有各种变化。

从系统分析的角度来看，风险具有系统特性和动态特性。风险实际上并非某一单一实体或事物的固有特性，而是属于一个系统的特性。若系统发生变化，很容易就会使事先对风险所做的估算随之发生变化。

火灾风险评估模式包括：

(1) 系统认定：即明确所要评估的具体系统并定义出风险抵御措施的过程；

(2) 风险估算：即设定关于火灾的发生几率和严重后果及其伴随的不确定性的衡量标准或尺度，计算和量化系统中的指标的过程；

(3) 风险评估：对该标准或尺度进行分析和估算，确定某一特定风险值的重要性或某一特定风险发生变化的权重。

1.1.2 风险模型

风险即是以下三个要素发生的机会：

(1) 威胁——事件或行为，一般来自系统外部，可能在某些地方会影响固有的弱点，造成影响。

(2) 弱点——系统内部存在的弱点，可能在某些地方受到威胁的诱发。

(3) 影响——短期与长期的影响，威胁碰巧诱发弱点会产生影响。

考虑风险的性质，得到如下的公式：

$$\text{风险} = \text{威胁} \times \text{弱点} \times \text{影响}$$

表面上看，该公式意味着具有高威胁、弱点或影响的系统是高风险的系统。尽管如此，是威胁与弱点的组合造成影响的存在。而对系统的破坏程度依赖于一个事件的发生与影响的促使。用数学语言来说，是威胁与弱点的“逻辑与”。

如：威胁与弱点的特定组合也许仅仅偶尔存在，十分显然，几乎没有弱点“与”/“或”威胁的系统就不大可能长期受到影响。另一方面，一个脆弱的系统，一个具有许多大的潜在影响的系统更有可能遭到毁坏，这是风险管理的基本点，它本身是任何一个组织完好管理中的重要元素。

管理者一般通过引导系统转向风险缓和的活动，如设置合适的控制框架，来寻求减少弱点、威胁与影响。

包含至少两个重要因素（如：高威胁与弱点）的组合能产生比仅具较低或中等水平因素组合更高的风险。任何一个因素降为零，风险将降得更大。

§1.2　风险评估

1.2.1　风险评估

风险评估(Risk Assessment)是指,在风险事件发生之后,对于风险事件给人们的生活、生命、财产等各个方面造成的影响和损失进行量化评估的工作。

风险评估是对一个系统面临的威胁、存在的弱点、造成的影响,以及三者综合作用而带来风险的可能性的评估。作为风险管理的基础,风险评估是组织确定一个系统安全需求的一个重要途径,属于组织系统安全管理体系策划的过程。

长期以来,人们至少在两种意义上,不知不觉地进行着风险评估的活动。

首先,每个人一天中都多次地就自己在特定情况下的行为所能造成的不期望的后果的相对概率进行分析。例如,在横穿马路时,是根据交通信号,还是视当时的交通状况来行动。在作这种判断时,人们既要评估受伤的可能性,也要考虑它的严重性。

另一种意义上的风险评估是基于法律对雇主的要求,判断在特定的情况下,应采取什么样的合理的预防性措施。在此过程中,人们要对风险的程度及随后可能出现的一系列后果,消除或减少风险的工作量和成本做出全面的考虑后进行决断。

现在由框架指令所反映的各地法律要求的风险评估与上述传统方法有所不同。

首次正式的评估报告完成后,要根据实际情况经常更新,在必要时,要用演练作为强制性的检查手段,从而发现那些作业场所传统的安全性方面的漏洞。

风险评估使得控制措施得以合理配置。人们需要有关风险的重要性的概念和尽量地了解这些风险的种类及内容,从而使人们能够就风险控制做出决策,而这种决策应当是可行的又是合算的。

1.2.2　风险评估任务

风险评估主要任务包括以下几个方面:

(1) 识别系统面临的各种风险;

(2) 评估风险概率和可能带来的负面影响;

(3) 确定系统所能承受风险的能力;

(4) 确定风险消减和控制的优先等级;

(5) 推荐风险消减对策。

1.2.3 风险评估类型

风险评估有两大类，它们之间并不互相排斥。

一类是把已知的风险的信息应用到所考虑的环境中去，从而计算出目标概率，这是一种定量的风险评估。

另一类风险评估是一种主观分析，这是一种以风险的综合数据为依据的个人判断，是一种定性分析。

除了对特别的高风险案例外，公众所关心的是哪里会发生事故，事故有多大多严重。在回答这些问题时，用定性风险评估较为简单，也较为适合。法律所要求的也是这一类评估，除非有理由要求使用更加严格的方法。

虽然危害、风险存在于不同的物理领域或者作业场所，一个可以覆盖它们的基本标准的通用的风险评估，还是可以做出的。这就是所谓的“通用”的或者“模式化”的评估，而且应当包括在安全政策的文件中。有时，出于特别的情况或者特殊的理由，当未能给出足够详细的评估时，这些情况要在安全政策中有所说明来引起注意，以便采取进一步的行动。也有另一种情况，这时与特定情况相联系的特定危害要求，每一次都要进行特殊的评估。例如，拆除、装配钢结构作业过程当中的危险性等。

1.2.4 风险评估方法

在风险管理的前期准备阶段，组织已经根据安全目标确定了自己的安全战略，其中就包括对风险评估战略的考虑。所谓风险评估战略，其实就是进行风险评估的途径，也就是规定风险评估应该延续的操作过程和方式。

风险评估的操作范围可以是整个组织，也可以是组织中的某一部门，或者独立的信息系统、特定系统组件和服务。影响风险评估进展的某些因素，包括评估时间、力度、展开幅度和深度，都应与组织的环境和安全要求相符合。组织应该针对不同的情况来选择恰当的风险评估途径。目前，实际工作中经常使用的风险评估途径包括基线评估、详细评估和组合评估三种。

1. 基线评估

如果一个组织（系统）的运作不是很复杂，并且对信息处理和网络的依赖程度不是很高，或者组织信息系统多采用普遍且标准化的模式，基线风险评估（Baseline Risk Assessment）就可以直接而简单地实现基本的安全水平，并且满足组织及其商业环境的所有要求。

采用基线风险评估，组织根据自己的实际情况（所在行业、业务环境与性质等），对组织中某个系统进行安全基线检查（拿现有的安全措施与安全基线规定的措施进行比较，找出其中的差距），得出基本的安全需求，通过选择并实施标准

的安全措施来消减和控制风险。所谓的安全基线，是在诸多标准规范中规定的一组安全控制措施或者惯例，这些措施和惯例适用于特定环境下的所有系统，可以满足基本的安全需求，能使系统达到一定的安全防护水平。

组织可以根据以下资源来选择安全基线：

(1) 国际标准和国家标准；

(2) 行业标准或推荐规范；

(3) 来自其他有类似目标和规模的组织的惯例；

(4) 组织自行建立的基线。

基线评估的优点是需要的资源少，周期短，操作简单，对于环境相似且安全需求相当的诸多组织，基线评估显然是最经济有效的风险评估途径。当然，基线评估也有其难以避免的缺点，比如基线水平的高低难以设定，如果过高，可能导致资源浪费和限制过度；如果过低，可能难以达到充分的安全。此外，在管理安全相关的变化方面，基线评估比较困难。

基线评估的目标是建立一套满足信息安全基本目标的最小的对策集合，它可以在全组织范围内实行，如果有特殊需要，应该在此基础上，对特定系统进行更详细的评估。

2. 详细评估

详细风险评估要求对资产进行详细识别和评价，对可能引起风险的威胁和弱点水平进行评估，根据风险评估的结果来识别和选择安全措施。这种评估途径集中体现了风险管理的思想，即识别资产的风险并将风险降低到可接受的水平，以此证明管理者所采用的安全控制措施是恰当的。

详细评估的优点在于：

(1) 组织可以通过详细的风险评估而对系统安全之风险有一个精确的认识，并且准确定义出组织目前的安全水平和安全需求；

(2) 详细评估的结果可用来管理安全变化。

当然，详细的风险评估可能是非常耗费资源的过程，包括时间、精力和技术，因此，组织应该仔细设定待评估的系统范围，明确系统环境、操作和资产的边界。

3. 组合评估

基线风险评估耗费资源少、周期短、操作简单，但不够准确，适合一般环境的评估。

详细风险评估准确而细致，但耗费资源较多，适合严格限定边界的较小范围内的评估。

在实际评估活动中，组织多是采用二者结合的组合评估方式。

为了决定选择哪种风险评估方法，组织首先对所有的系统进行一次初步的高级风险评估，着眼于系统的社会价值和可能面临的风险，识别出组织内具有高

风险的或者对其系统运行极为关键的部分(或系统),这些部分或系统应该划入详细风险评估的范围,而其他系统则可以通过基线风险评估直接选择安全措施。

这种评估途径将基线评估和详细风险评估的优势结合起来,既节省了评估所耗费的资源,又能确保获得一个全面系统的评估结果,而且,组织的资源和资金能够应用到最能发挥作用的地方,具有高风险的系统能够被预先关注。当然,组合评估也有缺点:如果初步的高级风险评估不够准确,某些本来需要详细评估的系统也许会被忽略,最终导致结果失准。

4. 风险评估方法另一种划分法

风险评估方法也可以用另一种方式来描述。在风险评估过程中,可以采用多种操作方法,包括基于知识(Knowledge-based)的分析方法、基于模型(Model-based)的分析方法、定性(Qualitative)分析和定量(Quantitative)分析。无论何种方法,共同的目标都是找出组织信息资产面临的风险及其影响,以及目前安全水平与组织安全需求之间的差距。

(1) 基于知识的分析方法

在基线风险评估时,组织可以采用基于知识的分析方法来找出目前的安全状况和基线安全标准之间的差距。

基于知识的分析方法又称作经验方法,它牵涉到对来自类似组织(包括规模、商务目标和市场等)的"最佳惯例"的重视,适合一般性系统的安全。采用基于知识的分析方法,组织不需要付出很多精力、时间和资源,只要通过多种途径采集相关信息,识别组织的风险所在和当前的安全措施,与特定的标准或最佳惯例进行比较,从中找出不符合的地方,并按照标准或最佳惯例的推荐选择安全措施,最终达到消减和控制风险的目的。

基于知识的分析方法,最重要的在于评估信息的采集,信息源包括:

- 会议讨论;
- 对当前的安全策略和相关文档进行复查;
- 制作问卷,进行调查;
- 对相关人员进行访谈;
- 进行实地考察。

为了简化评估工作,组织可以采用一些辅助性的自动化工具,这些工具可以帮助组织拟订符合特定标准要求的问卷,然后对解答结果进行综合分析,在与特定标准比较之后给出最终的推荐报告。

(2) 基于模型的分析方法

2001 年 1 月,由希腊、德国、英国、挪威等国的多家商业公司和研究机构共同组织开发了一个名为 CORAS 的项目,即 Platform for Risk Analysis of Security Critical Systems。该项目的目的是开发一个基于面向对象建模特别是 UML 技

术的风险评估框架，它的评估对象是对安全要求很高的一般性的系统，特别是 IT 系统的安全。CORAS 考虑到技术、人员以及所有与组织安全相关的方面，通过 CORAS 风险评估，组织可以定义、获取并维护 IT 系统的保密性、完整性、可用性、抗抵赖性、可追溯性、真实性和可靠性。

与传统的定性和定量分析类似，CORAS 风险评估沿用了识别风险、分析风险、评价并处理风险这样的过程，但其度量风险的方法则完全不同，所有的分析过程都是基于面向对象的模型来进行的。CORAS 的优点在于：提高了对安全相关特性描述的精确性，改善了分析结果的质量；图形化的建模机制便于沟通，减少了理解上的偏差；加强了不同评估方法互操作的效率；等等。

(3) 定量分析

进行详细风险分析时，除了可以使用基于知识的评估方法外，最传统的还是定量和定性分析的方法。

定量分析方法的思想很明确：对构成风险的各个要素和潜在损失的水平赋予数值或货币金额，当度量风险的所有要素（资产价值、威胁频率、弱点利用程度、安全措施的效率和成本等）都被赋值，风险评估的整个过程和结果就都可以被量化了。

简单来说，定量分析就是试图从数字上对安全风险进行分析评估的一种方法。

定量风险分析中有几个重要的概念：

• 暴露因子（Exposure Factor，EF）——特定威胁对特定资产造成损失的百分比，或者说损失的程度。

• 单一损失期望（Single Loss Expectancy，SLE）——或者称作 SOC（Single Occurance Costs），即特定威胁可能造成的潜在损失总量。

• 年度发生率（Annualized Rate of Occurrence，ARO）——即威胁在一年内估计会发生的频率。

• 年度损失期望（Annualized Loss Expectancy，ALE）——或者称作 EAC（Estimated Annual Cost），表示特定资产在一年内遭受损失的预期值。

考察定量分析的过程，从中就能看到这几个概念之间的关系：

① 首先，识别资产并为资产赋值；

② 通过威胁和弱点评估，评价特定威胁作用于特定资产所造成的影响，即 EF（取值在 0～100%之间）；

③ 计算特定威胁发生的频率，即 ARO；

④ 计算资产的 SLE：

$$SLE = Asset\ Value \times EF$$

⑤ 计算资产的 ALE：

$$ALE = SLE \times ARO$$

例：假定某公司投资 500,000 美元建了一个网络运营中心，其最大的威胁是火灾，一旦火灾发生，网络运营中心的估计损失程度是 45%。根据消防部门推断，该网络运营中心所在的地区每 5 年会发生一次火灾，于是我们得出了 ARO 为 0.20 的结果。基于以上数据，该公司网络运营中心的 ALE 将是 45,000 美元。

我们可以看到，对定量分析来说，有两个指标是最为关键的，一个是事件发生的可能性(可以用 ARO 表示)，另一个就是威胁事件可能引起的损失(用 EF 来表示)。

理论上讲，通过定量分析可以对安全风险进行准确的分级，但这有个前提，那就是可供参考的数据指标是准确的，可事实上，在生产过程日益复杂多变的今天，定量分析所依据的数据的可靠性是很难保证的，再加上数据统计缺乏长期性，计算过程又极易出错，这就给分析的细化带来了很大困难。

(4) 定性分析

定性分析方法是目前采用最为广泛的一种方法，它带有很强的主观性，往往需要凭借分析者的经验和直觉，或者业界的标准和惯例，为风险管理诸要素(资产价值、威胁的可能性、弱点被利用的容易度、现有控制措施的效力等)的大小或高低程度定性分级，例如“高”、“中”、“低”三级。

定性分析的操作方法可以多种多样，包括小组讨论、检查列表(Checklist)、问卷(Questionnaire)、人员访谈(Interview)、调查(Survey)等。定性分析操作起来相对容易，但也可能因为操作者经验和直觉的偏差而使分析结果失准。

与定量分析相比较，定性分析的准确性稍好但精确性不够，定量分析则相反；定性分析没有定量分析那样繁多的计算负担，但却要求分析者具备一定的经验和能力；定量分析依赖大量的统计数据，而定性分析没有这方面的要求；定性分析较为主观，定量分析基于客观；

此外，定量分析的结果很直观，容易理解，而定性分析的结果则很难有统一的解释。组织可以根据具体的情况来选择定性或定量的分析方法。

1.2.5 风险评估工具

在各种风险评估工具出现以前，进行风险评估只能手工进行。但是，信息收集、风险识别、风险计算和数据分析等环节工作费时，繁琐，容易出现疏漏。风险评估工具不仅可以将分析人员从繁重的手工数据分析、整理工作中解脱出来，更主要的是它能够将专家知识与技术探测数据进行集中，使专家的经验知识得以推广。点评估工具、渗透性测试工具等风险评估工具的出现，大大提高了风险评估的效率和评估结果的科学性。

风险评估工具的分类

目前对风险评估工具的分类还没有一个统一的理解。风险评估工具被分为三类：预防、响应和检测。

通常情况下安全管理者发现解决安全的问题在于预防。在此基础上，许多国家和组织都建立了针对预防安全事件发生的风险评估指南和方法。基于这些方法，开发出了一些工具，如 CRAMM、RA 等，这些工具统称为风险评估工具。这些工具主要从管理的层面上，考虑包括信息安全技术在内的一系列与安全有关的问题，如安全规定、人员管理、通信保障、业务连续性以及法律法规等各方面的因素，对信息安全有一个整体宏观的评价。

一个完整的风险评估所考虑的问题不只是关键资产在某个时间状态下的威胁、脆弱点情况，以往一段时间内的攻击情况和安全事故都是风险分析过程中用于确定风险的客观支持。对风险评估工具的类型划分是人们在对信息安全风险评估不断认识以及对评估过程不断完善的过程中逐渐形成的。根据在风险评估过程中的主要任务和作用原理的不同，将信息系统风险评估工具分为三类：综合风险评估与管理工具、信息基础设施风险评估工具、风险评估辅助工具。

综合风险评估与管理工具。这种工具根据系统所面临的威胁的不同分布进行全面考虑，在风险评估的同时根据面临的风险提供相应的控制措施和解决办法。这种风险评估工具通常建立在一定的算法之上，风险由关键信息资产、资产所面临的威胁以及威胁所利用的脆弱点三者来确定，如 RA。也有通过建立专家系统，利用专家经验进行风险分析，给出专家结论，这种评估工具需要不断进行知识库的扩充，以适应不同的需要，如 COBRA。

信息基础设施风险评估工具。包括脆弱点评估工具和渗透性测试工具。脆弱点评估工具也称为安全扫描、漏洞扫描器，评估网络或主机系统的安全性并且报告系统脆弱点。这些工具能够扫描网络、服务器、防火墙、路由器和应用程序发现其中的漏洞。通常情况下，这些工具能够发现软件和硬件中已知的安全漏洞，以决定系统是否易受已知攻击的影响，并且寻找系统脆弱点，比如安装方面与建立的安全策略相悖等。渗透性测试工具是根据漏洞扫描工具提供的漏洞，进行模拟黑客测试，判断是否这些漏洞能够被他人利用。这种工具通常包括一些黑客工具，也可以是一些脚本文件。

风险评估辅助工具。这种工具在风险评估过程中不可缺少，它用来收集评估所需要的数据和资料，帮助完成现状分析和趋势分析。如入侵监测系统，帮助检测各种攻击试探和误操作，它可以作为一个警报器，提醒管理员发生的安全状况。同时安全漏洞库、知识库都是风险评估不可或缺的支持手段。

1.2.6 风险评估过程注意事项

在风险评估过程中，有几个关键的问题需要考虑：

(1) 要确定保护的对象(或者资产)是什么？它的直接和间接价值如何？

(2) 资产面临哪些潜在威胁？导致威胁的问题所在？威胁发生的可能性有多大？

(3) 资产中存在哪些弱点可能会被威胁所利用？利用的容易程度又如何？

(4) 一旦威胁事件发生，组织会遭受怎样的损失或者面临怎样的负面影响？

(5) 组织应该采取怎样的安全措施才能将风险带来的损失降低到最低程度？

解决以上问题的过程，就是风险评估的过程。

进行风险评估时，有几个对应关系必须考虑：

(1) 每项资产可能面临多种威胁；

(2) 威胁源(威胁代理)可能不止一个；

(3) 每种威胁可能利用一个或多个弱点。

§1.3 风险评估组织

1.3.1 何时应用风险评估程序

风险评估是为了用于：

(1) 危害看来会造成重大威胁及不清楚现有或计划控制措施原则上或实际上是否恰当的场合。

(2) 组织超过法律最低要求，寻求继续改善管理体系。

当初步研究表明风险微不足道或前期评估显示现有或计划控制措施符合下述条件时，风险评估程序是不必要的或经济上不合算的：① 符合已有的法律要求或标准；② 与任务相称；③ 已为或将为每个有关人员理解和采用。

除确保继续采取适当的控制手段外，这里无须进一步的措施。低风险的小型组织尤应慎重选择用来进行详细评估的风险。将力量投在评估微不足道的风险和标准控制措施上，往往会造成收集的信息过多，并出现在一大堆谬误性的文件资料中忽视了重要因素的现象。

1.3.2 风险评估的重要性

风险评估是风险管理的基础，是制定计划、审核方案的重要依据。只有找到什么地方会出现问题，才有可能对问题进行防范与控制。

风险评估是雇主必须履行的法律义务，其主要目的在于确定计划的或现行的控制措施是否充分，其意图是在伤害发生之前使风险得到控制。

多年来，人们往往采用不规范的形式进行风险评估。现在认识到，风险评估是预防性（事前主动的）管理的重要基础，系统化程序则是风险评估成功的必要保证。

以共同参与的方式进行风险评估为管理人员和劳动者就组织的程序达成共识提供了机会：

（1）程序是以对危害和风险的认识一致为基础的；

（2）程序是必要的和可操作的；

（3）程序会成功地预防事故。

抱着评估是官僚主义强加的负担这种态度去进行计划欠佳的评估，只会浪费时间而不会引起任何改变，不会得出有益的结果。而且，组织可能会陷入形式主义的困境中，即完成了形式上的评估也就结束了评估本身。

风险评估应提供一个行动的清单以形成履行控制措施的基础。

有的风险评估工程师可能会变得自以为是。过于接近危害的人反而可能看不见危害，或把风险看得微不足道，因为就他们所知尚无人遭到伤害。我们的宗旨是，每人都应以全新的眼光和怀疑的态度着手进行风险评估。

应由具备一定实践经验、有能力的工程师来进行风险评估。更可取的是有组织中其他部门的同事的参与，因为他们更客观。只要有可能，培训一些小组来进行评估工作不失为一种很好的方法。

理想上，每人都应该为与之相关的评估尽力。例如，他们应该告诉评估人员，他们想要的是什么以及某些特殊风险控制措施的实用性。在较大的组织中，应有个有能力、有影响且通常来自组织内部的人物来协调和指导评估者的工作。当然，还需寻求专家的指导和提供咨询。

1.3.3　风险评估过程

风险评估的基本步骤：

（1）业务活动分类：编制一份业务活动表，其内容包括厂房、设备、人员和程序，并收集有关信息；

（2）辨识危害：辨识与各项业务活动有关的所有重大危害。考虑谁会受到伤害以及如何受到伤害；

（3）确定风险：在假定计划的或现有控制措施适当的情况下，对与各项危害有关的风险作出主观评估。评估人员还应考虑控制的有效性以及一旦失败所造成的后果；