ICS 25.040
N 10

中华人民共和国国家标准

GB/T 21109.3—2007/IEC 61511-3:2003

过程工业领域安全仪表系统的功能安全 第3部分:确定要求的安全完整性等级的指南

Functional safety—Safety instrumented systems for the process industry sector—Part 3:Guidance for the determination of the required safety integrity levels

(IEC 61511-3:2003,IDT)

2007-10-11 发布　　2007-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

GB/T 21109.3—2007/IEC 61511-3:2003

中华人民共和国
国家标准
过程工业领域安全仪表系统的功能安全
第3部分:确定要求的安全完整性
等级的指南
GB/T 21109.3—2007/IEC 61511-3:2003
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946　68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 2.75　字数 72 千字
2008年1月第一版　2008年1月第一次印刷
*
书号:155066·1-30413　定价 30.00 元

GB/T 21109.3-2007

引起火灾的严重和大范围事件的已减轻事件的可能性相加，并用于类似下面的公式中：

——火灾造成的致命风险＝(所有易燃物质释放的已减轻的事件可能性)×(引燃的概率)×(一个人在区域内的概率)×(在火灾中造成致命伤害的概率)。

将引起有毒物质释放的严重和大范围影响事件应被加上，并用于类似下面的公式中：

——有毒物质释放造成的致命性风险＝(所有有毒物质释放的已减轻的事件可能性)×(一个人在区域中的概率)×(在释放中造成致命伤害的概率)。

风险分析专家的专业知识和小组的知识，对把公式中的因素调节到工厂和受影响的社团所要求的条件来说是重要的。

把应用这些公式所得到的结果加起来就可确定该过程对公司的总风险。

如果它满足或者小于公司受影响的人口数的准则，LOPA 也就完成了。然而，因为受影响的人口有可能经受来自其他现有单元或新项目的风险，如果在经济上能实现的话，提供附加的减轻和风险降低是明智的。

F.14 示例

下面是用来描述在 HAZOP 研究中识别的一个影响事件的 LOPA 方法的一个示例。

F.14.1 影响事件和严重性等级

HAZOP 研究把一个间歇聚合反应器中的高压识别为一个偏差。不锈钢反应器被串联到一个填充钢纤维的增强型塑料塔和一个不锈钢冷凝器。纤维增强型塑料塔破裂将释放易燃蒸汽，如果存在一个点火源就有发生火灾的可能性。因为影响事件将导致在场人员的严重伤亡，LOPA 小组使用表 F.2 选择严重性等级时选择为严重的。影响事件及其严重性分别填入图 F.1 的第 1 列和第 2 列。

F.14.2 引发原因

HAZOP 研究列出了高压的两个引发原因，即至冷凝器的冷却水中断和反应器蒸汽控制回路失效。这两个引发原因被填入图 F.1 的第 3 列。

F.14.3 引发可能性

工厂已有在此区域中每 15 年会发生一次冷却水中断事件的经验。作为一种保守的估计，小组选择每 10 年发生一次冷却水中断事件。在图 F.1 第 4 列中填入 0.1 事件/年。在处理其他引发原因(反应器蒸汽控制回路失效)前，从头到尾直到得出结论都支持这个引发原因是合理的。

F.14.4 保护层设计

过程区域设计具有一个防爆电气等级，并且该区域有一个有效的过程安全管理计划。计划的一个要素是在区域内更换电气设备的更换规程管理。由于更换规程管理，LOPA 小组估计存在点火源的风险将降低 10 倍。因此根据过程设计，图 F.1 第 5 列应填入 0.1 的一个值。

F.14.5 BPCS

在反应器中，高压还伴随高温。BPCS 有一个控制回路，它可根据反应器中的温度调节输入到反应器夹套中的蒸汽。当反应器温度超过设定值时，BPCS 将关断到反应器夹套的蒸汽。因为关断蒸汽足以防止高压，BPCS 是一个保护层。BPCS 是一个很可靠的 DCS(分散型控制系统)并且生产人员从未有过温度控制回路不能使用的失效经历。因此 LOPA 小组决定 0.1 的一个 PFD_{avg} 是恰当的并在图 F.1 第 5 列的 BPCS 下面填入 0.1(对 BPCS 来说，0.1 是最低允许值)。

F.14.6 报警

在流到冷凝器的冷却水上装有一个变送器，它被连接到 BPCS 的另一不同的输入和一个不同于温度控制回路的控制器上。流到冷凝器的冷却水流量低将被报警，并要求操作员干预关断蒸汽。因为报警装置装在与温度控制回路不同的一个 BPCS 控制器中，所以它也被看作是一个保护层。由于操作员一直呆在控制室中，LOPA 小组商定 PFD_{avg} 为 0.1 是恰当的，并把此值填入图 F.1 第 5 列的报警装置下面。

目　　次

——限制接近。

减轻层可以降低影响事件的严重性,但不能防止影响事件的发生。其例子有:

——防火或防烟雾释放用的喷水系统;

——烟雾报警器;和

——撤离规程。

LOPA 小组应确定所有减轻层的恰当的 PFD 并把它们列入图 F.1 的第 6 列中。

F.9　独立保护层(IPL)

图 F.1 第 7 列中列出了满足 IPL 准则的保护层。

把一个保护层(PL)看作一个 IPL 的准则是:

——提供的保护大量降低已识别的风险,即最小降低 100 倍;

——提供可用性程度很高(0.9 或更高)的保护功能;

——它具有以下重要特点:

a)　专一性:IPL 只被设计用来防止或减轻一个潜在的危险事件(例如失控反应、有毒物质的释放、安全壳损坏或者火灾)的后果。由于多种原因都可能导致同一危险事件,因此多个事件情景都可由一个 IPL 来启动动作。

b)　独立性:IPL 是与已验明的危险相关的其他保护层相独立的。

c)　可信性:可信任 IPL 能执行所设计的那些功能。在设计中处理了随机失效和系统失效两种失效模式。

d)　可审核性:它被设计成能有助于定期确认保护功能。安全系统的检验测试和维护是必要的。

只有满足可用性、专一性、独立性、可信性和可审核性测试的那些保护层才可被归类为独立保护层类。

F.10　中间的事件可能性

引发可能性(图 F.1 第 4 列)乘以保护层和减轻层的 PFD(图 F.1 第 5 列～第 7 列)即可得出中间的事件可能性。算出的数的单位为事件/年,并被填入图 F.1 的第 8 列中。

如果中间的事件可能性小于你公司的该严重性等级的事件的准则,则可不用附加的 PL。但是如经济上合适的话,还应进一步降低风险。

如果中间的事件可能性大于你公司的该严重性等级的事件的准则,则需要附加的减轻。在使用安全仪表系统(SIS)型式的附加保护层之前,应考虑固有的较安全的方法和解决办法。如果能进行固有安全设计的改变,则应更新图 F.1 并重新计算中间的事件可能性,以确定它是否低于公司准则。如果不能通过上述方法降低中间的事件可能性至公司准则之下,则要求一个 SIS。

F.11　SIF 完整性等级

如果需要一个新的 SIF,则可由该事件的严重性等级的公司准则除以中间的事件可能性来计算所需的完整性等级。低于此数的 SIF 的一个 PFD_{avg} 被选作 SIS 的最大值并填入第 9 列中。

F.12　已减轻事件的可能性

把第 8 列和第 9 列的数值相乘就可计算出已减轻事件的可能性,结果填入第 10 列中。这种计算一直进行到小组算出每个已识别能查明的影响事件的已减轻事件的可能性为止。

F.13　总风险

最后一步是把显现相同危险的所有严重和大范围事件的已减轻的事件可能性加起来。例如,所有