符合 ISO 26262 标准的安全案例

北京经纬恒润科技有限公司汽车电子事业部

摘要:道路车辆功能安全标准 ISO 26262 为开发安全相关系统提供了开发流程和要求；其中一个关键的要求是生成安全案例（Safety Case），安全案例是通过结构化的论证来证明安全相关系统是可接受安全的。本文通过安全气囊的例子来呈现如何用 GSN（Goal Structuring Notation）方法建立符合 ISO 26262 标准的安全案例。

Abstract: Road vehicle functional safety standard ISO 26262 provides development process and requirements for development of safety-related systems, one of the critical requirements is to create a safety case, which is a structured argument to show the system is acceptably safe. This paper shows how to use the GSN method to create a safety case according to ISO 26262 standard by taking the airbag system as an example.

关键字：ISO 26262， 安全案例， GSN

Keywords: ISO 26262，Safety Case，GSN

一、 引言

如今，道路车辆上（Road Vehicles）越来越多的安全相关功能由电子/电气系统实现。这些系统如果出现功能故障（Malfunction），就有对车辆乘员或者其他道路使用者造成伤害的风险，比如，电动助力转向系统（Electrical power steering, EPS）如果出现助力反向的功能故障，车辆将不能按照驾驶员预期的方向行驶，可能会导致严重车祸，造成人员伤害。为了保证安全，应考虑如何将风险降低到可接受的范围。2011 年 11 月正式发布的道路车辆功能安全标准 ISO 26262[1]就是为了解决这一问题，该标准为开发安全相关系统提拱了过程和要求，其中一个很重要的要求就是生成安全案例（Safety Case），安全案例的目的是通过结构化论证（Argument）来证明安全相关系统是可接受安全的。但是，ISO 26262 标准对安全案例的描述的篇幅很短，并没有给出开发安全案例的指南。本文基于安全气囊系统来介绍如何利用 GSN（Goal Structuring Notation）[2]方法开发符合 ISO 26262 标准的安全案例。

本文的结构为:第二部分首先介绍了安全案例的起源和概念，然后介绍了安全案例的描述方法 GSN;第三部分介绍如何用 GSN 的方法来开发安全气囊系统的安全案例。

二、 安全案例

其他行业如核工业、化学工业、海上石油、铁路行业等，都有法律法规要求在其设施正式投入使用之前，必须提交安全案例以证明其产品是可接受安全的。安全案例

起源于 1957 年英国温茨凯尔火灾（Windscale fire）事故[3]。该事故发生后，成立了英国核监管部门——核设施监察局（Nuclear installations inspectorate, NII），核设施为了获得运营许可，需要向 NII 提交一系列报告以证明设计的安全，此被广泛认为是第一个安全案例，虽然这时候还没有采用“安全案例”这个概念。许多标准给出了安全案例的定义[4]，ISO 26262 标准中的定义为：安全案例应该清晰、全面、合乎情理的论证（有证据支撑）系统在特定的环境中不存在不合理风险。从此定义中可以看出，安全案例包含三个主要的元素：论点(Requirement)，论证(Argument)、论据(Evidence)。论点是指为了保证系统的安全，必须满足的安全需求，对应 ISO 26262 中的安全目标以及各阶段的安全需求；论据是指证明安全的证据，对应 ISO 26262 中的工作产品，比如测试报告、FMEA 分析报告、评审报告等；论证解释论据为什么能够支撑论点，阐述了论点和论据之间的关系，这三个元素之间的关系可以用图 1 表示。

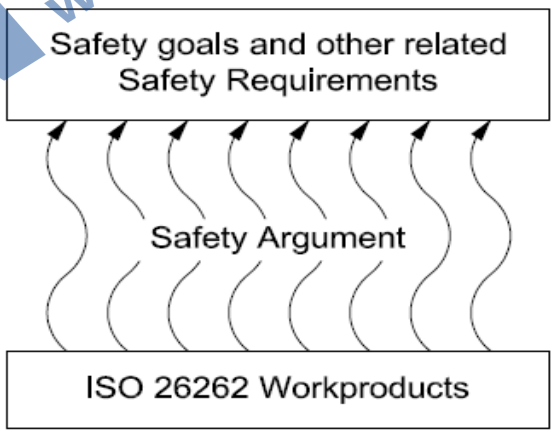

图 1 安全案例三元素之间的关系

没有证据的安全案例是没有基础的，空洞而不具备说服力；没有论证的安全案例是无解释的，证据和需求之间的关系不清楚。安全案例包含两种类型[5]：安全论证（Safety Argument）和置信度论证（Confidence Argument）。安全论证主要证明产品满足危害分析过程中推到出的安全需求，是论证的核心；论证的过程中可能论证的推理或使用的证据有缺陷，比如：测试报告证据，由于测试的人员的能力问题或者测试用例覆盖率不够等原因，使得测试报告的置信度降低，那么论证的说服力也大打折扣，所以这两个类型的论证是缺一不可，相互补充的。ISO 26262 标准中关于避免系统失效的措施属于是置信度论证，比如基于过程的论证（Process-based argument），通过证明产品的开发过程满足标准中定义的过程，安全计划、项目计划、确认措施报告等都是与过程相关的工作产品。标准中关于探测系统失效的措施属于安全论证，比如 FMEA 分析报告、安全措施等都是与产品相关的工作产品。将安全论证和置信度论证分开有利于安全案例的复用[6]、管理和评审。

安全案例是为了向有关机构呈现的，证明系统的安全的。如何撰写论证清晰的安

全案例也是很重要的一个问题。安全案例可以用纯文字描述，但是纯文字的描述方式很难使读者识别安全案例的元素和结构，所以用图表的方式会更清楚，比如：表格式的(tabular)[4]、跟踪矩阵式的(traceability matrix)[7]、Goal Structuring Notation(GSN)。每种方式各有优缺点，这里我们选用 GSN 方法，因为其语法、语义清晰、简单，支持模块化[8]、复用，并且有可遵循的使用指南[9]。

在这里简单介绍一些 GSN 各个符号，关于符号的详细介绍以及 GSN 六步构造方法请参考文献[8]

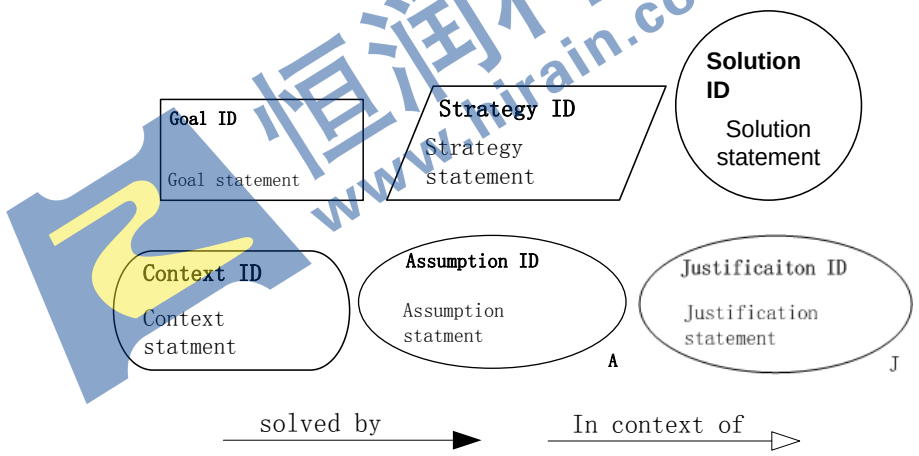

图 2 GSN 图例

目标(Goal)是指要满足的需求，比如：系统 XX 是可接受安全的、模块 XX 是按照 ASIL D 的等级开发的。满足一个目标通常需要通过满足子目标，所以一个目标通常需要进行分解；策略(Strategy) 放在母目标和子目标之间，用于解释为什么母目标可以分解为子目标；解决（Solution） 是指支撑目标的证据；除了以上的核心元素外，环境（context）是指安全论证所处的环境；假设（Assumption）是指论证所基于的假设；说明（Justification）是指对采用策略或呈现安全目标进行理由说明。元素之间的连接线 Solved by 表示目标之间以及目标和证据之间的关系，In context of 表示目标或策略和环境之间的关系。除了这些基本图例外，GSN 支持模块化[9]，如图 3 表示了 GSN 模块，在其他地方展开论证。

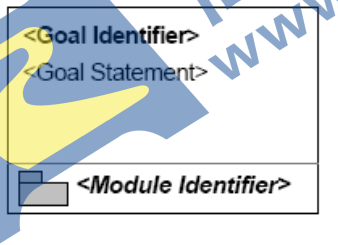

图 3 GSN 模块图例

三、 安全气囊系统

1) 项目定义（Item Definition）

安全气囊的初始架构如下图所示（用 Medini Analyze 工具搭建）。

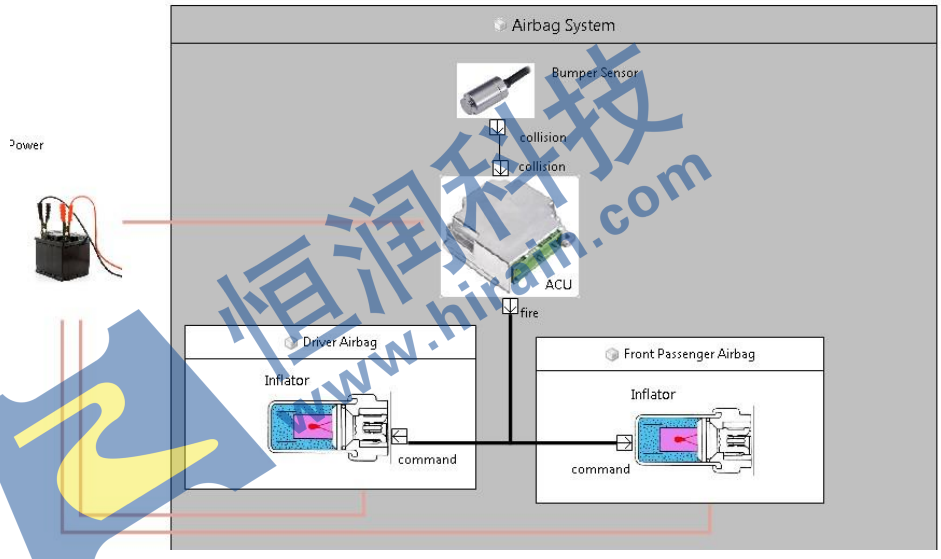

图 4 安全气囊系统初始架构

安全气囊是一种乘员约束系统，当发生汽车碰撞时，气囊快速地打开，避免乘员撞击到车内的物体，比如：方向盘、车窗。安全气囊设计在概念上比较简单；中央控制单元——安全气囊控制单元（Airbag control unit， ACU）监控车内的碰撞传感器（Bumper sensor）。当条件达到或者超过阈值时，安全气囊控制单元触发气体产生点火器，快速的打开尼龙织物气囊。当车辆乘员撞到或挤压气囊的时候，气体以受控的方式通过出气孔排放气体。

2) 危害分析和风险评估（Hazard Analysis and Risk Assessment）

本文章主要针对安全气囊系统中的功能故障“气囊非预期打开”，驾驶场景为“正常驾驶”；经过风险评估，此危害事件的风险等级为 ASIL D，其中暴露率 E 为 E4，可控性 C 为 C3，严重度为 S3。

3) 安全目标和安全概念（Safety Goal and Safety Concept）

安全目标为防止气囊非预期打开，ASIL D，安全状态为关闭安全气囊系统。

功能安全概念为：探测故障并且关闭安全气囊系统。

由于篇幅有限，我们基于以上信息来建立安全气囊系统的安全案例。

图 5 是安全气囊系统的安全案例，图 6 是对图 5 中危害分析和风险评估置信度模块的论证，图 7 是对图 5 中功能安全概念合理性模块的论证。

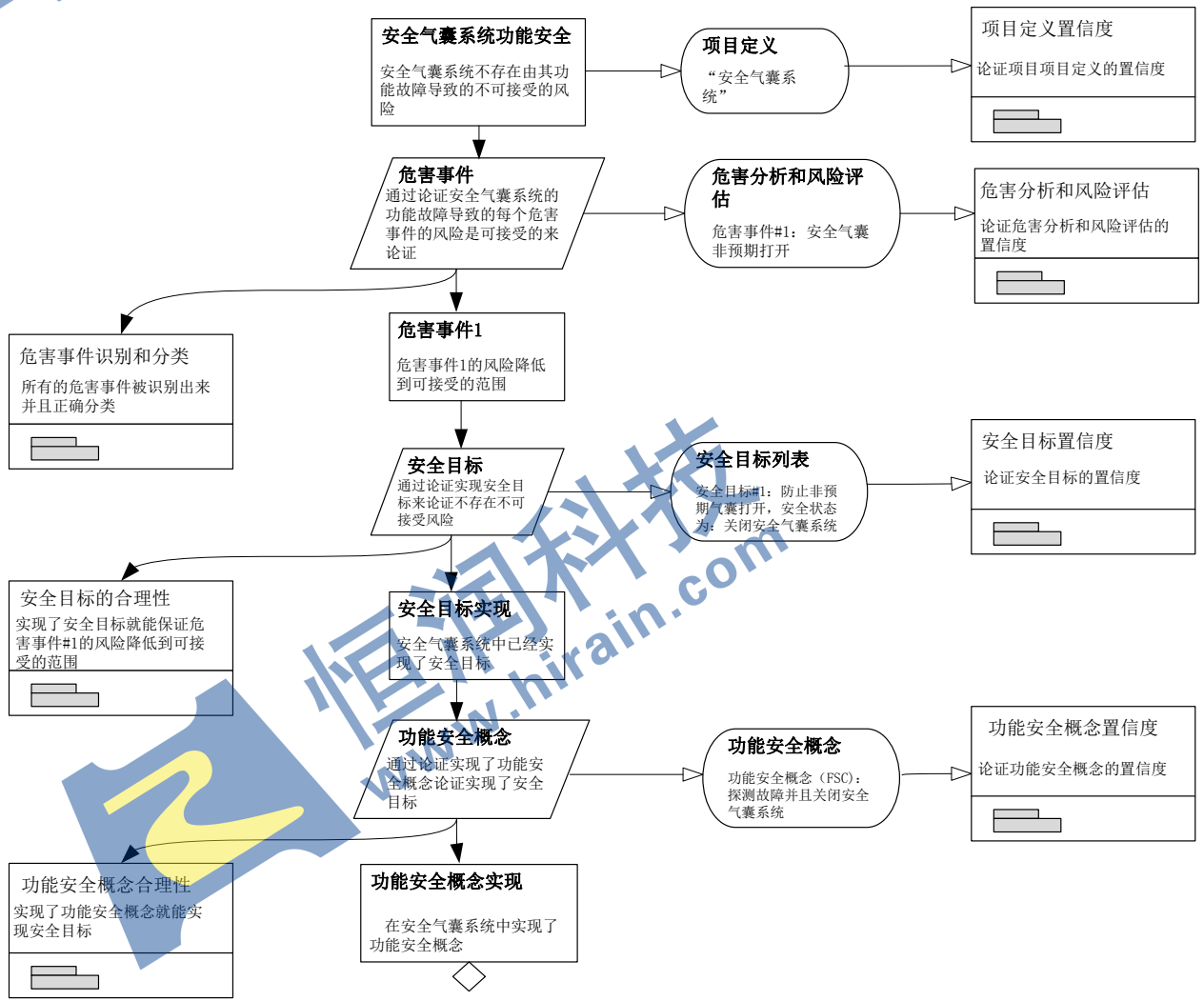

图 5 安全气囊系统功能安全论证

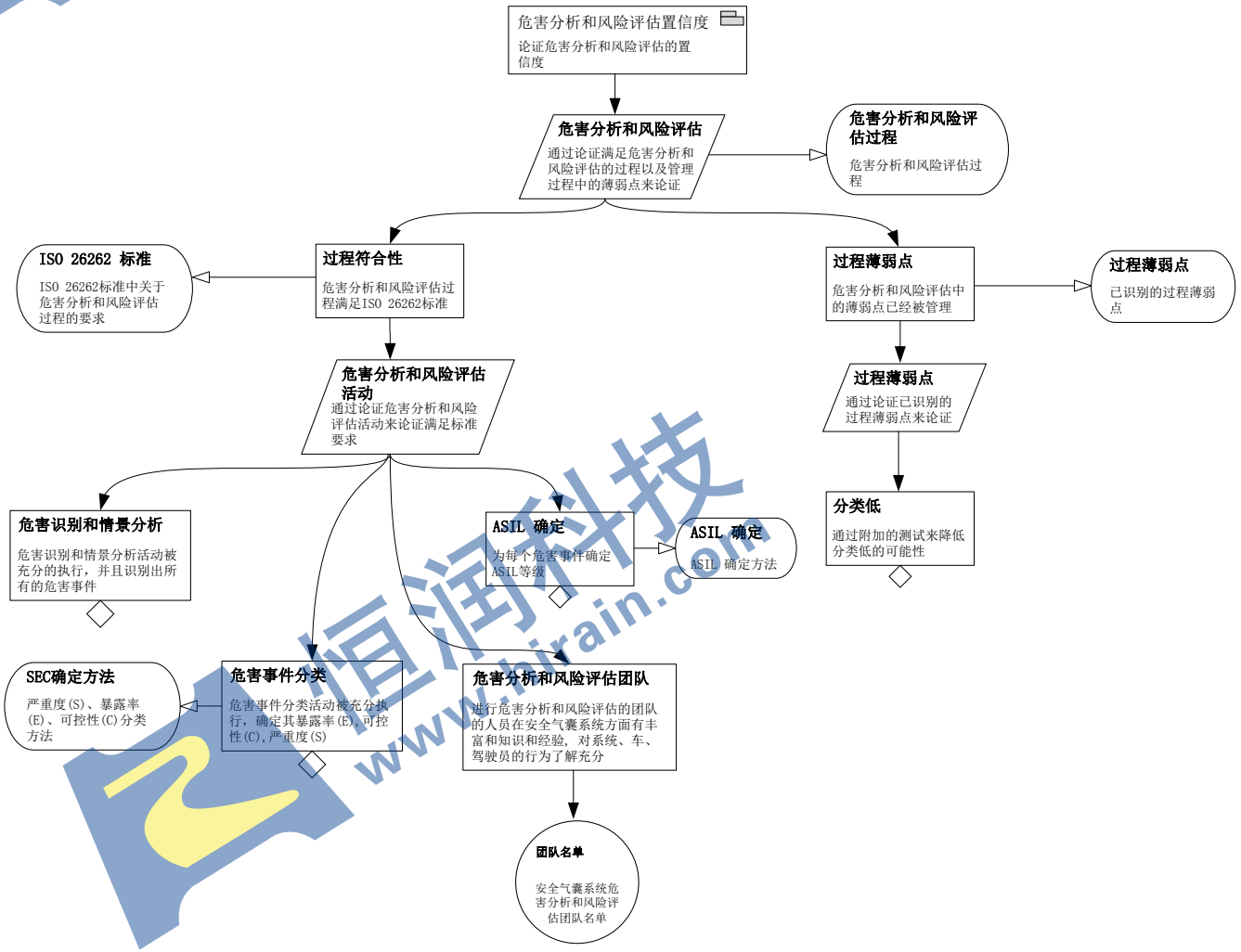

图 6 危害分析和风险评估置信度论证

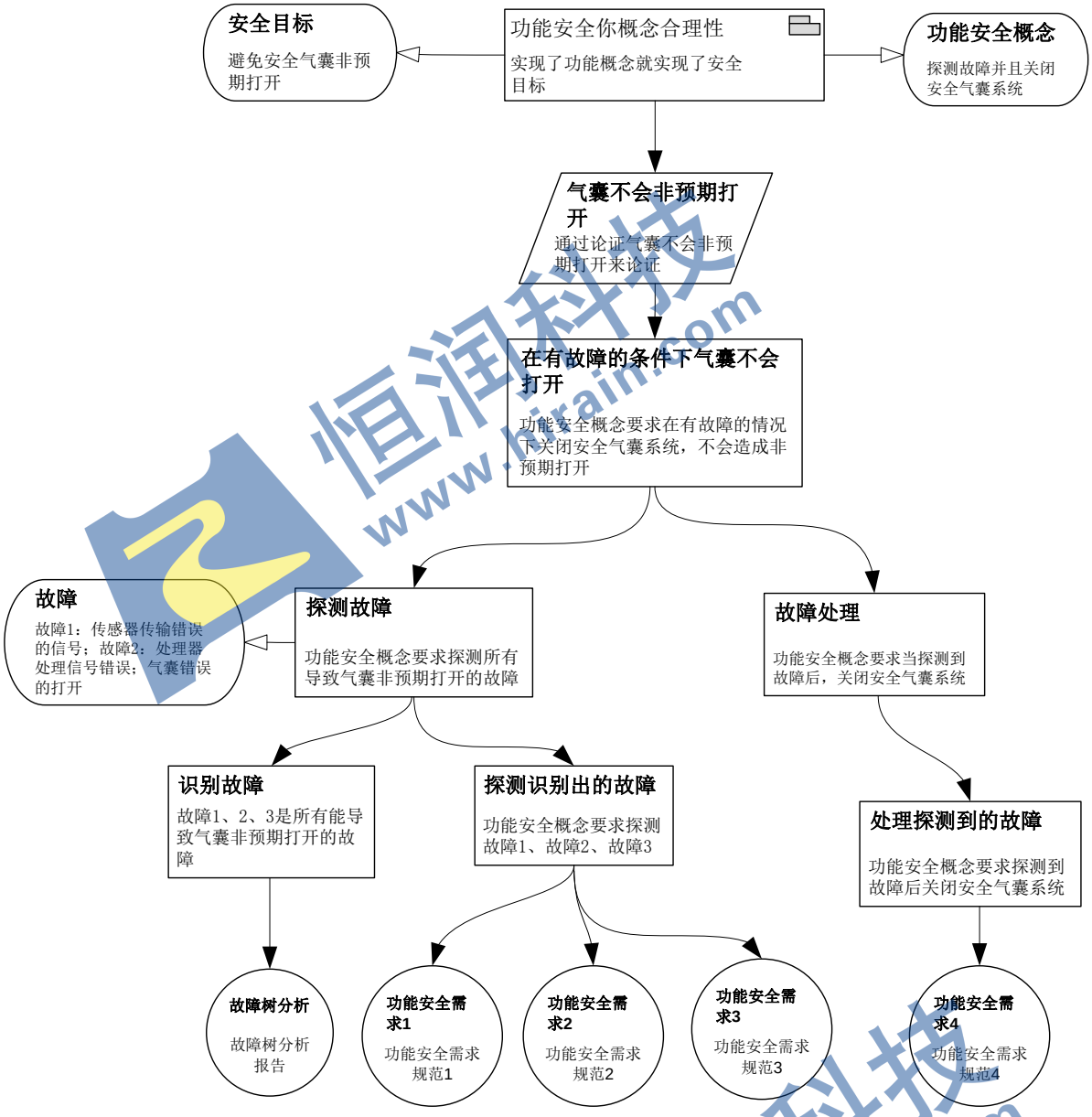

图 7 功能安全概念合理性论证

四、 结论

ISO 26262 标准中明确提出要求生成安全案例，但是标准中没有给出生成安全案例的指南，本文主要介绍了安全案例的起源、概念、描述方式，并且以安全气囊系统为例介绍了如何构建安全案例。

五、 参考文献

[1] ISO: ISO 26262 Road Vehicles -- Functional Safety. ISO Standard (2011)

[2] Kelly, T.: A systematic approach to safety case management. In: Proc. Society of Automotive Engineers (SAE) World Congress (2004)

[3] L. Arnold, Windscale 1957: Anatomy of a Nuclear Accident. London: Macmillan, 1992

[4] MoD, “JSP 430 - Ship Safety Management System Handbook,” Ministry of Defence January 1996; MoD, “00-55 Requirements of Safety Related Software in Defence Equipment,” Ministry of Defence, Defence Standard August 1997.

[5] Habli I., Kelly T. P., “Process and Product Certification Arguments: Getting the Balance Right”, Workshop on Innovative Techniques for Certification of Embedded Systems, in Conjunction the 12th IEEE Real-Time.

[6] R. Alexander, Tim Kelly, Zeshan Kurd, John McDermid. Safety Cases for Advanced Control Software: Safety Case Patterns. Department of Computer Science University of York, 2007.

[7] P. Bishop, R. Bloomfield, L. Emmet, C. Jones, and P. Froome, Adelard Safety Case Development Manual. London: Adelard, 1998.

[8] Bate I. J., Kelly T. P., “Architectural Considerations in the Certification of Modular Systems,” 21st International Conference on Computer Safety, Reliability and Security (SAFECOMP02), September 2002.

[9] T. P. Kelly, “A Six-Step Method for the Development of Goal Structures,” York Software Engineering, Flixborough, U.K. 1997.