RAMS 技术

GSN 安全论证方法在产品安全案例变更管理中的应用

徐征捷，王　奇
（湖南中车时代通信信号有限公司，湖南 长沙　410005）

摘　要：在产品安全生命周期中，安全案例不可避免地会受到不断变化的法规要求、额外的安全证据以及设计变更的影响。为了保持对系统安全的准确描述，必须评估安全案例变更对系统原始安全论据的影响。文章采用目标结构表示法 (goal structuring notation, GSN) 构建安全论证变更管理模型，提出一个清晰的安全案例变更管理分析流程用于明确地表示安全目标与安全案例间相互依赖性，从而能够结构化和系统化地推理和处理变更。目前，该方法已应用于轨道交通信号设备的变更管理中，取得了良好的效果。

关键词：安全论证；目标结构表示法；变更管理；安全案例管理；轨道交通信号设备

中图分类号：X951；TP273.5　　**文献标识码：**A　　**文章编号：**2096–5427(2020)02–0095–05

doi:10.13889/j.issn.2096–5427.2020.02.018

Application of GSN Safety Demonstration Method in Change Management of Product Safety Case

XU Zhengjie, WANG Qi
(Hunan CRRC Times Signal & Communication Co.,Ltd., Changsha, Hunan 410005, China)

Abstract: In the life cycle of product safety, safety cases are inevitably affected by changing regulatory requirements, additional safety evidence and design changes. In order to maintain an accurate description of system security, it is necessary to assess the impact of changes on the original security arguments. In this paper, the goal structuring notation (GSN) was used to construct the security demonstration change management model, and a clear security case change management analysis process was proposed to clearly express the interdependence between security objectives and security cases, so that the change can be reasoned and processed structurally and systematically. This method has been applied in the change management of rail transit signal equipment, and good results have been achieved.

Keywords: safety demonstration; goal structuring notation; change management; safety case management; rail transit signal equipment

0　引言

安全相关机构对产品安全可接受性的认识主要取决于安全认证过程中产生的安全案例是否全面、准确 [1]。安全案例通常在系统首次运行之前构建和呈现，因此，安全论证通常基于估计和预测的操作行为而不是观察到的证据。同时，即使在没有改变系统或监管环境的情况下，安全案例在整个产品生命周期之间不可避免地需要进行更新。虽然 IEC 62278 等标准 [2] 对安全案例的修订提出了明确要求，但对如何开展此类行动没有提供具体的建议。

安全案例是一个复杂的相互依赖的网络，通常包含安全目标、证据、设计和论证过程信息。因此，对安全案例的单一更改可能需要变更许多其他相应的部分，从而产生“涟漪效应”。当前安全案例管理面临的困难在于需要通过结构不良的文档来辨别那些相应的变化，更新安全案例的成功与否很大程度上取决于对文件的理解程度。几乎无法保证所有变更都得到了平等和系统的处理，因为主观

收稿日期：2019–04–15
作者简介：徐征捷（1988—），女，硕士，工程师，主要从事轨道交通信号设备功能安全分析研究。

性在安全案例维护中发挥的作用超出了预期。

基于此，本文采用目标结构法 (goal structuring notation, GSN) 构建安全论证变更管理模型。GSN 方法提供了一个清晰的安全案例概念模型，从而能够有效地整合安全分析中的安全证据材料，明确地表示安全目标与安全案例间的相互依赖性 [3]。通过将该方法应用于轨道交通信号设备的变更管理中，验证了采用 GSN 方法构建安全案例变更管理模型能够系统化地推理和处理变更，提高了变更管理的准确性和全面性。

1 GSN 方法

工程变更是制造企业生产经营活动中贯穿整个产品生命周期的重要活动之一，它可以是简单的对发布文档的重新修正，也可以是复杂的对产品设计和制造过程的重新设计。引起工程变更的原因很多，从设计、工艺、制造到销售服务，几乎每个环节都可能提出变更请求 [4]。由于工程变更活动影响企业多个部门，容易造成产品数据不完整、更改反复等问题，因此，有效管理工程变更的能力是体现企业敏捷性的重要标志之一 [5]。

工程变更过程中，在对项目进行安全评估和认证时，项目管理者需要构建和展示相关的安全案例，从而表明产品满足了相关安全要求。这些安全案例通常被称为安全论据。安全论据用于证明系统危险失效所产生的风险已经减轻到可接受的等级，其与安全目标之间存在着逻辑上的关联关系，意味着层次更接近安全目标的安全论据需要以更底层的安全论据作为支撑，而安全论证是实现安全论据逐步支撑安全目标的方式。

GSN 方法是一种用来呈现安全论证过程的图形化语言 [6]，被广泛应用于核电、航空、汽车行业等与安全相关的领域。这种图形化语言不但可以清楚地论证安全目标与安全论据之间的逻辑关系，而且可以使安全审核人员关注安全证据本身而不是文字的推敲上，因为安全证据与安全目标之间的逻辑对应关系才是安全论证的核心。GSN 中各元素的图形表示和描述如图 1 所示 [7]。

图 1 GSN 中各元素图形表示和描述

Fig.1 Graphic representation and description of elements in GSN

2 GSN 在安全案例变更管理中的应用

2.1 安全案例要素关系

一个完整的安全案例通常由以下 4 个要素组成 [8]：为确保安全必须解决的安全目标 / 需求，来自相关系统的研究、分析和测试的证据，显示证据如何满足安全目标 / 需求的论证过程，以及目标或论证过程所处的环境、所依据的标准或假设等上下文信息。图 2 中所示的概念模型表明这 4 个元素之间存在着宏观依赖关系 [9]，识别这些依赖关系有助于保持变更处理过程的一致性。

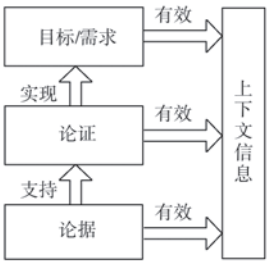

图 2 安全案例要素之间的依赖关系

Fig.2 Dependencies among security case elements

2.2 构建 GSN 安全论证配置模型

传统的配置管理包含配置项和配置关系。使用 GSN 构建框架模型，可以将这些概念与安全案例相关联。本文使用 GSN 构建配置模型，将其应用于安全案例的变更管理中。表 1 对传统配置模型与基于 GSN 的安全论证模型进行了对比。

表 1 传统配置模型与基于 GSN 的安全论证模型的区别

Tab.1 Differences between traditional configuration model and GSN-based security demonstration model

项目	传统配置模型	基于 GSN 的安全论证模型
定义	在给定参考时间点构成系统硬件、软件、固件、服务和供应的相互关系	在给定参考时间点构成安全论证的目标 / 需求、论证、证据和上下文信息之间的相互关系
配置项	配置中满足最终使用功能的实体，一类是产品的组成部分，例如需求文档、设计文档、源代码、测试用例等等；另一类是在管理过程中产生的文档，例如各种计划、报告等	GSN 安全论证模型中的单个实体，即目标 / 需求、论证、解决方案及上下文信息等
配置关系	在开发生命周期的给定阶段建立的配置项之间的关系	GSN 安全论证模型中的各个元素之间建立的关系

3 基于 GSN 的变更管理分析模型

3.1 变更类型分析

安全案例中安全论据的作用是建立可用证据、安全目标和上下文信息之间的关系。任何变更引入的变化类型与典型目标结构的元素之间存在对应关系，这些关联关系如表 2 所示。

一个安全案例必须在目标 / 要求、证据和上下文信息这 3 个方面保持正确、一致和完整。例如，如果安全案例中列出的要求未正确表达监管背景的适用安全要求，则安全案例无效；如果安全案例中使用的设计信息

与运行中的系统设计不一致，则安全案例无效；类似地，选择性地省略已知系统破坏性证据的安全案例也是无效的。安全案例维护的难点在于这 3 类变更类型中的任何一个或全部可能随时间而变化。

表 2　变更类型与目标结构实体之间的关系

Tab. 2　Relationship between change types and target structure entity

变更类型	相应的目标结构要素	目标结构符号
目标 / 要求	目标描述	Goal ID 目标描述
	环境描述	Context ID 环境描述
证据	证据描述	Solution ID 证据描述
	环境描述	Context ID 环境描述
上下文信息	假设描述	Assumption ID 假设描述 A
	论证依据描述	Justification ID 论证依据描述 J
	环境描述	Context ID 环境描述

3.2　构建 GSN 变更管理流程

安全案例变更活动包括 2 个阶段：评估阶段是评估变更对安全案例安全性论点的影响；修正阶段是确定修正行动的过程，并追踪该行为在修正安全论证方面的后果。这两个阶段之间存在迭代关系，修正安全案例破坏部分的行为也可能导致安全案例其他证据损坏。对于任何一次更改，可能需要对变更过程进行多次迭代才能再次形成一致且正确的安全案例，这突出了开展这些活动的有效性和系统化过程的重要性。安全案例变更管理流程如图 3 所示。

图 3　安全案例变更管理流程

Fig.3　Security case change management process

3.2.1　识别变更点

安全目标、安全证据和上下文信息可以看作是安全案例的论据，变更其中任何一个给定条件都将破坏安全案例的有效性，安全案例维护的难点在于这 3 种论据可能会随着时间的推移而改变。可能发生变更的情况有：

（1）操作事故后需要增加额外的监管要求；

（2）系统因纠正或自适应维护等原因需要更新设计；

（3）作为证据的操作经验、实验及测试数据等被质疑。

3.2.2　用 GSN 表示变更

变更类型与目标结构要素之间的对应关系如表 2 所示，在产品发生变更前已经完成了整个系统安全案例的构建，当 GSN 元素或关系受到变更时，在该项上放置一个叉 (×)。本步骤关注的是对目标结构安全论证的初始变更，即起始点的变更影响，而不是总的影响。

3.2.3　用 GSN 识别影响

若证据类型发生变更，通过证据支持连接线（实心箭头表示）可能导致与之相关联的目标的有效性受到影响。同样，若上下文信息类型发生变更，通过补充说明连接线（空心箭头表示）可能导致与该上下文信息类型关联的所有目标的有效性受到影响。确定了单一变化造成的影响程度后，通过结构传播效果逐步线性推理可能受到影响的节点和对象。

3.2.4　确定修改方案

在上一步骤结束时，确定了安全案例中遭到破坏的部分，确定安全案例修改方案可以通过采用一个完全不同的支持论据取而代之，或者可以采用已经使用的论据形式通过更新内容或数据信息对遭到破坏的安全论据进行变更。

3.2.5　修正损坏的安全论据

修正过程是从已确定要求变更节点开始，自上而下一步一步地修正论点，直到安全目标可以与现有证据联系起来。在上一步骤中提出的修改方案将作为变更节点上下文信息的重要组成部分，是目标结构的更改历史记录的一部分，应在变更节点时添加对目标 / 要求涉及的上下文信息的描述。

4　应用实例

本文选择轨道交通信号设备为分析对象，应用 GSN 方法对其时序分析有效性进行安全论证模型的构建，旨在通过实例说明基于 GSN 的模型构建对变更管理的实现过程及其产生的效果。

4.1　构建基于 GSN 的安全论证变更流程

4.1.1　识别变更点

在初步接受安全论证后，发现静态时序分析工具存在一个缺陷，变更涉及的直接影响是导致测试结果不准确，因此识别出变更点为 S1（时序测试结果）有误。

4.1.2　用 GSN 表示变更

在检查了安全论证的 3 种变更类型（上下文信息、解决方案和目标 / 需求）之后，确定上述变更直接涉及

S1（时序测试结果）的变更，如图 4 所示。由于 S1（时序测试结果）是安全论证的初始变更点，因此在该项上放置一个叉（×）。

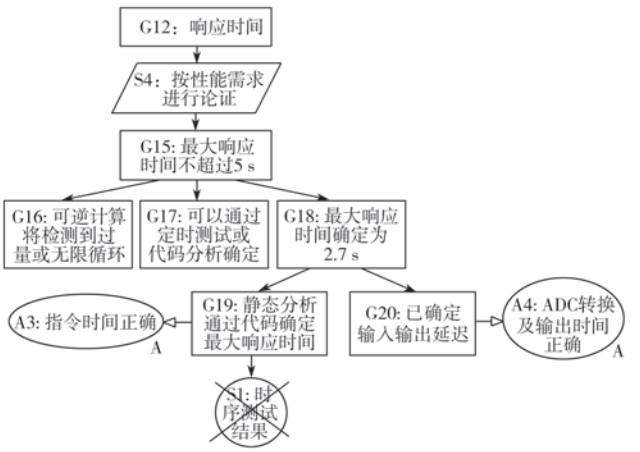

图 4　响应时间安全论证结构模型

Fig.4　Structural model of the response time safety demonstration

4.1.3　用 GSN 识别变更影响

由于静态时序分析工具存在一个缺陷，从而直接导致变更点 S1(时序测试结果) 有误，也就是说，起始变更点为 S1。此时，通过图 4 的结构模型自下向上推理，判断 G19, G18, G15, G12 可能会受到变更影响。由于 G12“响应时间”是系统软件功能需求之一，为了审核整个安全论证结构模型中间接影响到的变更部分，还需要自下向上地将 GSN 模型进行推理。图 5 所示为在安全认证之初构建的安全论证模型，从 G12 继续向上追踪，以推导并确定变更造成的间接影响。

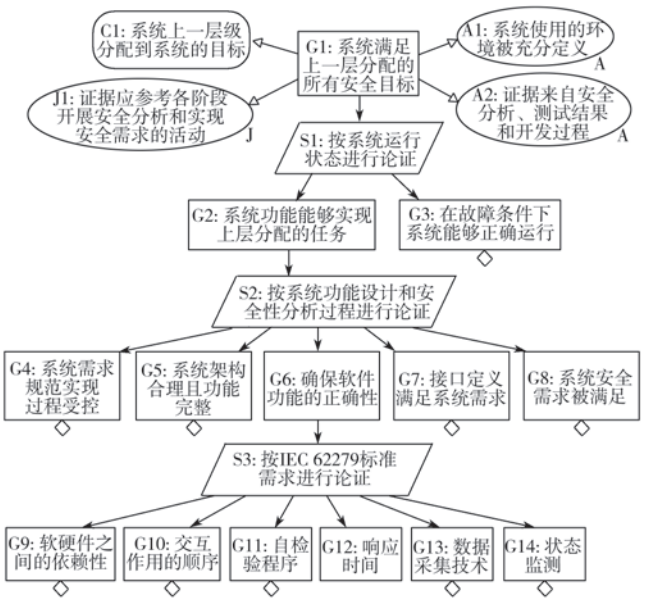

图 5　系统功能安全论证结构模型

Fig. 5　Structural model of the system functional safety demonstration

通过图 5 的安全论证结构模型，自下向上推导出 G6，G2 和 G1 可能会受到变更的影响。经过分析，由于 G15“最大响应时间不超过 5 s”是标准中对系统响应时间的要求，故 G15 不会发生变更，从 G15 向上的分支节点（包括 G12，G6，G2 和 G1）也不会因此受到影响，所以可以确定最终受到变更影响的节点和分支为 G18, G19 和 S1。

4.1.4　确定修改方案

因变更仅仅是由于工具中存在缺陷，对工具更正版本后进行重新分析，以相同的形式修正安全论证结构模型中受到直接或间接影响的分支和对象是最有效的选择。

4.1.5　修正受到影响的安全论据

在将时序分析工具更正版本时，需重新进行时序分析，以方便安全工程师修正损坏的安全论据。假设新结果显示最大响应时间为 2.9 s，则需要重新调整 G18。当 G18 修正后，接下来必须检查 G19 和 G20，并考虑是否还需要重新调整。经分析，变更涉及的直接影响是导致测试结果不准确，G19 与最大响应时间的确定有关，而 G20 仅涉及输出延迟时间的确定，与静态时序分析工具无关。因此，需要对 G19 进行修正，对 G19 的证据 S1 需要进行检查，从而确定是否需要对其进行重新定义。实际上，必须更改 S1 以引用新的时序分析结果；同时，作为记录目标结构的更改历史记录部分，应在修正过程的起始点添加对更改描述和决策的上下文信息描述 A5，这样的注释有助于将来理解结构，并为安全相关方审阅提供一些论证依据。修正后的安全论据模型如图 6 所示。

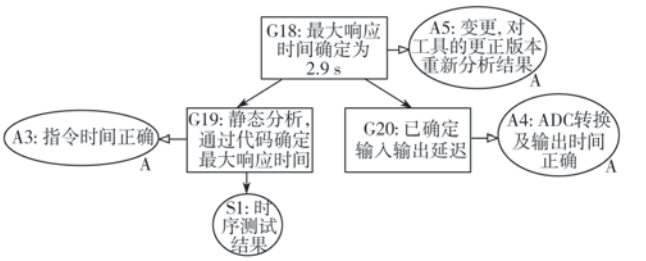

图 6　修正后的安全论证结构模型

Fig.6　Restored structure model of the security demonstration

4.2 变更结果

使用 GSN 方法明确安全目标与安全案例间的依赖性，从变更起始点 S1 通过安全论证模型逐步通过结构传播效果自下向上推出 G19, G18, G15, G12 等安全目标可能会受到变更影响；线性推理可能受到影响的节点和对象，经分析判断，确定最终受到变更影响的节点和分支为 G18, G19 和 S1，并逐步修正论点，直到安全目标可以与现有证据联系起来。该方法能够系统化地推理和处理变更，提高变更管理的准确性和全面性。

5　结语

安全案例变更过程中，采用 GSN 方法能够准确识别出需要对模型中的目标、证据和上下文信息中的哪一项进行变更，从而能够有效应对系统因为结构复杂而导致的变更点不明确问题。

准确识别变更点后，由于 GSN 安全论证过程以图形化的方式进行呈现，采用了更具逻辑性的推理过程来识别变更节点所影响分支的上一层目标或下一层目标或证据，因而能够全面识别变更所造成的影响。

采用 GSN 方法重新构建变更后的安全论证模型，能够方便系统安全相关方对安全论据进行交流、复查，从而进一步加强对安全案例持续有效性的信心。但本文仅给出了轨道交通信号设备在时序有效性方面的变更管理实例，分析并构建不同场景下的产品变更管理模型是下一步的研究内容。

参考文献：

[1]　徐征捷 . 基于模糊 FMECA 方法列控中心安全风险评估研究 [D]. 兰州 : 兰州交通大学 , 2014.
[2]　International Electrotechnical Commission. Railway applications specification and demonstration of reliability, availability, maintainability and safety: IEC 62278-2002[S].
[3]　林虹 . 基于 GSN 方法的 CTCS-3 级车载安全计算机安全论证 [D]. 北京 : 北京交通大学 ,2013.
[4]　刘东升 , 王建明 , 孙家广 . 工程更改管理的设计与实现 [J]. 计算机集成制造系统 , 2001,7(7) : 41-46.
[5]　杨煜俊 , 刘清华 , 万立 , 等 . 基于产品结构的工程变更研究 [J]. 中国机械工程 , 2004, 15(12): 1055-1059.
[6]　牛儒 , 唐涛 . 安全论证方法及其在铁路信号开发安全保障中的应用 [J]. 铁道学报 , 2014, 36(4): 54-59.
[7]　徐征捷 , 殷源 , 黄爱萍 , 等 . 基于 GSN 的安全论证方法在产品功能安全评估中的应用 [J]. 控制与信息技术 , 2019(2): 72-76.
[8]　张杰亮 . FLEDS 的功能安全评估与形式化建模的研究 [D]. 上海 : 华东师范大学 , 2017: 8-10.
[9]　赵长啸 , 阎芳 , 邢培培 , 等 . 面向民机综合化航电系统的安全例证法研究 [J]. 中国安全科学学报 , 2017(7): 82-87.
[10]　徐征捷 . 基于测试的应答器车载设备安全分析方法研究 [J]. 铁道标准设计 , 2017 (10): 162-166.

（上接第 94 页）

（3）对样机在实际环境中的通信距离进行了实测，2 个通信节点分别布设在湘江河岸两边某处，测得可正常收发数据的距离为 1.1 km，如图 7 所示。

图 7　节点通信距离测试

Fig. 7　Node communication distance test

测试结果表明，通信误码率为 0.019 97%，达到无线通信准误码率（2E-04）要求，且系统设计时以连续两次通信无误码情况表示通信有效，通信可靠性在系统设计允许范围内；通信距离为 1.1 km，达到通信要求。

4　结语

本文针对微型无人机集群通信的特点，设计了基于图论的无人机集群信息传递方案，研制了自组织通信网络硬件节点并设计了相应控制软件。通过点对点通信、通信恢复、故障节点识别、数据收发与距离等测试，验证了该信息传递方案的合理性和自组织通信网络节点的可用性，为微型无人机集群通信的实现提供了途径，也为其他自组织网络通信的设计提供了一种参考。

参考文献：

[1]　牛轶峰，肖湘江，柯冠岩 . 无人机集群作战概念及关键技术分析 [J]. 国防科技 , 2013, 34(5): 37-43.
[2]　李崇鞅 . 无线自组织网络的组成及特点 [J]. 数字通信世界 , 2016(3): 20-22.
[3]　吴超宇 , 王明珠 , 张旭东 , 等 . 浅谈无人机集群组网通信技术 [J]. 信息通信，2019,199(7): 128-130.
[4]　徐义桂，陈维义，吕玉萍 . 无人机集群作战通信自组网的关键技术探讨 [J]. 无线互联科技，2019,1(2): 1-2.
[5]　吴平 , 唐文照 . 无人机集群数据链组网技术研究 [J]. 空间电子技术 , 2012(3): 61-64.
[6]　谷文成 , 滕艳平 , 孙晓滨 , 等 . 一种无线自组织网络信息传输的优化方案 [J]. 齐齐哈尔大学学报，2019,35(3):34-38.
[7]　杨迪 . 通信网络中图论的应用方法 [J]. 通讯世界 , 2017(15): 86.
[8]　朱照红 . WiFi 和 ZigBee 混合自组织组网技术在飞行器通信系统中的应用研究 [J]. 电子测试，2018(24): 35-37.
[9]　宋连庆，韩兴会，袁世博 . ZigBee 无线传感器网络平台设计与实现 [J]. 计算机与数字工程，2018，46(3): 508-512.
[10]　杨名权 , 戴欢 , 曾庆燕 . 基于 Zigbee 的无线传感器网络节点设计 [J]. 科技广场 , 2017(2):98-103.
[11]　宋佳 , 门宇博 , 雷丹丹 , 等 . 无线自组织网络 MAC 协议研究综述 [J]. 数字技术与应用，2019,37（6）: 31-33.
[12]　马鹏飞 , 常书杰 , 黄成亮 , 等 . 无线自组织网络 MAC 帧传输技术研究 [J]. 通信技术 , 2012,45 (1): 75-77.