信号系统独立安全评估工作计划大纲

陈国雄 孙达成 沈亦斌 URS/伟信集团

概　　要: 现今铁路系统正处於急速发展的阶段，其铁路网络变得较从前更广阔及多样化。在这繁复的网络中，要取得稳定而有效的营运，信号系统是不可或决的。事实上，在一般铁路控制，以至铁路安全，也需依赖信号系统帮助，方能达到预期效果。为了令信号系统更稳定安全及更具效率，第三方的独立安全评估是必须的。本文将以深圳轨道交通龙华线(4 号线)二期工程〔港铁轨道交通(深圳),合同编号 :C446,以下简称为 C446〕为蓝本，简介URS/伟信集团在以上项目中的信号系统安全评估工作，其中包括以英国铁路为基准的工程安全管理程序（黄皮书）、 URS/伟信集团独立安全评估方法要点概述、评估方法、质量控制和咨询团队。

1.0 工程安全管理

1.1 工程安全管理-黄皮书 (The Yellow Book)

《工程安全管理》(Engineering Safety Management)（以下简称为 黄皮书）是由英国铁路安全与标准委员会(UK's Railway Safety and Standards Board - RSSB)出版，为确保了工程的安全水平、安全相关系统或安全关键系统的完整性提供了工程安全管理的指导方针和最佳实践，适合英国的法律和监管环境。对系统进行独立的专业审查是良好的工程管理的其中一环。审查的类型包括由审核员或审核队伍对系统的运行进行独立安全审计和独立安全评估。C446 工程项目的招标文件恰如其分地列明了须以《黄皮书、 4 版》(The Yellow Book-Issue 4)的标准进行独立安全评估。

URS 伟信的独立安全评估方法遵循了黄皮书的指引和程序。我们的审核和评估方案和程序符合了黄皮书的清单和要求，然而，虽然技术和程序评估是独立安全评估的一部分，但黄皮书中并没有为其评估方法提供具体指南。在技术和程序评估方法方面，URS 伟信采用了一些更高层次及有效的方法（相比传统的分析技术而言），如 Hazard and Operability Study (HAZOP)和 Fault Tree Analysis (FTA)等）。以下将会概述我们所提议的评估方法，通过这高效的评估方法，我们能满足工程的各种要求。

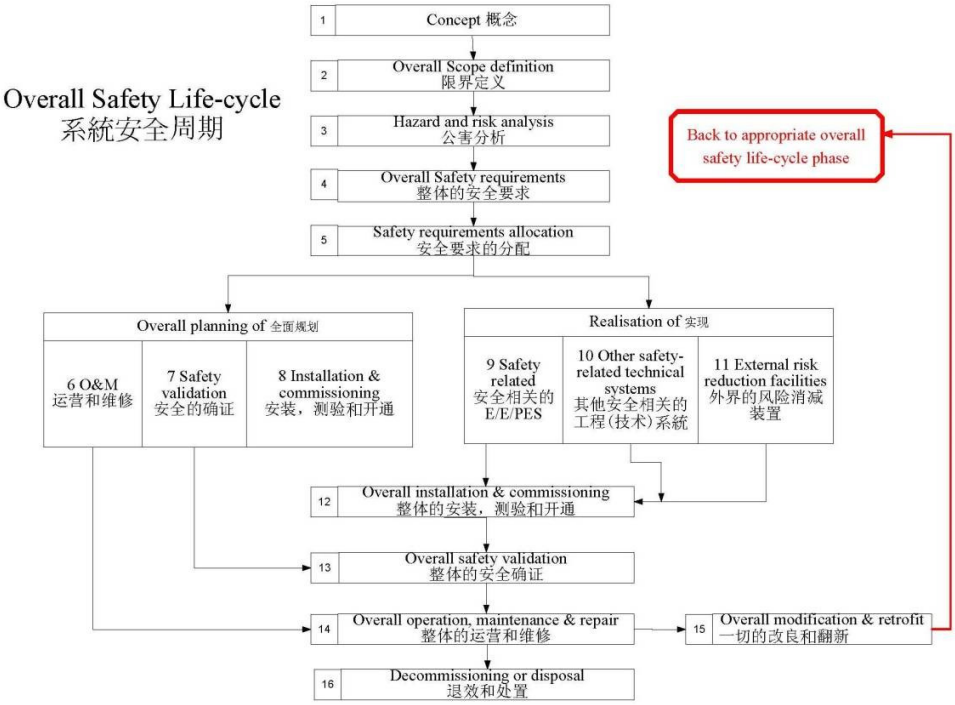
1.2 黄皮书中关于独立安全评估的关键

黄皮书中要求，独立安全评估需要能对项目进行及时、精确的反馈，才能避免浪费不必要的财力物力，以此辅助工程顺利进行。同时，它也提供了具体指南，详细说明了独立安全评估的内容、时间和程序，具体参照《独立安全评估 2.0 版操作指南 4》(Application Note 4-Independent Safety Assessment Issue 2.0)。但是，黄皮书并没为技术和程序评估提供具体指南。传统的评估方法为通过核对审核内容清单，对工程队伍或承建商提交的安全成果与文件的涵盖范围和准确性进行审核。

我们也曾外雇独立安全评估队伍对其他铁路项目进行安全评估，但是，经验告诉我们，这类方法并无法达到预期的效果，外雇的评估队伍往往会忽略一些非常重要的隐患，或者在工程的最后阶段才发现，以致某些灾害无法得到有效控制。事实上，一些由英国国防部资助的研究项目证实，在使用传统的方法或技巧的情况下，仅有 80%到 85%的灾害能在系统的工地测试阶段被侦测出来。因此，如欲为审查的系统提供及时且准确的反馈和事前的安全保证，就必须要有一套更有效的技术和程序评估方法。我们的方法能够达到这个目标，关键之处如下。

1.3 URS 伟信独立安全评估方法要点概述

大多数险情的发生都是因为系统错误。除非管理得当，否则这类错误将于工程系统生命周期的各个阶段出现。(见下图 1)。



图(1)：系统安全周期

开展安全审核与评估的最终目的是为了尽可能多的找出这些系统错误并尽早修正。系统错误可根据它们的属性/性质分为不同类别，并需根据不同的方法对症下药。此外，在不同阶段产生的系统错误通常会具有不同的属性（因此需要采用不同的方法以找出/控制这些错误）。我们的方法尤其适合用来识别在不同阶段产生的系统错误。

2.0 评估方法

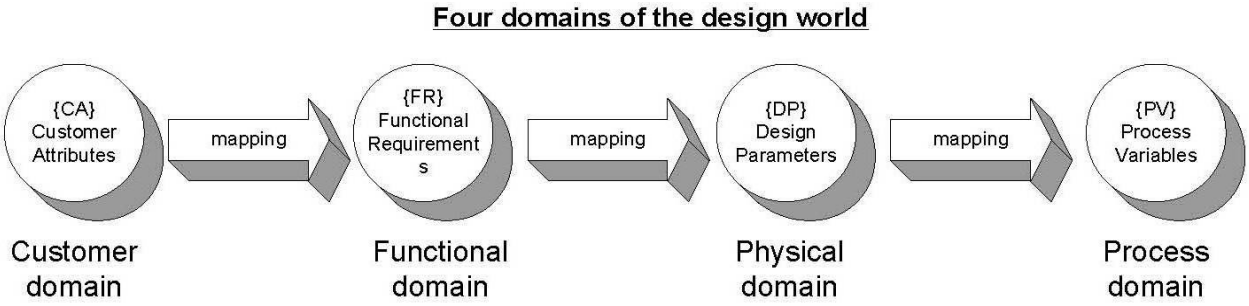
2.1 Independent Safety Assessment (ISA)

对于 C446 ISA 项目，我们建议采用一套基于公理化设计框架、TRIZ-Theory of Inventive Problem Solving（创造性解决问题方法）及危害分析与记录方法的方法。

2.2 公理化设计框架

公理化设计理论与框架由一位麻省理工学院的教授研发，用于开发高质量的产品。该框架在美国、亚洲（韩国、台湾）、欧洲（荷兰）及其他国家被广泛采用。有关该框架的文字介绍及在各不同学科与行业的应用情况，请点击以下网站查看 http://www.axiomaticdesign.com/publications/default.asp

该框架原本是用于开发产品，将开发周期分为四个阶段 / 领域（见下图 2）。



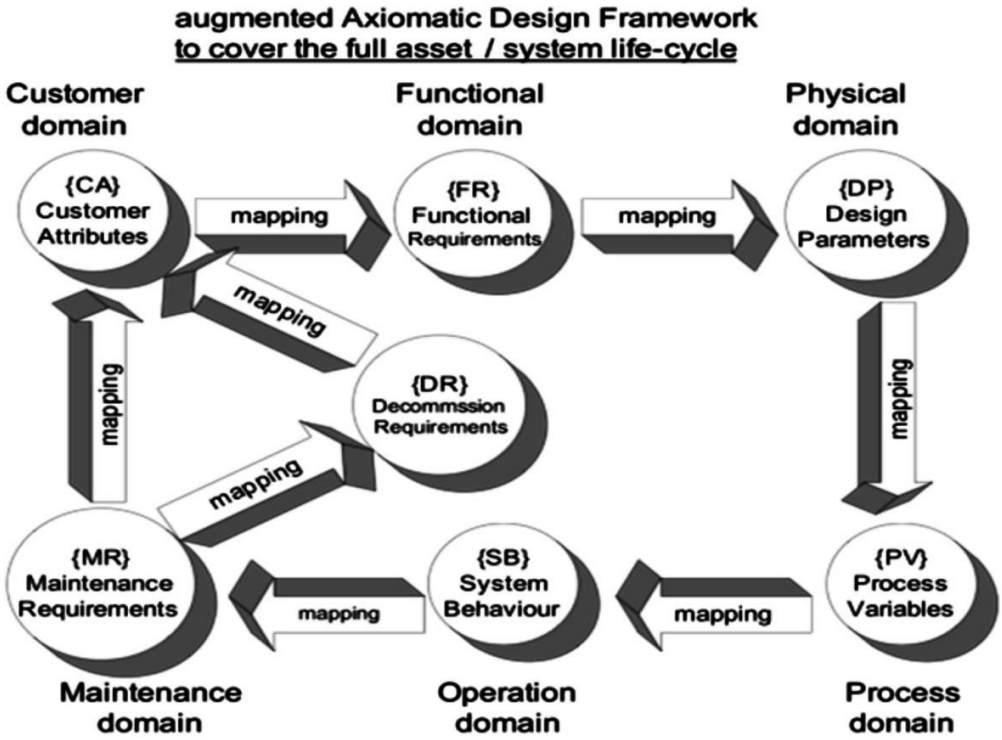
(Figure 1.2 of the Axiomatic Design Framework)
{x} are the characteristic vectors of each domain. During the design process we go from the domain on the left to the domain on the right. The process is iterative in the sense that the designer can go back to the domain on the left based on the ideas generated in the right domain.

图 (2) : 开发周期的四个阶段

其核心概念是识别各个领域内那些对产品质量有关键作用的因素 / 属性（通常包括性能、功效、可靠性、工艺与安全性等）。通过绘制各个领域的属性 / 因素图，可以有效地实现产品在要求 / 属性方面的可追溯性。

该框架实际上可广泛应用于所有工程学科类型（电气、电子、机械、软件之类等等）。

我们将该框架的范围扩大至全面涵盖系统周期的运营、养护及报废阶段（见下图 3）。



图(3)：URS/伟信集团采用的开发周期

通过采用公理化设计框架的概念，同时结合其它相关技术（在下一部分会有具体阐述），我们就能在独立安全评估工作的早期阶段有效地找出安全隐患。

2.3 Theory of Inventive Problem Solving (TRIZ)

TRIZ 是“创造性解决问题方法”的缩写，由俄国专利注册办公室的一名工作人员发明。该方法在形成过程中分析了 47，000 个专利案例，为解决不同性质/领域的工程问题提供了 40 项原则。TRIZ 在世界各国都非常流行，以下网址可以找到关于该方法的详细介绍：

http://www.triz-journal.com

http://www.triz40.com/affPrinciples.htm

TRIZ 为我们进行独立安全评估（ISA）的工程师提供了一套系统的方法，用以衡量减少危害的设计方案是否稳健。另一方面，它又增强了我们查找由于设计缺陷类安全隐患的能力。

除了以上提及的方法和技术，对于客运列车安全关键系统的技术评估，我们还拥有一套自己的评估项清单。下面的总结构图（见下图 4）就是关于一条铁路各工程系统一些关键因素的例子（包括界面）。

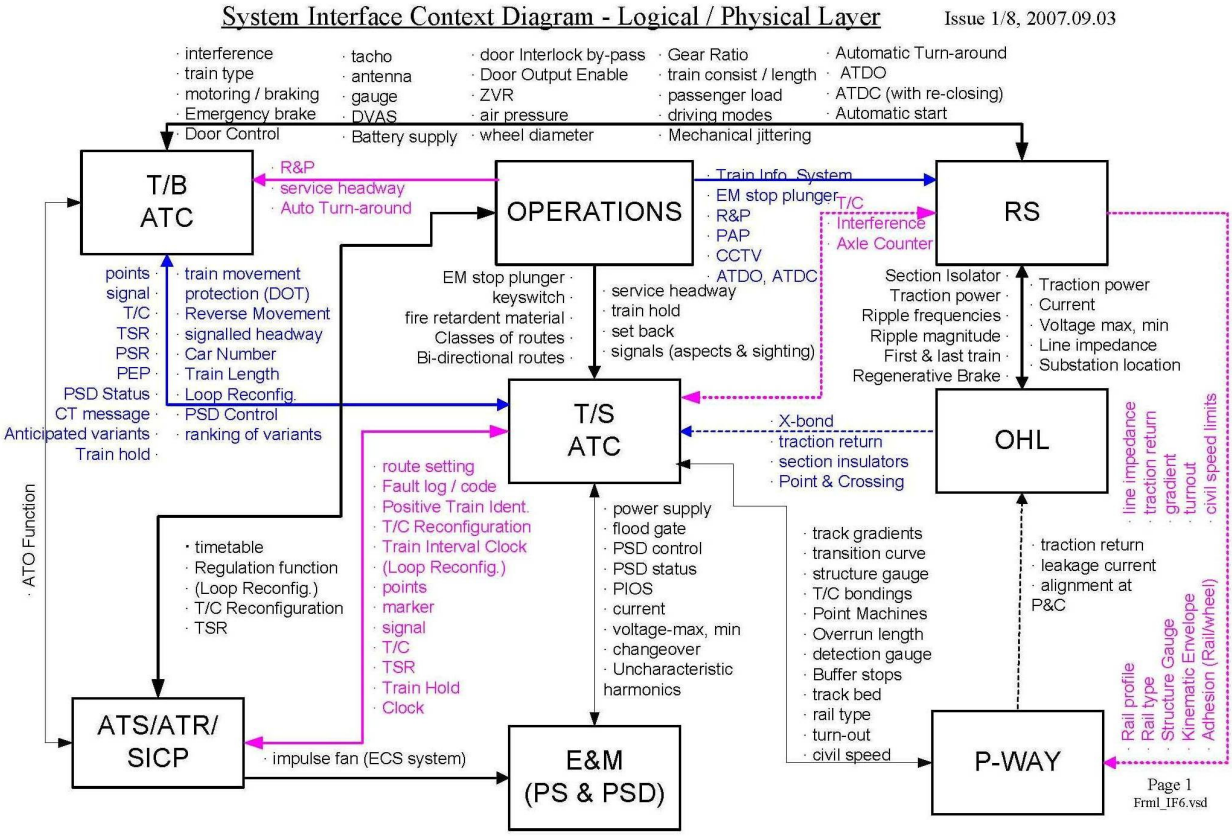


图 (4): 铁路工程系统总结构图

ATS / ATR	自动列车监察调控系统
E&M	机电系统
Operation	车务
OHL	牵引电力系统
PS	供电系统
PSD	屏蔽门
P-Way	（路基、道床、路轨）
RS:	车辆, 列车
T/B ATC:	车载 ATC 系统
T/S ATC:	軌旁 ATC 系統

表(1) 铁路工程系统总结构图词汇解释

此外我们还开发了一套清单，用于检测遗漏了的潜在隐患。

以上方法的早期形式/版本在港铁公司的运营铁路独立核查程序中有过多年的应用，当时是由我们的首席评估顾问在港铁公司工作时发展出来的一套方法。实践证明这套方法在查找新的或遗漏的安全隐患以及危害控制/缓解的测量方面是非常有效的。

综上所述，有一点应该明确的是，这个方法本身不会改变信号传输合同/承建商设计与开发程序的要求，也不需要承建商做额外的工作（在承建商已经做好了必要的和充分的安全保障工作的前提下）。另一方面，该方法又为承建商/项目采用的技术提供了更多的选择。

3 质量控制

URS 伟信项目组将采用《URS 伟信质量手册》中的 URS 伟信质量管理系统 (Scott Wilson Quality Management System)。该手册编制的目的是为了确保 URS 伟信安全要求的确立、维持和控制。URS 伟信安全要求达到、部分甚至超过了 ISO9001：2000 的要求。手册包括一个方针陈述，同时还涉及《URS 伟信质量程序手册》中定义的具体的工作程序。

补充手册包括：

- 方针与程序
- 专业与技术标准
- 索赔评估
- 计算机系统普通用户手册
- 计算机辅助绘图（CAD）参考手册
- 准备草图
- 驻地盘工作人员手册

质量控制团队每 2 个月举行一次会议，对这些手册进行审议，在必要时对其进行更新，并且通过文件的控制确保文件的更新和更新后的使用。每个项目都经过审计，以确保项目正在按照正确的流程开展，出现的错误已经得到纠正。同时还会为系统和抽查的项目引入第三方审计，确保符合 ISO9001 的要求。

每个项目都有项目质量计划，在计划中会安排主要员工的责任，并明确哪些责任应在内部完成，又或是在旗下分公司甚至外判分包顾问完成。质量管理系统成功运行的关键在于对系统需求的了解和对所有员工的培训，

4 咨询团队

为确保 URS 伟信 C446 项目在开展系统独立评估时提供高质量服务并满足客户预期的要求，URS 伟信派出的专业团队中绝大多数的员工在相关的铁路项目有丰富的经验，而整个团队拥有所有项目必须的技能和设备——软件工程、车辆/列车自动控制界面、EMC、牵引动力、RAMS 分析与演示、安全风险管理、安全审计和评估以及系统集成。

在信号系统独立安全评估工程中，我们团队的评估和审计涵盖以下三个主要系统（包括软、硬件）：

a. 轨道信号系统

b. 电务信号系统

c. 信号控制系统（火车自动调度监控）

URS 伟信将采用全面、有效的安全审计和评估方法。其中重点就在于，通过 10 年来香港和其他地区铁路项目的实践证明采用的方法是行之有效的。

结　　语: 安全评估工作可以外部或内部形式进行，前者是由营运者邀请第三方来进行有关工作，後者则是由营运者进行内部评估。现今不少铁路营运者都倾向采取以外部形式进行信号系统安全评估工作是建基於前者的独立性，希望以更客观的角度和手法，找出铁路在安装、测试、设计、生产、及调试阶段内的安全管理是否能确保讯号的稳定传递。

不管是全新培训或者对以前培训的巩固。我们将指定一名培训经理，负责员工的培训计划，确保不同职位员工都得到适当的培训机会。我们每年会对培训需求进行统计。

在这十年间，全球铁路在各个层面的需求不断提升，如列车速度至车厢设施等。故此，铁路在硬件及软件上便需要不断改变来迎合需求。但是，在迎合需求的同时，其改变也为讯号的稳定传递带来警号。当中，有些改变是不明显的。而独立的评估工作有助找出这些改变，从而协助铁路营运者实行有关措施来配合这些改变。

有见及此，讯号系统独立安全评估工作在铁路营运上有着重要的建树，也间接促进了铁路的发展。

参考文献

[1] 英国铁路安全与标准委员会(UK's Railway Safety and Standards Board)，黄皮书 (The Yellow Book)

[2]http://www.axiomaticdesign.com/publications/default.asp，公理化设计框架

[3]http://www.triz-journal.com ， TRIZ 的介绍

[4]http://www.triz40.com/affPrinciples.htm ， TRIZ 的 40 条应用定律

[5]深圳轨道交通龙华线(4 号线)二期工期，合同编号 C446，信号系统独立安全评估-第二册 技术标书 (2010 年 1 月)

[6]伟信顾问集团有限公司，URS 伟信质量程序手册(Scott Wilson Quality Procedures Manual)