

DOI:10.16356/j.1005-2615.2015.04.006

基于本体的陆空通信风险识别与分析方法

王洁宁¹ 周 沅² 黄俊祥³

(1. 中国民航大学天津市空管运行规划与安全技术重点实验室, 天津, 300300;

2. 中国民用航空华东地区管理局, 上海, 200335; 3. 中国民用航空厦门空中交通管理站, 厦门, 361006)

摘要:陆空通信是实施空中交通管制的重要手段,也是民航空管运行中造成不安全事件的重要因素之一。提出针对陆空通信危险识别与分析的系统参量和引导词,应用 BPMN 和 HAZOP 模型识别与分析陆空通信危险偏差。建立陆空通信风险识别与分析本体模型。构建概念之间的 TBox 描述逻辑关系和推理,案例推理证明了方法的有效性。该方法能够实现规范化、术语化风险描述和归类,避免通过自然语言进行风险识别与分析的缺点,为更有效地进行风险项分析提供科学分类和统计依据。

关键词:空中交通管制;陆空通信;风险识别与分析;本体

中图分类号:TP391

文献标志码:A

文章编号:1005-2615(2015)04-0508-09

Air-Ground Communication Risk Identification and Analysis Method Based on Ontology

Wang Jiening¹, Zhou Yuan², Huang Junxiang³

(1. Tianjin Key Laboratory of Operation Programming and Safety Technology of Air Traffic Management, Civil Aviation University of China, Tianjin, 300300, China;

2. CAAC East China Regional Administration, Shanghai, 200335, China;

3. CAAC Xiamen Air Traffic Control Station, Xiamen, 361006, China)

Abstract: Air-ground communication plays an important role in air traffic control. Many incidents have relation to air-ground communication faults. A set of system parameters and guide words for the hazards identification and analysis is proposed. Combining BPMN with HAZOP, the negative deviation from normal operation is detected. Meanwhile, an ontology model aiming at risk identification and analysis is also implemented using Protégé tool. With the construction of description logic among the ontological concepts of TBox, the reasoning approach is realized and validated via real incident case. This method has benefit on risk description and category by standard terminology to overcome shortcomings of natural language description. It is also useful to classify risk items clearly for further post statistic analysis.

Key words: air traffic control; air-ground communication; risk identification and analysis; ontology

空中交通管理系统作为民用航空运输系统的重要组成部分,其运行安全问题长期受到关注^[1-2]。笔者针对空管运行安全问题,通过文献分析,总结出空管系统的三大特征,即空管系统是:高度分布

式系统、复杂联合认知系统、社会-技术系统,在空管系统中存在大规模的人员与技术系统交互行为^[3]。由于空管系统在运行安全方面的这些特征,客观上需要通过系统化的方法对其运行安全进行

基金项目:中央高校基本科研业务费专项资金(3122013P008, 3122014D040)资助项目;空管科研课题(GKG201410003)资助项目。

收稿日期:2015-07-15; **修订日期:**2015-08-01

作者简介:王洁宁,男,研究员,研究领域:空管运行安全及空管系统仿真。

通信作者:王洁宁, E-mail: wang_jiening@aliyun.com。

管理,为此,国际民航组织在文献[4]中推荐采用安全管理系统(Safety management system, SMS)实施空管运行安全管理。SMS是一个完整的管理体系,它包括安全政策和目标、安全风险、安全保障及安全提升四个方面,其中风险管理作为SMS的基础和关键,在SMS体系建设中得到了广泛的重视^[5-6],事实上,风险这一概念所关心的内容与未来、可能性以及尚未发生的事情有关,因此采用模型化方法和规范化描述识别与分析风险是实施风险管理的先决条件。

文献[7]中指出:风险分析是系统地利用既有信息,识别出危险,并预测其对于人员、财产和环境的危险,其核心步骤为:危险识别、频度分析和后果分析。针对危险识别学者们提出数十种经典分析模型^[8],例如系统危险分析、故障树分析、失效模式及影响分析及危险与可操作性分析等。传统的危险识别与分析方法主要是以已有经验知识为基础,通过识别获得可能导致事故发生的潜在条件,以此为基础分析各种潜在条件状态转移,并给出相应的危险后果分析。危险有3个基本要素:危险元素,即构成危险的基本元素;触发机制,即引起危险发生的触发事件;对象和威胁,即易受到伤害和/或破坏的人或事物。危险是建立在危险识别与分析基础之上的评估,是对危险可能性和严重性的刻画,即 $\text{危险} = \text{可能性} \times \text{严重度}$ 。由此可以看出,经验知识在危险识别与分析中扮演着重要的作用,然而单一依靠“头脑风暴”的知识汇聚无法适应复杂系统的危险识别与分析需要,通过系统化知识建模的方法改进传统危险识别与分析模型,有效利用人工智能技术,形成面向危险识别与分析规范化信息传递、复用和共享,是解决危险识别与分析的有效途径之一。针对这种方法,国内外一些学者开展了一系列探索,Bosse等采用时态追踪语言(Temporal trace language, TTL)在微观层面,应用Agent思想对空管风险进行了分析^[9-10];荷兰宇航研究所建立了TOPAZ方法模型^[11],并从Agent的角度设计了一系列针对空管运行危险识别与分析模型^[12-13];Kuroake和Cameron等针对HAZOP和FMEA的传统方法,建立了面向危险识别与分析的领域本体,并给出了应用框架^[14-15];吴重光等从领域知识本体出发,建立了剧情对象模型SOM方法^[16]。

陆空通信是实施空中交通管制的重要手段,它通过地面管制与飞行航空器建立的陆空通信通道对航空器飞行进行管制调配。由于陆空通信在管

制工作的日常性和频繁性,管制员和飞行员之间的陆空通信差错或失效,包括相互之间的协调不畅、配合不当等都会影响到空中交通的顺畅、有序运行,甚至威胁到空中交通的安全运行。通常陆空通信是在通信设施支持下进行的陆空通话活动,管制员负责管制许可的发送和监听,飞行员负责管制许可的监听和复诵,通过闭环控制确保管制许可的无差错执行。从总体上讲,这类风险涉及到两个方面的问题,一是陆空通信设施失效,二是陆空通话活动偏差。

本文主要从民航陆空通信危险识别与分析问题入手,首先在总结HAZOP模型的基础之上,提出针对陆空通信危险识别与分析的系统参量和引导词,并应用BPMN和HAZOP模型识别与分析陆空通信危险偏差;其次,从知识表示框架的角度出发,提出陆空通信危险概念知识表示,即陆空通信发生危险主体、危险要素、危险致因因素、风险评估数值属性和危险要素顶层归结覆盖公理等概念类;第三,从描述逻辑的角度出发,建立概念之间的TBox描述逻辑关系和推理,并通过案例进行推理验证。采用本体方法,能够实现规范化、术语化危险描述和归类,避免了以往主要通过自然语言进行危险描述的缺点,为更有效地进行危险项后分析提供科学分类和统计依据。

1 基于HAZOP的陆空通信危险识别

1.1 HAZOP分析

HAZOP分析模型是一种结构化、系统化危险检查方法,主要针对具有过程化运行特征系统开展危险识别与评估,该方法广泛应用于化工领域。按照不同应用,HAZOP分析分为4种类型:面向过程的HAZOP分析、面向人因的HAZOP分析、面向程序的HAZOP分析和面向软件的HAZOP分析。HAZOP分析的实施以专家会议的方式进行,通过集合各位专家的智慧从多个方面分析系统可能出现的偏差,具体分析过程是通过将系统中节点的分割,形成针对特定过程节点的分析,如图1所示。该分析过程是一个不断迭代的过程。

HAZOP分析的关键是系统参量和引导词的概念元素的抽取,通过将一组系统参量与一组引导词进行关联比较形成对危险偏差的描述,即:引导词+系统参量=偏差。传统的HAZOP分析是建立在专家经验的基础之上,随着知识表示技术的发展,人们开始研究基于模型的HAZOP分析技术^[14],例如通过本体技术建立泛化的HAZOP节点分析概念模型来规范HAZOP分析知识表示。

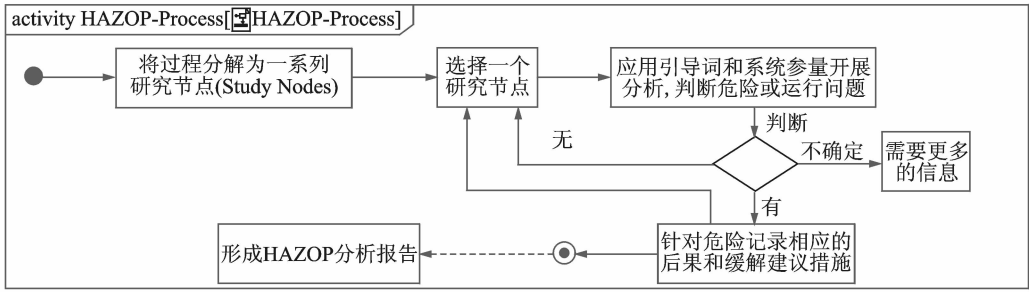


图 1 HAZOP 分析过程

Fig. 1 HAZOP analysis process

考虑到陆空通信的规范化过程特征, 本文主要采用面向过程的 HAZOP 分析方法, 通过建立严格的本体描述逻辑, 对其危险进行识别与分析。

1.2 陆空通信危险识别

国际民航组织针对陆空通信建立了一系列的规范, 本文依据陆空通信的规范化流程和 HAZOP 分析过程, 建立用于进行陆空通信危险识别的过程描述模型, 该模型采用标准的 BPMN 规范, 如图 2、3 所示。

陆空通信过程包括 3 个重要的节点: (1) 建立双向通信, (2) 对区域内航空器实施管制, 即发布管制指令管制运行航空器, (3) 航空器移交。图 2 中

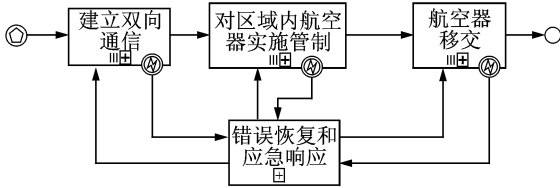


图 2 陆空通信过程 BPMN 流程图

Fig. 2 BPMN process diagram

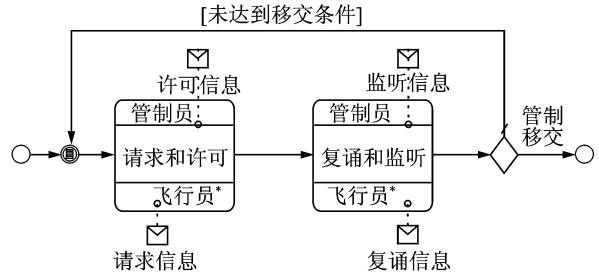


图 3 陆空通信信息交互 BPMN 编排图

Fig. 3 BPMN choreography diagram

的流程能够进一步分解, 图 3 给出了管制指挥情况下管制员与多个飞行员之间的信息交互流程。事实上, 依据 BPMN 对于节点的定义, 可以将分析节点分为两种类型: 一类是活动节点, 包括循环活动、顺序活动、并行活动等; 另外一类是网关节点, 包括选择网关、事件网关及并行网关等。在具体分析中可以依据节点语义的不同, 采用相应的引导词和系统参量进行偏差分析。本文按照陆空通信的特征, 设计了如表 1 所示的系统参量和引导词。

表 1 陆空通信系统参量和引导词表

Tab. 1 System parameters and guide words for air-ground communication

系统参量	引导词	偏差描述
通信移交 (Transfer of communication)	过早/过晚/忘记 (Too early/Late/Missing)	过早通信移交 (Too early transfer of communication)
通信 (Communication)	失去/非法/并发 (Prolonged Loss/Unlawful/Simultaneous)	失去通信 (Prolonged loss of communication)
话音接收质量 (Transmission reception quality)	衰减/阻塞/中断/弱 (Fading/Jammed/Broken/Weak)	话音接收阻塞 (Jammed transmission reception quality)
无线电通信失效 (Radio communication failure)	未探测/不恰当/质量差 (Not detect/Inadequate/Poor)	未探测双向通信失效 (Not detect radio communication failure two way)
监听/复诵 (readback/hearback)	忘记/忽略/不正确 (Missing/Omitted/Incorrect)	飞行员忘记复诵 (Pilot missing readback)
说话 (Speak)	过快/过慢/口音/语调 (Too fast/Too slow/Accent/Tone)	管制员说话过快 (Controller speak too fast)
频率 (Frequency)	不正确 (Incorrect)	扇区频率不正确 (Incorrect sector frequency)
信息 (Message)	混淆/混合/长指令 (Confusing/Mixed/Too long)	消息指令过长 (Message too long)
标准通话术语 (Standard phraseology)	未使用 (Not using)	未使用标准通话术语 (Not using standard phraseology)

系统参量和引导词都是对陆空通信过程中节点危险特性的刻画,它们代表了某个特定时间或条件下发生陆空通信危险的表象。由此,可以得到相应的陆空通信危险表象描述,这里称之为危险致因因素。例如,飞行员忘记复诵等,在第 2 节本体模型将详细给出。

2 基于本体的陆空通信风险识别与分析

2.1 风险识别与分析知识表示框架

风险是关于以下 3 个问题的综合答案。(1) 为什么会发生问题?(2) 发生问题的可能性有多大?(3) 后果是什么? 本文中的风险是指对引起问题发生事件及其影响和后果的综合度量,该度量包括 3 个方面:严重度评估、发生可能性评估及风险控制策略。风险识别与分析的结果就是辨识出潜在的危险致因因素,并从这些表象出发,归结到相应的风险因素,进一步对各风险因素进行综合度量。

本文从构建领域本体知识的角度出发,提出针对风险识别与评估的知识表示框架。本体通过构造概念集合及其关系来刻画领域内概念的含义,达到对领域知识的共同理解,本文所提出的领域本体以描述逻辑(Description logic, DL)为基础。设 V 为领域本体所采用的符号或词汇,可以定义一个模型 $\langle S, I \rangle$, 其中 $S = \langle D, R \rangle$ 为该领域中对象的概念化表示, D 表示领域中对象概念, R 表示对象概念之间的关系, $I: V \rightarrow D \times R$ 表示领域中本体概念的一个解释。DL 是一种知识表示语言,它包含一组基本符号,形成领域术语概念结构化和形式化描述,它采用概念和规则的基本操作符号将原子概念和原子关系通过一阶和二阶逻辑谓词构建新的概念和关系描述。DL 知识表示结构如图 4 所示, DL 知识表示包含 TBox(T) 和 ABox(A), 其中 TBox 是关于领域概念和关系公理集合, ABox 是关于概念实例的断言,即 TBox 中所包含概念和关系的实例集合,是描述具体实例的公理集合。本文采用 OWL-DL 符号。

TBox 针对衍生概念进行推理,包括概念的满足性、包含性、等价性及互斥性。ABox 推理则主要证明概念实例与 TBox 集合中概念的一致性(Consistent)。本文重点构造陆空通信风险识别与分析的 TBox 公理集合,通过危险识别与分析方法,如 HAZOP, 建立危险致因因素概念及危险主

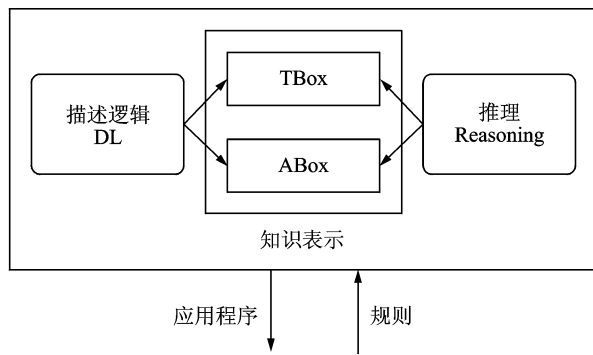


图 4 基于 DL 的知识表示框架

Fig. 4 Knowledge representation architecture based on DL

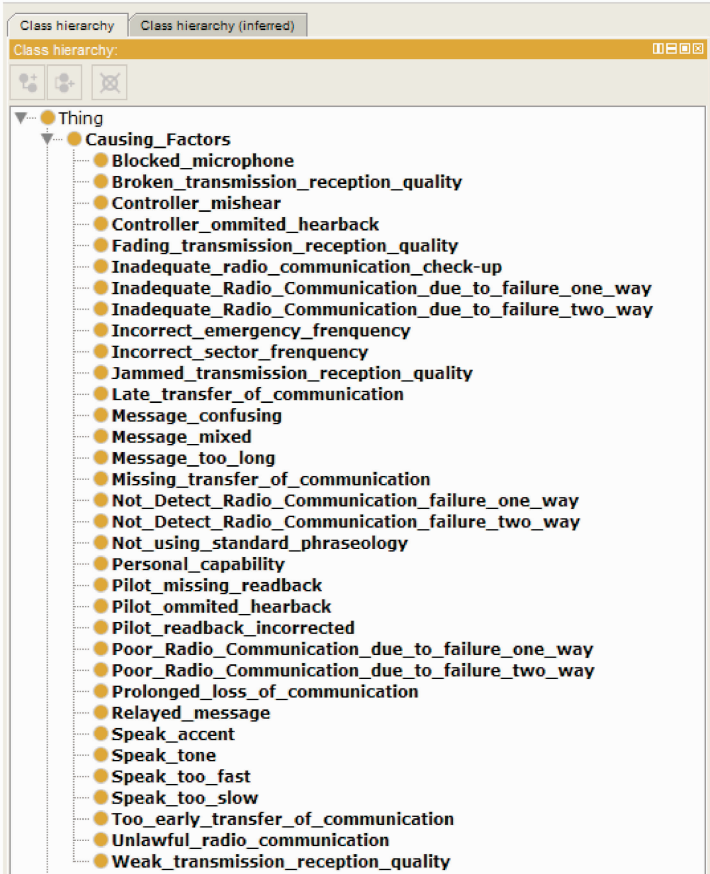
体概念集合,通过先验经验总结建立风险要素概念集合,包括风险概念术语及风险评估指标值等,采用 OWL-DL 建立概念集的描述逻辑关系,利用 TBox 公理推理形成针对特定危险致因因素概念(即表象)的风险要素,从而得到一致本体概念表示的风险及其评估。

2.2 陆空通信风险要素知识表示

如上所述,本文的目标是通过本体技术建立面向陆空通信的危险致因要素和风险要素之间的逻辑推理关系,这里所指风险要素是通过经验归结出的层次化风险项,包括风险的概念术语和相应的严重度和可能性评估。设 h_i 为一个危险致因, r_i 为一个风险要素,考察关系 $T \subseteq H \times R$, 其中 H 为一组危险致因因素集合,由上述 HAZOP 分析获得, R 为层次化的风险要素集合,即符合 TBox 的概念术语。定义关系 $T \in \mathcal{T}$, 且 $T = \langle T_h, T_r \rangle$, $T_h \in H, T_r \in R$, 则 $\langle T_h, T_r \rangle$ 表示危险致因要素与风险相关;如果有 $\forall T \in \mathcal{T}$ 且 $h_i \in T_h \Rightarrow r_i \in T_r$, 则 h_i 对 r_i 是必要的;如果有 $\exists T', T'' \in \mathcal{T}$ 并且 $h_i \in T'_h \wedge h_i \in T''_h \Rightarrow r_i \in T'_r \wedge r_i \notin T''_r$, 则 r_i 是危险致因子 h_i 的潜在风险。

经过 HAZOP 分析,本文形成了如图 5 的陆空通信危险致因因素概念集合,为了 Protégé 软件可视化和推理的需要,图中概念术语采用英语,与其相对应的部分汉语概念术语如图 5 右侧所示。

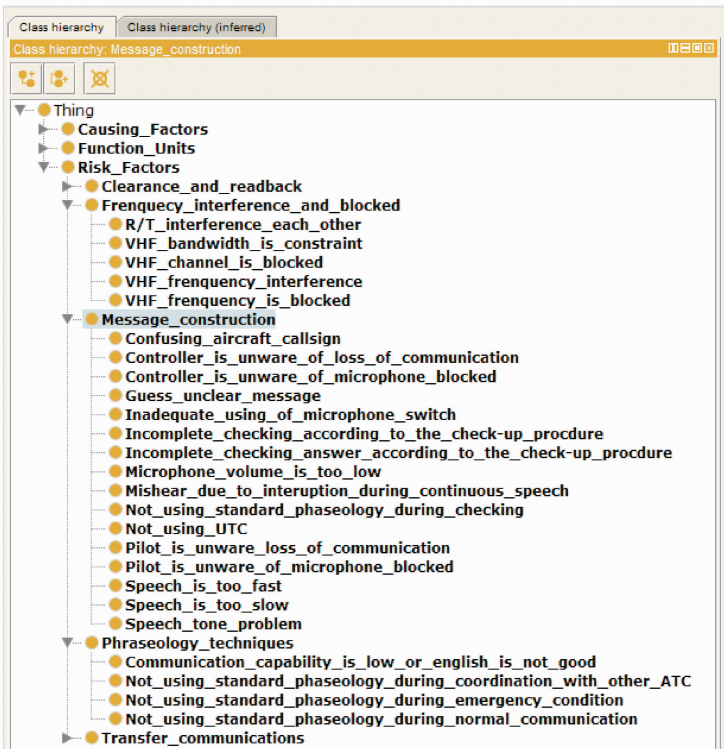
经过大量的调研和专家咨询,本文形成了如图 6 所示的陆空通信层次化风险要素概念术语集合,为了 Protégé 软件可视化和推理的需要,图中概念术语采用英语,与其相对应的部分汉语概念术语如图 6 右侧所示。



- 致因因素
- 话筒卡组
- 话音传输接收中断
- 管制员误听
- 管制员未正常监听
- 话音传输接收衰减
- 无线电检查不完整
- 由于单向通信失效导致无线电通信不完整
- 由于双向通信失效导致无线电通信不完整
- 应急频率不正确
- 扇区频率不正确
- 话音传输接收阻塞
- 通信移交过晚
- 信息混淆
- 信息混合
- 信息过长
- 忘记通信移交
- 未探测单向通信失效
- 未探测双向通信失效
- 未使用标准通话术语
- 人员能力
- 飞行员忘记复诵
- 飞行员忽略监听
- 飞行员复诵不正确
- 由于单向通信失效导致无线电通信质量差
- 由于双向通信失效导致无线电通信质量差
- 长时间丧失通信
- 中继信息
- 通话口音
- 通话语调
- 语速过快
- 语速过慢
- 过早通信移交
- 非法无线电通信
- 话音传输接收弱

图 5 陆空通信危险致因因素

Fig. 5 Hazard factors of air-ground communication



- 通话内容
- 混淆飞机呼号
- 管制员没有察觉到语音通信失效
- 管制员没有察觉到话筒卡组
- 主观猜测不清晰的通话内容
- 通话发送开关使用不当
- 无线电检查程序内容不完整
- 无线电检查回答内容不完整
- 话筒音量调节过低
- 连续通话被不当介入造成误听
- 无线电检查程序通话不规范
- 通话未采用世界协调时
- 飞行员没有察觉到语音通信失效
- 飞行员没有察觉到话筒卡组
- 通话语速过快
- 通话语速过慢
- 通话语调不正常

图 6 陆空通信层次化风险要素

Fig. 6 Risk factors of air-ground communication

至此,得到了关于陆空通信的危险致因因素概念集合和风险要素概念集合,另外一个需要考虑的问题是发生风险主体,同样需要建立相应的概念术语集合,本文针对陆空通信的特点,给出了 5 种风险发生的主体,分别是:管制员、飞行员、机载通信设备、地面通信设备和话筒。

2.3 陆空通信风险识别与分析领域本体构建

领域本体的构建需要遵循一定的准则,本文所提出的领域本体参考了 Gruber 提出了本体构造的 5 个准则^[17]:

明确性:本体应该有效地表达所定义术语的含义。定义应该是客观的,并独立于社会或计算场景。一致性:本体应该是一致的,也就是说,它应该支持与其定义相一致的推理。它所定义的公理以

及用自然语言进行说明的文档应该具有一致性。可扩展性:本体应该为可预知的任务提供概念基础。它应该可以支持在已有的概念基础上定义新的满足特殊需求的术语,而不需要修改已有的概念定义。最小编码的误区:概念的描述不应依赖于某一特殊的符号层的表示方法。最小的本体约定:本体约定应该最小,只要能够满足特定的知识共享需求即可,通过定义约束最弱的公理以及只定义必需的交互词汇就可以保证这点。

针对领域本体的构建,人们提出了诸如骨架法、七步法、SENSUS 法、METHONTOLOGY 法等多种方法。本文从概念抽象和概念间逻辑关系抽取角度出发,采用 UML 建立了如图 7 所示的概念化陆空通信风险本体框架。

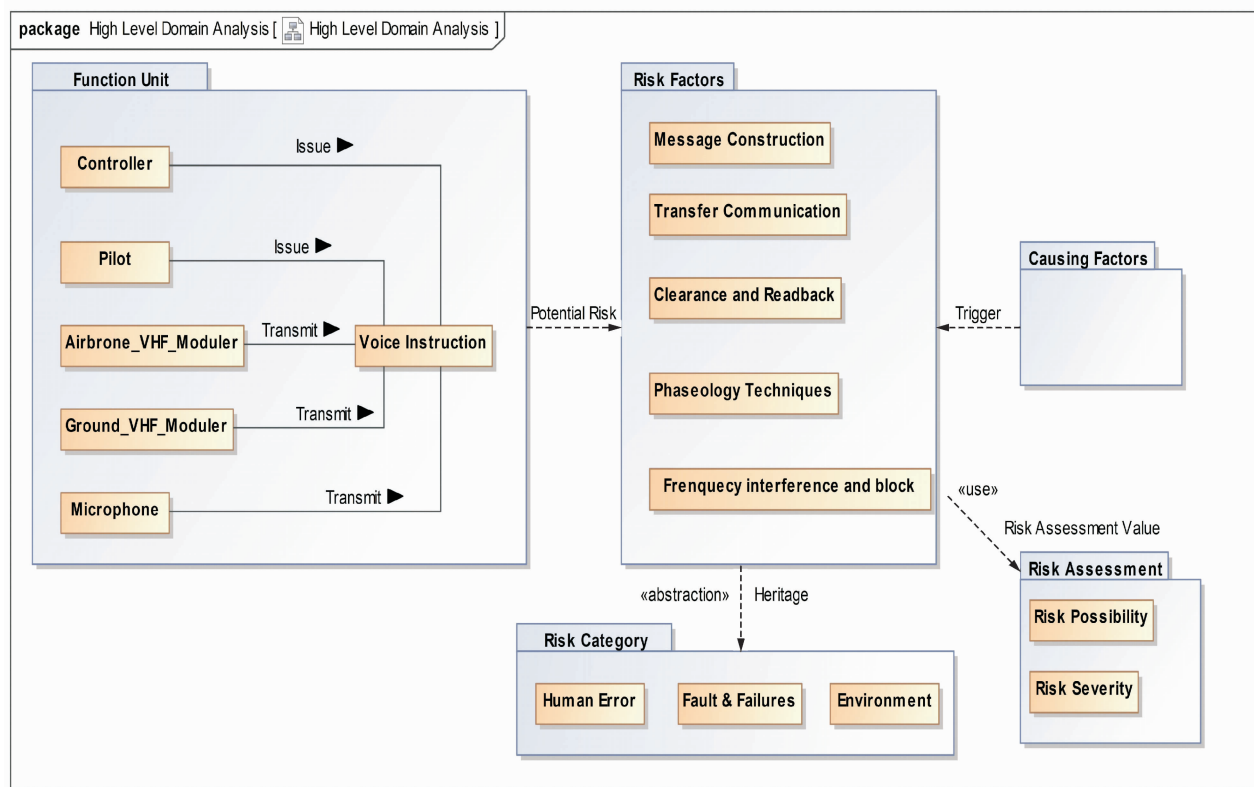


图 7 概念化陆空通信风险本体框架

Fig. 7 Conceptualized ontology framework of air-ground communication risk

由图 7 可知,陆空通信风险本体包含 5 类概念集合,分别是:发生风险主体概念类(Function_Unit)、风险要素类(Risk_Factors)、危险致因因素类(Causing_Factors)、风险评估数值属性(Risk_Assessment)和风险要素顶层归结覆盖公理(Risk_Category)。对于风险要素 TBox 而言,显然有:

$$T = \{ \exists \text{ hasFunctionUnit. Function_Units } \cap$$

$$\exists \text{ hasCausingFactor. Causing_Factors } \cap \geq 1 \text{ Causing_Factors } \cap \exists \text{ hasRiskpossibilityValue. RiskAssessment } \cap \exists \text{ hasRiskseverityValue. RiskAssessment } \}$$

TBox 概念集合定义需要符合 OWL-DL 的性质,包括互斥、存在量词、补集、数值约束、互逆关系,自反射和传递关系等,具体定义如表 2 所示,其

中 AL 代表 Attributive language。

表 2 OWL-DL 概念及关系构造符定义

Tab. 2 Constructor of OWL-DL concepts and roles

构造符含义	AL	构造语法
互斥 (disjunction)	U	$C \cup D$
存在量词 (qual. exist. res)	E	$\exists R. C$
补集 (negation)	C	彙緋 C
数值约束 (number restrictions)	N	$(\geq k. R)$ $(\leq k. R)$
数值约束 (qual. number restrictions)	Q	$(\geq kR. C)$ $(\leq kR. C)$
互逆关系 (inverse role)	I	R^{-}
关系覆盖 (role closure)	reg	R^*

本文 2.2 节已经建立了相应的概念集合,为了实施概念推理,需要针对陆空通信风险要素进行关系定义,即按照表 2 的语法定义相应风险要素的概念内涵。定义风险要素和危险致因之间的关系: $hasCausing$ 和 $isCausedby$, 并且 $hasCausing = isCausedby^{-}$; 定义风险要素和发生风险主体之间

的关系: $hasFunctionUnit$ 和 $isFunctionUnitof$, 同样 $hasFunctionUnit = isFunctionUnitof^{-}$; 定义风险要素的风险评估数值关系: $hasRiskPossibilityValue$ 和 $hasRiskSeverityValue$; 定义风险要素归结类的覆盖属性关系: $hasRiskCategory$, 这里归结类为枚举数据 $\{Human_Error, Fault\&Failures, Environment\}$ 。在以上分析的基础之上,本文采用 Protégé 软件构建了如图 8 所示的陆空通信风险识别与分析本体。

本文针对陆空通信风险要素逐条建立了本体逻辑描述,例如混淆飞机呼号定义为如下表达式:

$Confusing_aircraft_callsign \sqsubseteq Message_construction \sqsubseteq Risk_Factors$

$\forall Confusing_aircraft_callsign: (\exists hasCausing. Message_confusing \cup \exists hasCausing. Message_mixed) \cap \exists hasFunctionUnit. Controller \cap (\exists hasRiskSeverityValue \cap \exists hasRiskPossibilityValue)$

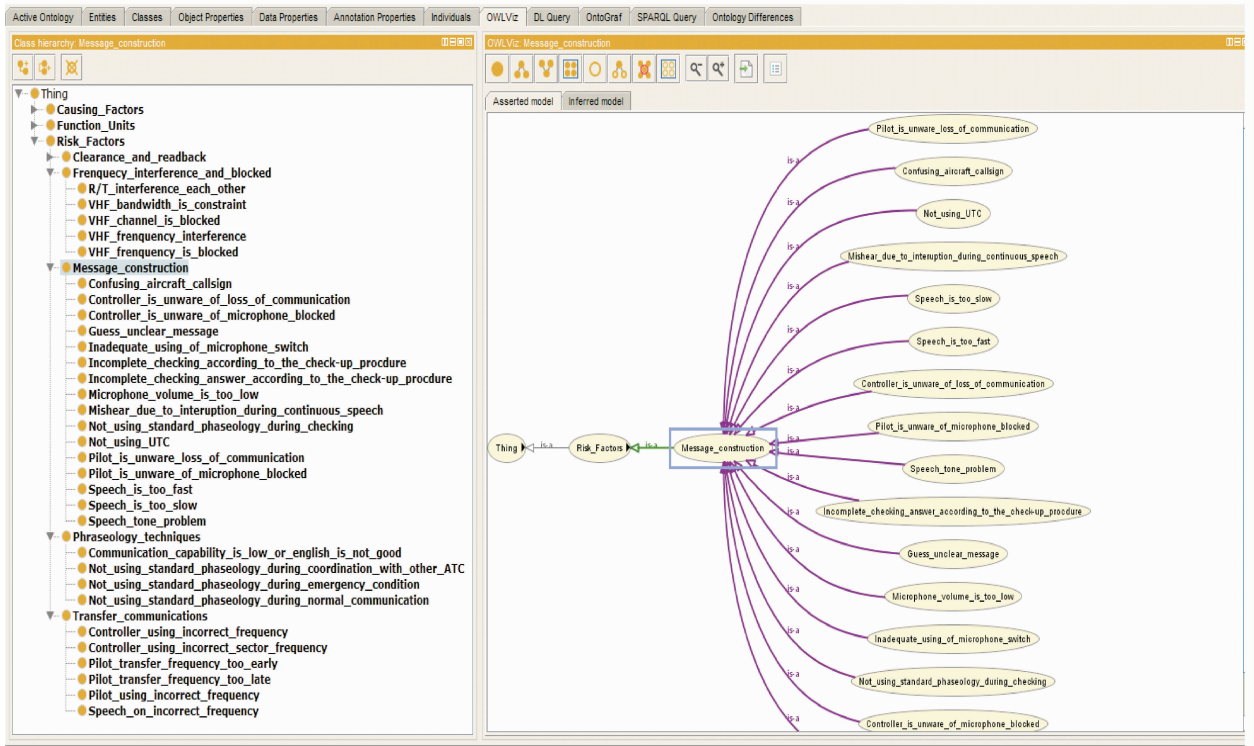


图 8 采用 Protégé 软件构建的陆空通信风险识别与分析本体

Fig. 8 Air-ground communication risk identification and analysis ontology using Protégé

2.4 陆空通信风险要素推理

本文所涉及的推理是针对 TBox 推理,按照 DL 知识模型的定义,如果一个解释 I 是本体 $O = \langle \mathcal{T}, \mathcal{A} \rangle$ 的模型, I 必须满足 \mathcal{T} 和 \mathcal{A} 的所有断言。TBox 推理包括以下几个方面:

概念满足性: 若概念 C 满足 \mathcal{T} , 必须存在一个

关于 T 的模型 I 使得 C^I 不为空, 本文在概念定义阶段已经保证了这个性质。

概念包含性: 若概念 C_1 关于 T 包含于概念 C_2 , 则对于每个关于 \mathcal{T} 的模型 I 有 $C_1^I \subseteq C_2^I$, 本文在概念定义阶段已经保证了这个性质。

概念互斥性: 若概念 C_1 关于 \mathcal{T} 与概念 C_2 互

斥,则对于每个关于 \mathcal{T} 的模型 I 有 $C_1^I \cap C_2^I = \emptyset$, 本文在概念定义阶段已经保证了这个性质。

概念等价性:若概念 C_1 关于 \mathcal{T} 等价于概念 C_2 , 则对于每个关于 \mathcal{T} 的模型 I 有 $C_1^I = C_2^I$, 这是本文需要通过推理获得的结果,即给出一个概念 C 的 DL 描述,能够通过推理得到其等价的风险要素集合,这样就可以有针对性地判断一组危险表象所涉及的风险条目。

本文采用了 Protégé 软件内嵌的开源推理引擎 FaCT++ 实施概念等价性推理,如前所述,其他推理属性在本体建模阶段已经得到了保证。

3 案例分析

3.1 案例描述

为了验证领域本体的有效性,本文选择了文献 [18] 中一个案例进行推理验证。事件描述如下:

达拉斯·福特·沃斯堡塔台准许飞机在跑道 35 左起。当飞机对准跑道中线时,飞行员接管了飞机的操控。飞行员注意到有一架 MU2 飞机从左向右滑行,因此说道:“注意 MU2。”飞行员相信 MU2 在滑行道 A 上。MU2 自西向东穿过了跑道 35 左。飞行员再次向塔台证实是否允许起飞。飞行员的确再次得到了证实。此时, MU2 已经穿越了跑道 35 左,飞机开始在跑道上滑跑(当然机长已经将看到的情况通知了塔台)。通过检查机组复读通话内容发现以下情况:该机组驾驶的是 B737-500。MU2 也在塔台的频率上。机组听到塔台发布指令特别快速,飞行员把那种现象称之为“快得像拍卖师(说话)”。飞行员认为,管制员说话必须速度适当,让运行中的驾驶员能够听清楚才对,否则得有人告诉管制员。飞行员把 MU2 没有在跑道 35 左停止等待归结为管制员说话速度太快。

从陆空通信的角度分析该案例,按照 1.2 节的

分析可知主要存在以下问题:管制员语速过快、没有迹象表明两架飞机对滑行许可指令进行的复诵,即飞行员忘记了复诵。

3.2 案例推理

根据以上分析,该显然有:

\exists hasCausing. Speak_too_fast, \exists hasCausing. Pilot_missing_readback, 其中: $\text{Speak_too_fast} \sqsubseteq \text{Causing_Factors}$, $\text{Pilot_missing_readback} \sqsubseteq \text{Causing_Factors}$ 。

按照上述分析在 Protégé 软件中给出了如图 9 所示案例逻辑描述,通过 FaCT++ 推理得到了该案例所涉及的风险要素,分别是:通话语速过快、管制员没有意识到缺乏复诵或复诵错误,具体如图 10,11 所示。

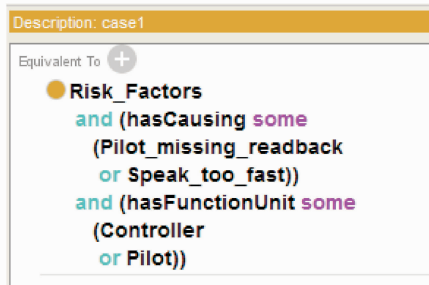


图 9 案例 OWL-DL 描述

Fig. 9 OWL-DL of study case

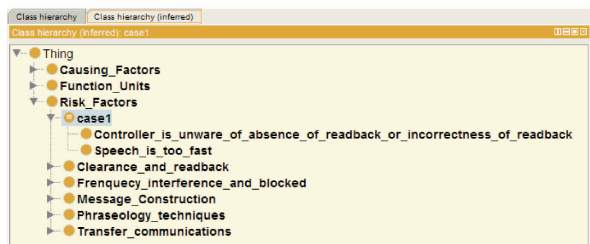


图 10 FaCT++ 推理结果

Fig. 10 Reasoning result by FaCT++

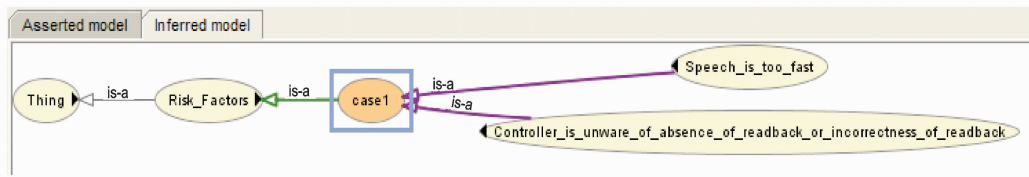


图 11 FaCT++ 推理结果 OwlViz 图形化关系

Fig. 11 OwlViz graph of reasoning result by FaCT++

4 结束语

为实现规范化、术语化风险识别、分析与描述,本文提出了一种基于描述逻辑 TBox 推理的陆空

通信风险识别与分析方法。首先通过 BPMN 和 HAZOP 分析获得危险偏差,然后建立风险分析领域本体,在本体推理的支持之下辨识危险偏差与风险要素的内关联关系,克服了单纯采用自然语言

进行风险识别与分析的缺点,为更有效地进行风险项后分析提供科学分类和统计依据。本文后续工作将进一步研究拓展 ABox 推理和本体查询推理。

参考文献:

- [1] Shorrock S T, Kirwan R. Development and application of a human error identification tool for air traffic control[J]. *Applied Ergonomics*, 2002, 33(4): 319-336.
- [2] 胡明华. 我国空管安全管理体系实然性研究[J]. *南京航空航天大学学报:社会科学版*, 2007, 9(1): 43-36.
Hu Minghua. An empirical study of China's ATC safety management system[J]. *Journal of Nanjing University of Aeronautics & Astronautics: Social Sciences*, 2007, 9(1): 43-36.
- [3] 施和平. 空管系统安全管理——基于资源、机制、效用模式的理论和实践[M]. 北京: 中国民航出版社, 2015.
Shi Heping. *ATM Systemic Safety Management* [M]. Beijing: Civil Aviation of China Press, 2015.
- [4] ICAO. ICAO 7970—2002[S]. ICAO ANNEX 19. Canada: ICAO, 2002.
- [5] ICAO. Doc 9859[S]. Canada: ICAO, 2009.
- [6] 罗帆, 刘小平, 杨智. 基于系统动力学的空管安全风险情景预警决策模型仿真[J]. *系统工程*, 2014, 32(1): 139-145.
Luo Fan, Liu Xiaoping, Yang zhi. Pre-warning decision-making model simulation of air traffic control safety risk based on system dynamics[J]. *Systems Engineering*, 2014, 32(1): 139-145.
- [7] International Electrotechnical Commission. CEI/IEC 300-3-9[S]. Geneva: ICE, 1995.
- [8] Ericson C A. 危险分析技术[M]. 赵廷弟, 焦健, 赵远, 等译. 北京: 国防工业出版社, 2012.
Ericson C A. *Hazard analysis techniques for system safety* [M]. Zhao Tingdi, Zhao Jian, Zhao Yuan, et al. Trans. Beijing: National Defense Industry Press, 2012.
- [9] Bosse T, Hoogendoorn M, Klein M C A, et al. Modelling collective decision making in groups and crowds: Integrating social contagion and interacting emotions, beliefs and intentions[J]. *Autonomous Agent Multi-Agent Systems*, 2013, 27(1): 52-84.
- [10] Bosse T, Mogles N M. Formal analysis of aviation incidents[C]//25th International Conference on Industrial Engineering and Other Applications of Applied Intelligent Systems. Dalian, China: Springer Verlag Berlin Heidelberg, 2012: 371-380.
- [11] Geisinger K. Guide to Methods & Tools for Safety Analysis in Air Traffic Management[EB/OL]. http://flightsafety.org/files/methods_tools_safety_analysis.pdf, 2003.
- [12] Stroeve S H, Blom H A P, van der Park M N J. Multi-agent situation awareness error evolution in accident risk modeling[C]//5th USA/Europe Air Traffic Management R&D Seminar. Budapest, Hungary: [s. n.], 2003.
- [13] Blom H A P, Stroeve S H, Bosse T. Modelling of potential hazards in agent-based safety risk analysis [C]//10th USA/Europe Air Traffic Management Research and Development Seminar. Chicago, USA: [s. n.], 2013.
- [14] Kuraoka K, Batres R. An ontological approach to represent HAZOP information[R]. Technical Report TR-2003-01, 2003.
- [15] Cameron I T, Seligmann B, Hangos K M, et al. A functional systems approach to the development of improved hazard identification for advanced diagnostic systems[C]//18th European Symposium on Computer Aided Process Engineering. Lyon, France: [s. n.], 2008.
- [16] 吴重光, 许欣, 纳永良, 等. 基于知识本体的过程安全分析信息化标准[J]. *化工学报*, 2012, 63(5): 1484-1491.
Wu Chongguang, Xu Xin, Na Yongling, et al. Standardized information for process hazard analysis based on ontology[J]. *CIESC Journal*, 2012, 63(5): 1484-1491.
- [17] Gruber T R. A translation approach to portable ontology specifications [J]. *Knowledge Acquisition*, 1993, 5(2): 199-220.
- [18] 比尔·克拉克. 跑道侵入[M]. 赵洪元 译. 北京: 中国民航出版社, 2005.
Clarke B. *Runway incursions* [M]. Zhao Hongyuan Trans. Beijing: Civil Aviation of China Press, 2005.