MBSE在核工程设计中的应用

蒋立国[1*],宋春景[1],李响[2]

1. 上海核工程研究设计院有限公司,上海 200233
2. 上海图阅智能科技有限公司,上海 200240

摘要 通过阐述目前核工程设计面临的问题和困难以及核电工程的复杂性与安全性,探究了一种面向未来的设计模式和方法——基于模型的系统工程(MBSE)。调研了国外核电研发企业对MBSE的实践和应用情况。针对核电项目非能动安全系统进行了MBSE实施流程的案例试点,探索了MBSE方法在核电研发设计中的指导作用,进而摸索了核电工程研发设计模式的创新,为数字化转型提供了一种可行的解决方案。

关键词 基于模型的系统工程;核工程;数字化

当前,国内的核电设计单位大部分采用的是基于文档的设计模式,这种设计模式会在大量设计文件、图纸、报告中体现与核电系统相关的信息,例如系统说明书、计算分析报告、布置图、设备详图等。但随着核电系统规模和复杂程度的急剧增加,以及未来核电对安全性、经济性和小型化、非能动、无人干预等需求的不断提升,基于文档的设计模式面临的困难越来越多,而且这些困难还会延伸至核电设备的采购、制造,核电设施的运行、维护、退役等整个生命周期过程。因此,亟需通过引入新的理念和思维,革新当前工程的设计模式。

1 核工程设计需求分析

1.1 当前面临的问题和困难

核电工程设计是一项多学科、多专业相结合的大型复杂系统,具有技术难度大、投入资金多、安全与可靠性要求高、协作部门单位众多、研发风险高和管理难度大等诸多特点。而当前设计过程普遍存在重设计分析、轻需求分析、专业协调差、综合集成能力低等现象,比较典型的问题主要有以下几个方面。

1)难以保证设计信息的完整性和一致性,且难于评估和确定数据信息间的关系。基于文档的信息可用性很差,变更影响分析不够彻底,设计问题频出,从而导致设计质量和效率低下。专业间、设计人员间和不同单位间的沟通不顺畅,从业人员对同一信息的理解程度不同,容易造成信息歧义,甚至错误。

2)核电站组成系统复杂,其系统运行场景很多且逻辑关系复杂。系统运行场景相关的功能活动是动态交互的,仅通过相对简单的文字描述和图表示意,很难完整表述系统的真实运行情景。功能活动还会涉及多

收稿日期:2018-12-01;修回日期:2019-02-25

作者简介:蒋立国(通信作者),工程师,系统设计与工艺布置,电子信箱:jiangliguo@snerdi.com.cn;李响,博士,研究方向为新一代系统建模环境、MBSE、智能设计等,电子信箱:xiang.lee@sysgraph.cn

引用格式:蒋立国, 宋春景, 李响. MBSE在核工程设计中的应用[J]. 科技导报, 2019, 37(7): 62-67; doi: 10.3981/j.issn.1000-7857.2019.07.009

个子系统、设备、信号的动作响应,逻辑关系很复杂,而且设备和信号的运行次序与核电的安全性也紧密相关。

3)核电工程的需求多、要求高,针对设计需求、设计约束的梳理不够清晰,而且基于文档的模式难以建立需求与功能、功能与系统部件之间的可追溯关系,导致工程设计演进过程中,专业间常常顾此失彼。此外,核电安全性方面的需求越来越高,来自核安全监管当局、社会民众的监督和检查越来越多。

4)核电工程的设计、采购、制造、建造、运维等阶段涉及的部门、单位众多,配合关系复杂,在实施过程中的各个阶段、各个部门单位之间存在大量动态的内部和外部接口[1]。这些接口往往潜伏着职责矛盾、利益冲突、变更风险,如果关系不清或处理不当,很可能就会出现责任推诿、冲突激化、风险失控,进而影响核电工程建设目标的实现。

1.2　核电领域工程设计的复杂性

核电工程作为一种复杂系统,存在着结构复杂性、功能复杂性和行为复杂性[2],这些复杂性与核安全有着密切关系,同时也是未来复杂系统设计与分析的主要挑战,这些复杂性主要体现在4个方面。

1)交互的复杂性,即系统部件交互作用的复杂性。核电作为一种交互性复杂系统,核事故通常是由系统部件之间的交互失效所引发的,而这些部件交互失效通常又是由设计缺陷所导致的。设计缺陷的产生通常又是因为需求定义错误或对需求理解偏差造成的。设计缺陷在部件层面主要有部件失效和部件交互事故,这两方面分别对应了系统的安全性和可靠性。

2)非线性的复杂性,即部件功能与系统性能的非线性。复杂系统的非线性通常会造成系统行为很难预测,行为预测不完整不但会对设计阶段有影响,更会对运行阶段造成影响。非线性因果关系在事故中亦可称为“系统性因素”,即系统特征或其环境会直接影响所有或大部分系统部件。AP1000的非能动理念和事故后72 h无人干预也是核电系统设计中对非线性事故处理的一种方法或模式。

3)动态的复杂性,即系统运行随时间变化的动态复杂性。虽然在设计时会假设核电系统满功率运行是稳态的,但在运行核电系统即便是满功率也不会是稳态的;因为随着部件动作、组织及人员行为的变化等,系统响应行为也处于不间断的动态变化中。针对核电系统及其运行环境灵活性的需求,需要在工程设计和运行管理技术中避免或控制不安全的动态变化,并在运行过程中持续监测这些变化。

4)构造分解的复杂性,即系统构造、分解结构的复杂性。当系统的分解结构与功能分解不一致时,就会出现构造分解的复杂性。这种复杂性会让设计人员和运维人员很难预测和理解系统的响应行为。核电安全性与系统及其部件功能行为有关,但安全性并非系统结构或架构的功能。构造分解的复杂性会让设计人员对于理解和排查设计缺陷变得越来越困难,也会大大增加核查核电系统设计和确认系统是否安全运行的难度。

2　MBSE内涵及国外核电设计中的应用实践

2.1　MBSE内涵认知

为了应对这些困难和挑战,国际系统工程协会(INCOSE)在21世纪初倡议并推广“基于模型的系统工程(MBSE)”设计理念,MBSE主张以结构化系统模型支持设计,并持续贯穿到系统的整个生命周期过程[3]。MBSE通过模型来更加规范地应用系统工程,并增强了获取、分析、共享和管理与系统相关信息的能力,其好处有以下5个方面。

1)增强开发利益攸关者之间的沟通能力。MBSE中系统信息是通过图形化的系统模型表达的,系统模型可以准确统一完整定义系统的各个方面,如需求、功能、详细设计、规范约束、运行场景和次序等,相对于大量的技术设计分析文档而言,更容易让设计人员对系统内部的各个细节形成统一且无歧义的理解,由此设计人员间的沟通会更加顺畅和高效。

2)提供多个维度检验系统模型并提升管理复杂系统的能力及分析变更影响。系统模型的构建是涵盖系统全生命周期过程,包括系统的需求、功能、设计、分析、验证和确认等活动,可以提供一个完整的、全面的、一致的并可追溯的系统信息,确保系统设计分析的一体化,变更影响分析更加准确高效,从而降低风险、缩减成本及进度等。

3)通过更加标准化的信息获取方式增强设计分析过程中各种信息的捕获、传递和转化。系统设计是将确立系统需求并将其分配至各个组成部分的过程。在这个过程中,包含着诸多信息的传递和转换过程。利用系统模型模块化的特点,让这些信息的获取、转换和

重用更加便捷和高效。

4）通过提供无歧义且精确、可评估且一致、可分析且完整的系统模型提升系统的设计质量。通过建立面向对象的一系列系统模型（包括需求模型、功能模型、行为模型、接口模型、质量模型、布置模型、时序模型、仿真模型等），让参与设计、制造、建造、调试、运行、维护、退役等各个阶段的人员更加详尽地理解系统，尽量在更早的阶段将问题暴露出来，从而提升质量、降低进度和成本风险等。

5）利用模型驱动方法的固有抽象机制，增强知识管理和信息重用。设计经验、现场反馈、制造约束等抽象化的隐性知识可以通过系统模型的方式存储在组织知识库中，并通过智能推送、主动干预的方式及时有效地优化设计方案，从而实现知识管理和信息重用的目的。

MBSE本质上还是系统工程，其需求定义、功能分解、逻辑架构、详细设计、综合集成、验证确认的整体思路并没有发生任何变化。但MBSE采用了一种崭新的手段来更好地实践系统工程，即在专门的系统工程建模工具上，构建图形化的系统模型表征系统需求、系统功能、系统架构、系统行为等。

2.2 国外核电系统研发中对MBSE的应用

1）西屋电气公司自动化和现场服务事业部在2007年基于Microsoft Visio开发了系统建模工具（图1）——基于模型的模块化应用功能（MAF），并将其用于核电仪控系统设计[4]。西屋在开发时选择将微软的Visio作为工具平台，为AP1000仪控系统设计建立了一致的、可重复的且高效的流程。通过平台开展仪控系统的功能设计、系统设计和子系统需求定义等工作。平台的模块化体现在架构元素的功能分配上，如将包含硬件I/O的功能模块赋予控制元素，将报警功能模块赋给其相应的架构元素等。

2）法国Areva公司近期也正在调查研究一种基于模型的方法，并将应用于与其他合作伙伴共同开展核电项目的工作分解结构[5]。能够解决的问题包括管理具有各自流程和方法的多个工业合作伙伴间的协作和为项目生成工作分解结构和工作包描述。模型带来的好处主要有：（1）融合一套通用流程，并与相关标准文档如规范书、说明书、设计和验证等一起应用；（2）通过产品分解结构快速生成工作分解结构，并作为成本分析和策划的基础；（3）为项目计划提供客观且中性的支持，实现更加高效的协作。

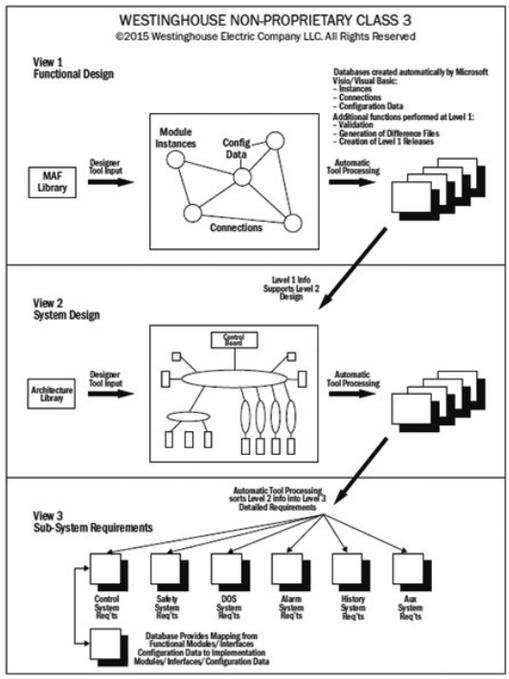

图1 MAF流程

Fig. 1 MAF process

3 未来设计模式之MBSE方法实践

3.1 MBSE实践流程

MBSE方法可贯穿系统需求定义、研发设计、综合、验证、运行及最终退役的整个系统生命周期，通过模型来串接表征系统的数据和关系，并识别和缓解所有重大风险。系统模型是通过各种不同视角的视图（图2[3]），展现系统内部各种层级的关系，这些视图分别对应了设计过程的需求分析、功能分析、逻辑架构和物理实现，并通过相互依赖、反复迭代和逐次递归的设计活动，实现系统信息的完整链条。

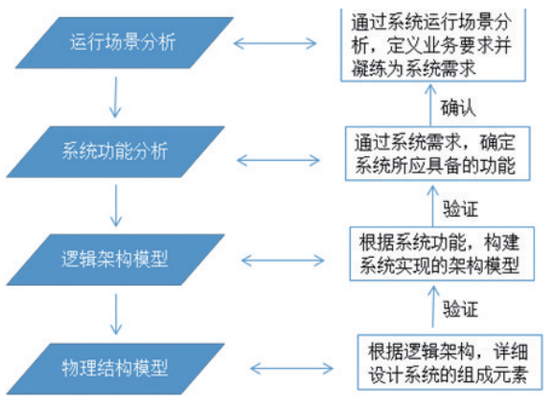

图2 不同视角的系统模型

Fig. 2 System model from different viewpoints

以CAP1400核电厂非能动堆芯冷却系统(PXS)的设计分析为例,利用SysGraph系统建模软件,建立符合SysML语言标准[6]的系统模型。在反应堆发生假想事故时,核电厂能够缓解可能威胁公众健康和安全的后果。那么安全系统的功能需求就是在假想事故场景下,PXS具备自动提供充足含硼补给水以保证堆芯淹没并带走衰变热的能力。在MBSE方法中,将核安全法规中相应的顶层安全需求转化为系统级的功能需求(图3),将系统功能的实现方式、实现手段和期望结果汇集起来归为该系统的"运行场景"。

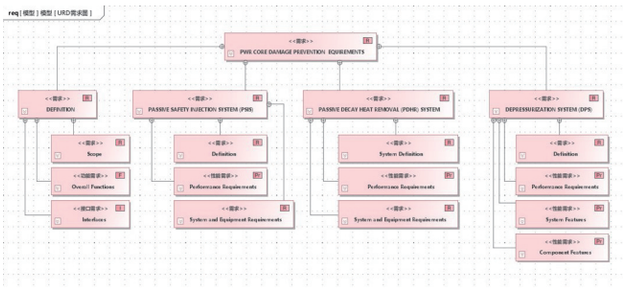

图3　系统功能需求图

Fig. 3　System functional requirement diagram

系统功能分析是将系统功能进一步细化,形成系统各场景的行为模型。PXS所执行的安全有关功能主要有反应堆冷却剂系统应急补给和硼化、安全注射、应急堆芯衰变热排出、事故后安全壳pH值控制等。按照功能执行的重要程度,以及功能执行期间、功能转换之间的状态关系,利用活动图和状态机图来展现系统的功能模型框架,并理顺系统功能执行的时序要素、状态衔接顺序的限制因素等。

根据系统功能分析模型,构建系统的逻辑架构模型(图4)。逻辑架构模型是系统实现的逻辑结构,主要

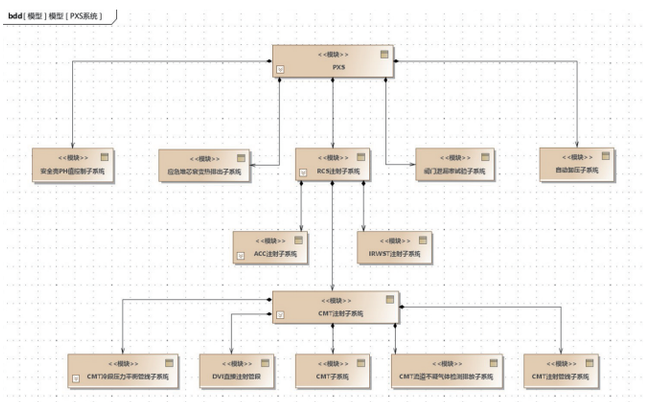

图4　系统结构组成

Fig. 4　System structure composite diagram

是表述系统实现其所有功能和状态所需的子系统,以及各个子系统之间的关系。对于具有特定功能的系统,其实现方案可能有很多种。通过综合考虑成本、性能、风险、安全性、可靠性等诸多因素,对这些设计方案进行权衡分析,确定最终能够满足系统功能的最优方案。逻辑架构是将"黑盒"逐步转变为"白盒"的建模过程,是把系统功能分配给子系统,并最终选定组成元素的架构过程。利用模块定义图和内部模块图展现PXS内各子系统、部件架构信息和关系以及与其他使能系统之间的关系(图5)。

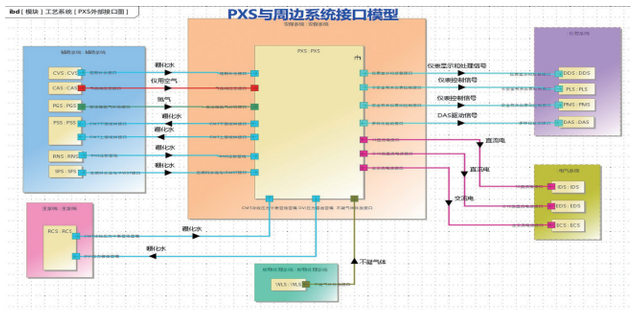

图5　系统接口示意

Fig. 5　System interface diagram

物理结构模型是将逻辑架构模型具体化的过程,是通过三维模型完整表征系统元素的设计,并体现零部件之间连接关系信息[7]。未来的物理结构模型将通过基于模型的定义(MBD)技术来完整表征产品定义信息,如系统元素的尺寸标注、公差信息、粗糙度要求、重量重心信息、加工制造要求、材料信息等。规范化的三维定义信息可生成部件加工制造数据集和部件检验数据集,方便后续阶段的加工制造和产品检验。

需要注意的是,系统模型中各层级都应建立与之相对应的场景分析、功能分析、逻辑架构和物理结构。如图6[3]所示,各层级设计是一种反复迭代和渐进递归的演进过程。

本次试点充分利用MBSE方法,结合核电工艺系统实际,将所有与系统相关的信息,如顶层需求、功能分解、系统说明、设备规范以及标准法规等都通过系统模型融合到一个集成的整体设计环境中,将系统需求、系统功能、系统架构、系统实现等各层级的信息通过系统模型这一中心枢纽关联起来,从而有效解决传统设计模式下人工接口多、复核校正难和变更影响难以保证的问题。同时,通过系统模型建立了基于多层级架构关联设计的并行机制,将上下游专业设计对象之间、专

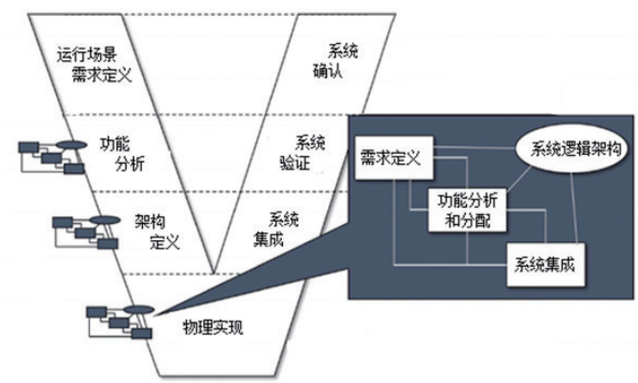

图6 反复迭代和渐进递归的设计演进过程

Fig. 6 Design evolution process of iteration and recursion

业内部设计对象之间的关联关系显性化,进而加快了设计分析迭代周期,提高了设计分析效率和质量。

3.2 MBSE应用的挑战

一个规模合理、目的明确的MBSE试点实践,即便项目再小,也能清晰显示MBSE的技术价值。但MBSE不是一种灵丹妙药,不能短时间提升组织的整体能力,但在领导力和专业人员的共同参与下,如果将MBSE作为一项持久战略决策,在不久的未来就会给企业带来切切实实的竞争优势,且企业所生成的产品或系统将会更能符合未来需求。

1)技术挑战。

目前主流的MBSE建模工具主要有No Magic公司的MagicDraw,IBM公司的Rational Rhapsody,但这些软件都是基于软件工程,通过增加SysML系统建模语言形成的专用系统建模工具。中国对MBSE建模工具的开发氛围和资助力度还不强烈,国内实践试点大多采用国外成熟产品,这将会导致国内自研工具难以得到认可,生存和发展的道路愈发狭窄。

当前国际上提出了很多MBSE方法,主要有INCOSE面向对象的系统工程方法(OOSEM)、IBM Rational Telelogic Harmony-SE、Vitech MBSE方法、JPL状态分析等[8]。中国对系统建模方法的研究力度很有限,为数不多的MBSE试点实践项目也是参照这些已有的国外成果。对MBSE方法论的认识不足,且缺乏体系性,会阻碍中国工程实践人员的认知和实践。

对于这些工具和方法的引进,在实际操作实践中,很难让每名参与人员对于这些工具和方法的理解都能达到完美或一致,所以更重要地是要培养系统工程的本质思维和基于模型的根本理念。此外,MBSE方法是跨学科跨领域的综合运用,系统工程师不但要掌握系统工程、MBSE核心理念以及建模语言,还要非常熟悉所关注系统的专业知识,综合能力要求很高。

2)机制挑战。

MBSE十分强调模型的重用和共享,模型可作为一种知识资源进行储备,随着模型资源的丰富和拓展,会为行业发展带来不可估量的价值。目前核电行业还未系统地形成模型库,缺乏权威组织机构领导模型库构建工作的实施。此外,系统模型与设计软件、分析工具之间的接口和转换技术标准还未统一,行业内资源共享的氛围十分不足,还未建立对模型知识成果的保护措施,因此模型重用和共享会受到很大的阻碍。

目前对MBSE方法的认知理解还不充分,对未来数字电厂设计模式的场景还不清晰,对MBSE方法实践的投入和人才培养方面还有诸多不足,这需要行业内特别是组织决策层对MBSE方法研究和实践提供必要的支持和鼓励,也应在组织内培养系统模型应用的价值文化,这会对MBSE方法的落地起到十分重要的推动作用。

4 结论

MBSE方法为数字化提供了一种崭新的视角,同时也是未来应对复杂系统设计和管理公认的解决方案。MBSE方法的运用,会对现有核电型号研发流程、设计模式造成很大冲击,从而给项目管理、技术管理、风险决策等带来根本变革。有必要结合自身的研发特点和未来发展需求,制定出长远发展规划。在吸收消化国外研究的同时,积极探索并形成特有的核电行业MBSE,进而提升核电产业整体数字化能力。

参考文献(References)

[1] 程平东, 孙汉虹. 核电工程项目管理[M]. 北京: 中国电力出版社,2006: 11-13.
Cheng Pingdong, Sun Hanhong. Nuclear power project management[M]. Beijing: China Electric Power Press, 2006: 11-13.

[2] Leveson N G. Complexity and safety[C]//Complex Systems Design & Management: Proceeding of the Second International Conference on Complex Systems Design & Management CSDM 2011. Berlin Heidelberg, NJ: Spinger, 2011: 27-38.

[3] Walden D D, Roedler G J, Forsberg K J, et al. Systems engineering handbook: A guide for system life cycle process and ac-

tivities[M]. 4th ed. San Diego, CA: John Wiley & Sons, Inc, 2015: 189-200.

[4] McWilliams G B. Modular applications functions: A westinghouse MBSE tool[J]. Insight, 2015, 18(2): 26-28.

[5] Marie C, Beuzelin G, Boutin S, et al. Fast and extensive model based project plan building in nuclear industry[C]//Complex Systems Design & Management: Proceeding of the Second International Conference on Complex Systems Design & Management CSD&M. Paris: Spinger, 2016: 245-246.

[6] Friedenthal S, Moore A, Steiner R. A parctical guide to SysML: The systems modeling language[M]. 3rd ed. New York: Morgan Kaufmann Publisher, Inc, 2014: 87-99.

[7] 程五四, 陈帝江, 张红旗. MBD技术标准化及应用研究[J]. CAD/CAM与制造业信息化, 2013, 9: 14-16.
Cheng Wusi, Chen Dijiang, Zhang Hongqi. MBD technology standardization and application research[J]. Digital Manufacturing Industry, 2013, 9: 14-16.

[8] Estefan J A. Survey of model-based systems engineering (MBSE) methodologies[R]. NASA Jet Propulsion Laboratory, 2008: 15-20. http://www.omgsysml.org/MBSE_Methodology_Survey_RevB.pdf.

On application of MBSE in nuclear engineering design

JIANG Liguo[1*], SONG Chunjing[1], LI Xiang[2]

1. Shanghai Nuclear Engineering Research & Design Institute Co., Ltd., Shanghai 200233, China
2. Shanghai SysGraph Lab Technology Co., Ltd., Shanghai 200240, China

Abstract This article explains the connotation and value of MBSE, and investigates the practice and application of MBSE by foreign nuclear power R&D enterprises. A case study of the MBSE implementation process for the passive safety system of nuclear power project is conducted, with the main contents including application of requirements analysis, functional analysis, and architecture definition in passive safety system design. The system model is used to express system requirements, structure, parameters, and behavioral information to achieve traceability and verification of various information in the system design process, improve design efficiency, and reduce design risk. The article also explores the guiding role of the MBSE method in nuclear power R&D and design, and then the innovation of nuclear power engineering R&D design mode to provide a feasible solution for digital transformation. According to the practice and understanding of MBSE, challenges faced by MBSE involving technology, culture, thinking and management are discussed in order to provide a reference for further application of MBSE concept in nuclear power design.

Keywords MBSE; nuclear design; digital design

（责任编辑　祝叶华）