基于 AADL 的信息物理融合系统架构级特定风险建模与分析

肖明睿[1]，董云卫[1]，苟倩文[1]，薛峰[2]，陈永华[2]
[1]西北工业大学计算机学院，中国西安市，710072
[2]南瑞集团有限公司（国网电力科学研究院有限公司），中国南京市，210000

摘要：信息物理融合系统在安全攸关领域的重要性日益增强。为了在研发早期确保系统的可信属性，特定风险分析扮演了安全性评估工作中的重要角色。人为因素和物理环境是特定风险评估中最为重要的组成部分。因此，有必要综合考虑人和物理环境的行为特征进行安全性分析。为提高架构分析与设计语言（AADL）的建模能力，提出一种新的特定风险模型，同时提出一种基于架构的特定风险分析方法支持信息物理融合系统模型层面的安全性评估。为实现特定风险模型的定量分析，提出从特定风险模型到确定性随机Petri网模型的转换方法。以电力系统中的安全稳定控制系统为例，采用所提方法进行架构模型建模和特定风险分析。

关键词：人-信息-物理融合系统；特定风险分析；架构分析与设计语言；确定性随机Petri网；特定风险模型
https://doi.org/10.1631/FITEE.2000428