doi:10.1631/FITEE.1800636

题目：针对无人机系统安全的新型层级式软件架构

概要：提出一种覆盖底层源代码到上层用户任务代码的新型层级式软件架构，用于提高无人机系统安全性与可靠性。每个软件模块采用形式化验证方法，验证其源代码是否符合设计规范，软件模块基于经过形式化验证的操作系统内核（certified kit operating system，CertiKOS），防止无人机由于意外软件故障而坠毁。考虑到无人机的机载传感器会对系统可靠性产生显著影响，对驱动传感器 SPI 总线与 I2C 总线形式化验证，并针对总线异常情况设计完成相关实验。实验结果表明，该软件架构能够有效提高无人机系统安全性与可靠性。

关键词：安全关键系统；无人机；软件架构；形式化验证