51st IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Quality and safety, a challenge for traditional and new space (1)

Author: Dr. Lei Qiao
Beijing Institute of Control Engineering, China Academy of Space Technology (CAST), China, 13811459711@163.com

Mr. Jinkun Zhang
Beijing Institute of Control Engineering(BICE), China Academy of Space Technology(CAST), China, jkz1993@163.com
Prof. Hua Yang
Beijing Institute of Control Engineering(BICE), China Academy of Space Technology(CAST), China, yangh@bice.org.cn
Prof. Bo Liu
Beijing Institute of Control Engineering(BICE), China Academy of Space Technology(CAST), China, liub@bice.org.cn
Prof. Hongjin Liu
Beijing Institute of Control Engineering(BICE), China Academy of Space Technology(CAST), China, liuhj@bice.org.cn
Prof. Mengfei Yang
China Academy of Space Technology, China, yangmf@bice.org.cn

FORMAL VERIFICATION TECHNIQUES ON SPACECRAFT EMBEDDED OPERATING SYSTEMS

Abstract

Embedded operating systems have been widely adopted in many safety-critical applications, including aerospace systems. OS being one of the most fundamental layers of software systems, a single bug or loopholes may cause the crash of all the applications running above it. Therefore its safety and security is the prerequisite to fulfill the “zero-defect” requirement of safety-critical systems. Formal verification has been viewed as a promising technique to ensure the safety and security of OS kernels, and has been a hot research topic in recent years. In this paper we plan to study the general methodology, theories and tools to formally verify safety-critical embedded operating systems. We would build models for all the stages of the system development, including models for requirements, design and implementation. Then we formally specify system requirements and key properties in the models of different abstraction levels. We use the contextual refinement theory as a general verification framework to establish the refinement between the high-level system requirements and the low-level executable code of the OS kernel. The full formalization and verification will be done in the proof assistant Coq, which can be used as a unified foundational logical framework. Based on this foundational logic, we can on the one hand reuse or develop various domain-specific theories and tools, and on the other hand to support their interaction and integration to provide rigorous safety and security guarantees for the whole system. Given the methodologies,theories and tools, we will verify SpaceOS, an embedded real-time OS that has been widely deployed in spacecrafts.