Property Oriented Verification, Testing and Monitoring of Safety Critical Software

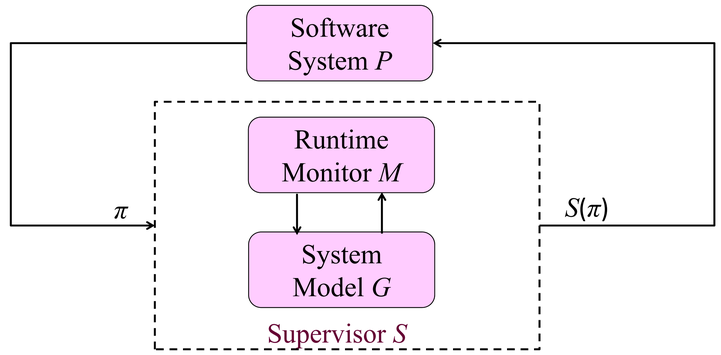
Wei Dong (wdong@nudt.edu.cn)
Professor, Department of Computer Science
National University of Defense Technology, China.

Runtime Verification and Active Monitoring

Software Active Monitoring

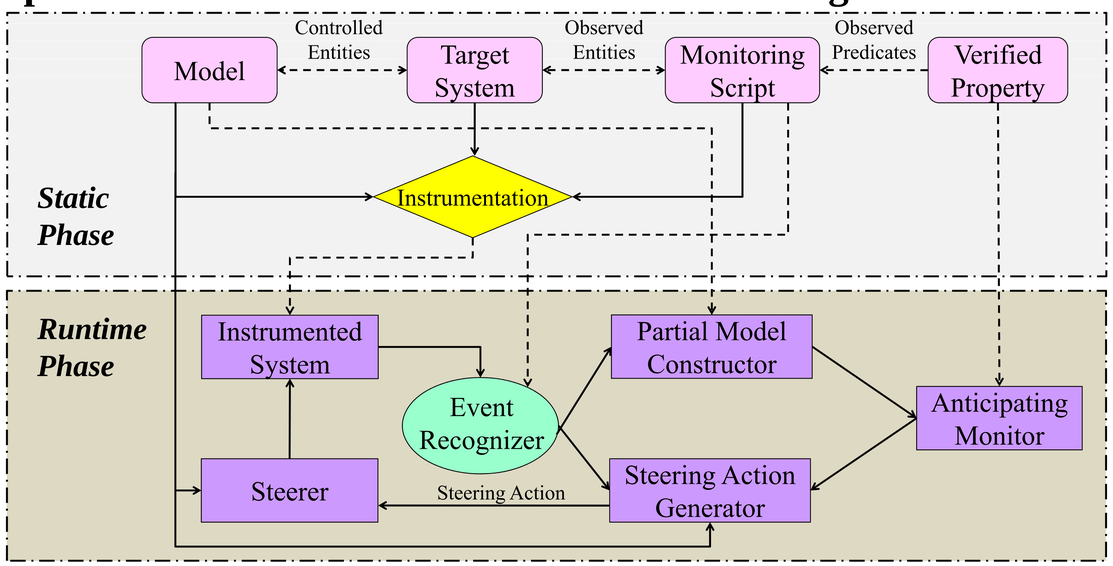
Improve the runtime verification technique to predict non-conformance (*prediction*), and prevent the system from reaching the real violation (*prevention*).

Feedback Loop of Active Monitoring



π: finite execution trace of P $S(\pi)$: steering action based on π

Implementation Framework of Active Monitoring



Some of Our Main Interests in Future

I: Analysis and Verification of Cyber Physical Software

Cyber-Physical System features the tight combination and coordination between computational and physical elements. Analysis and verification of CPS software will face some grand challenges which are also interesting.

II: Verification-Driven Embedded OS Development

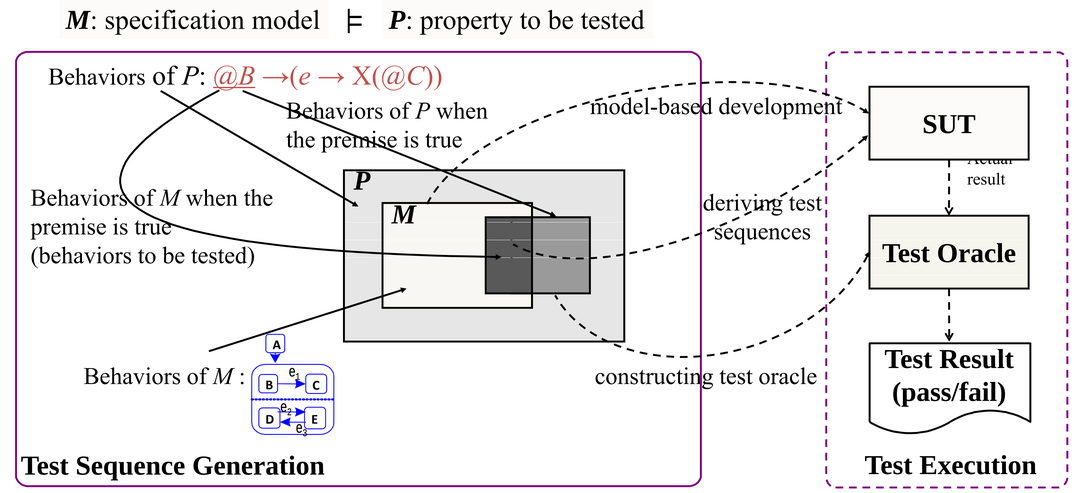
Integrating formal methods and tools, which include model checking, static analysis and theorem proving, to develop trustworthy microkernel based embedded operating system which will be use in critical areas.

Property Oriented Testing

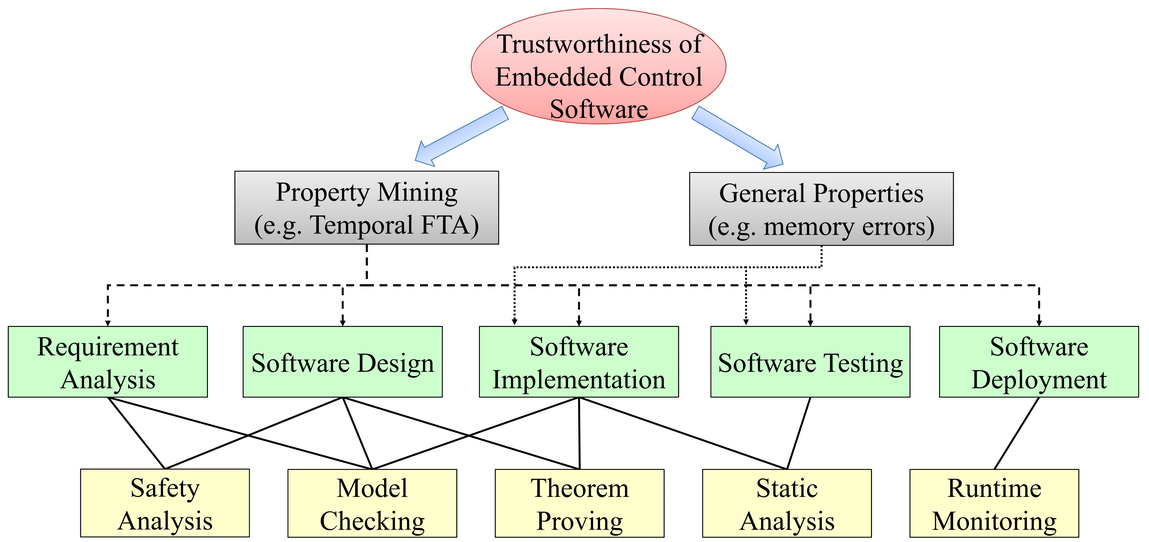
Background

- Model-based testing of reactive systems
- Traditional testing is not targeted but "comprehensive"
- It is desired to focus testing efforts on system behaviors of utmost interests
- Save testing budget and time

Principle of the Method



Trustworthy Property Guided Software Development



Domain Specified Property Mining

- Domain experience, e.g. failure modes
- Method based on analysis, e.g. via temporal fault tree analysis
- Described by temporal logic, etc.

General Property

- Language related, such as null pointer , memory leak, etc.
- Coding rules, e.g. MISRA C, etc.

Above work has been supported in part by the National Natural Science Foundation of China (NSFC) under Grants No. 60233020, 60303013, 60673118, 60970035, 91018013 and 61120106006.

國防科学技術大学 NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY