CENTER FOR
DIGITAL SAFETY & SECURITY

AUSTRIAN INSTITUTE
OF TECHNOLOGY

RUNTIME VERIFICATION OF CYBER-PHYSICAL SYSTEMS

WHAT IS RUNTIME VERIFICATION?

Complex systems evolve in time and generate behaviors which are progressions of state observations. For cyber-physical systems (CPS), such observations are typically real-valued quantities that evolve in real time. We evaluate the system's correctness, efficiency and robustness according to the properties of its behaviors. We can, for example, require or forbid sequences of events that follow a certain pattern.

We can also measure some quantitative properties of the behavior such as temporal distance between events, or the sum of the values of some state variable in a temporal window. We use the term runtime verification for the collection of techniques for specifying what we want to detect and measure and how to extract the information from the behaviors. Monitoring can be applied to real systems during their execution, for example, monitoring a chemical or a nuclear process, where the behaviors are constructed from sensor readings. In this case the monitoring procedure can give real time alerts about a potential deviation of the system from normal behaviors and even take some corrective action. Monitoring can also be applied during the model-based design process of the systems where behaviors correspond to simulation traces. In this context, monitoring can be viewed as part of the verification and validation (V&V) process, a lightweight form of formal verification which gives up the complete coverage associated with verification, but still uses a clean declarative specification language to classify behaviors.

HOW IT WORKS

AIT's runtime verification tools take as input a declarative specification derived from the CPS' functional requirements and automatically generate a runtime monitor from the specification. This monitor is then connected to the CPS implementation or its virtual simulation model, observes the system's execution traces and checks whether the system satisfies or violates its specification. In the case of property violation, the tool provides an explanation of the detected fault.

KEY FEATURES

- **Rigorous, yet efficient V&V methodology for CPS**
- Formal specification of CPS properties
- Reuse of runtime monitors at design-time and during operation of CPS
- Qualitative correctness and quantitative robustness measures
- Fault explanation

THE TEAM

The Dependable Systems Engineering research group at the AIT Austrian Institute of Technology has a systematic understanding of the development process of safety-critical and dependable systems. The group's expertise ranges from developing new standards, over providing workflow support, to verification & validation activities like testing and runtime verification.

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dejan Nickovic
Tel +43(0) 50550 4150
Giefinggasse 4, 1210 Vienna
dejan.nickovic@ait.ac.at
www.ait.ac.at