KhronoSim

Simulation and Testing of Real-Time Critical Cyber-Physical Systems
Topics

- Cyber-Physical Systems
- Complex Systems and System of Systems
- KhronoSim
  - High-Level Overview and Architecture
  - Simulator vs Real Equipment
  - Simulation Manager Overview
  - QEMU Manager Overview
  - Fault Injection Support
- KhronoSim (simulation example incl. video)
Cyber-Physical Systems

• Integrations of computation, networking, and physical processes

• Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa

• Physical processes are compositions of many things going on at once, unlike software processes, which are deeply rooted in sequential steps

• CPS design requires understanding the joint dynamics of: computers, software, networks and physical processes

• The mechanisms by which software interacts with the physical world are changing rapidly
Cyber-Physical Systems

- Tight coupling between on-board cyber (processing, communication) and physical (sensing, actuation) elements

  e.g. Cyber and physical elements of a space based communication system

<table>
<thead>
<tr>
<th>Cyber elements</th>
<th>Physical elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Communication node dynamics</td>
</tr>
<tr>
<td>Storage Systems</td>
<td>Noise and attenuation environment</td>
</tr>
<tr>
<td>Computation Resources</td>
<td>Free space loss</td>
</tr>
<tr>
<td>Network Topology</td>
<td>Access to energy collection</td>
</tr>
<tr>
<td>Hardware</td>
<td>Attitude dynamics</td>
</tr>
<tr>
<td>OSI Stack Layer</td>
<td></td>
</tr>
</tbody>
</table>
Cyber-Physical Systems

Complex Systems and Systems of Systems

- Integrated set of components and sub-systems
  - Tightly interacting together to achieve a specific goal

- Guaranteeing that individual sub-systems behave according to their specifications is a (relatively) “simple” task
  - The magnitude of the validation is much higher when it comes to provide guarantees on the correct integrated behaviour

- All the possible interactions between the sub-systems must be properly tested in order to capture all the system properties
Cyber-Physical Systems

Complex Systems and Systems of Systems

- Testing systems in actual environment is overly expensive and/or too slow
  - In particular when considering Cyber Physical Systems
  - Even simple algorithms and software may become extremely complex to test due to the interaction with the environment

- The use of model and platform simulators is growing in importance to address testing of complex systems
  - Nevertheless there is a challenge on how to integrate the different testing components

---

**Cyber-Physical Systems**

**Complex Systems and Systems of Systems**

- Testing systems in actual environment is overly expensive and/or too slow
  - In particular when considering Cyber Physical Systems
  - Even simple algorithms and software may become extremely complex to test due to the interaction with the environment

- The use of model and platform simulators is growing in importance to address testing of complex systems
  - Nevertheless there is a challenge on how to integrate the different testing components
KhronoSim

- Platform for testing Cyber-Physical Systems in closed-loop

- Distributed, modular, extensible and usable in multiple application domains

- Hard-real-time control, enabling the integration of simulation models to build a closed loop test environment and allowing the use of physical and virtual systems alike
KhronoSim High-Level Architecture

- **Launcher:**
  - Manage and control the access of a Runner to the SUT

- **Runner:**
  - Executes the test suite started by the Tester

- **Executive:**
  - Core component
  - Executes commands and actions requested by the Runner
    (e.g. sending messages and reading and/or writing electrical signals)
  - Interfaces directly with the SUT
KhronoSim: Simulator vs Real equipment

DDS Data Communication

Executive #1

Simulator #1

Simulator #X

Bus Protocol #1

Bus Protocol #Y

IO Manager #1

IO Manager #Z

Real Equipment #1

Real Equipment #W

Debug Manager
KhronoSim Simulation Manager Overview

• Runner sub-component

• Responsibilities of coordinating all the aspects of a simulation namely:
  • Start, stop, pause and resume simulation
  • Set simulator parameters
  • Send simulation tick (with a predefined order if needed)

• Simulator types:
  • Cooperative
    • Coordinated by the Simulation Manager, execute by a predefined order
  • Standalone
    • Not coordinated by the Simulation Manager, not executed by a predefined order

Simulators can interact between them
KhronoSim H/W Emulation-in-the-loop support

- **Integration of QEMU**

- **QEMU Manager features**
  - Load specific configurations of a platform and/or application
  - Start/Stop emulation
  - Suspend/Resume the execution of the emulated application
  - Execute and trap commands
  - Control the speed of emulation
KhronoSim Fault Injection support

- Fault Types such as:
  - Stuck at, single set, bit-flip, burst, bus-off
KhronoSim (simulation example: Automotive Cyber-Physical System)
Conclusions

KhronoSim tackles the challenge of testing and validating complex Cyber-Physical Systems

- Support mixture of real equipment and simulators
- Using hardware emulation in the testing loop, integrated with models and environment

KhronoSim’s QEMU Manager enables the integration of hardware emulation in closed loop