



UCEF Workshop

Background on Cyber-Physical Systems

Cyber-Physical Systems (CPS) are smart systems that include co-engineered interacting networks of physical and computational components [1]. CPS integrate computation, communication, sensing and actuation with physical systems to fulfill time-sensitive functions with varying degrees of interaction with the environment, including human interaction. These highly interconnected systems provide new functionalities to improve quality of life and enable technological advances in critical areas, such as personalized health care, emergency response, traffic flow management, smart manufacturing, defense and homeland security, and energy supply and use. CPS and related systems (including the Internet of Things (IoT) and the Industrial Internet) are widely recognized as having potential to enable innovative applications and impact multiple economic sectors in the worldwide economy [2].

The impacts of CPS will be revolutionary and pervasive – this is evident today in emerging smart cars, intelligent buildings, robots, unmanned vehicles and medical devices [3]. The development of these systems cuts across all industrial sectors and demands high-risk, collaborative research between research and development teams from multiple institutions. Realizing the future promise of CPS will require interoperability between heterogeneous systems and development processes supported by robust platforms for

experimentation and testing across domains. Meanwhile, current design and management approaches for these systems are domain-specific and would benefit from a more universally applicable approach.

Cyber-Physical Systems (CPS) experimentation suffers from isolated simulation tools and many cross-platform custom adaptors which increases complexity and cost. Yet the demand for more sophisticated experiments and configurations is growing.

The National Institute of Standards and Technology (NIST) and its partner, the Institute for Software Integrated Systems at Vanderbilt University [4], have developed a collaborative experiment development environment across heterogeneous architectures integrating best-of-breed tools including programming languages, communications co-simulation, simulation platforms, hardware in the loop, and others. This environment combines these simulators and emulators from many researchers and companies with a standardized communications protocol, IEEE Standard 1516 High Level Architecture (HLA) [5]. NIST calls this a Universal CPS Environment for Federation (UCEF).

UCEF is provided as an open source toolkit that:

- comprises a portable, self-contained, Linux Virtual Machine which allows it to operate on any computing platform;
- contains a graphical experiment and federate design environment – Web-based graphical modeling environment (WebGME) developed by Vanderbilt University that provides code generation for adapting models to the simulators;
- defines a language for exercising the collection of federates, the federation, in the course of the experiment;
- separates the design of experiments from the design of the models composed in an experiment;
- manages its own scope in the definition of federated interfaces, federations, experiments – but not model design and implementations;
- develops experiments that can be deployed independently on a variety and combination of platforms from large cloud systems to small embedded controllers;
- allows experiments to be composed among local simulations, hardware in the loop (HIL), cloud simulations, and collaborative experiments across the world;
- integrates federates designed in (expected as of this workshop): Java, C++, Omnet++, Matlab, LabView, Gridlab-D.

At this workshop, participants will learn the details of UCEF, obtain a copy that they can install at the workshop and take home with them on a USB drive, and participate in a hands-on exercise to design/implement/build a collaborative experiment involving all attendees.

We are looking for practitioners of these technologies who may be interested in not only using UCEF, but more importantly in contributing to its development and evolution.

To participate in the workshop exercise you will need a laptop with a Wi-Fi connection (during the federated experiment your laptop will be connected to a local private Wi-Fi network set up for this purpose). We will provide USB drive with software needed to load virtual machine on your computer. NIST will have a couple of secure USB drives for those who cannot connect an unencrypted USB to their laptop***.

Please join us on Thursday, July 27th to learn about this exciting technology and participate in its evolution.

Workshop Logistics

- Location: NCCoE (National Cybersecurity Center of Excellence)
- Directions: 5.04 Google reviews Government office in Montgomery County Address: 9700 Great Seneca Hwy, Rockville, MD 20850 Phone: (301) 975-0200
- Date: 27 July 2017
- Time: 8:00 a.m. to 5:45 p.m.
- Registration Link: <https://appam.certain.com/profile/web/index.cfm?PKWebId=0x14555479a>
- Organizer Contacts: Martin Burns martin.burns@nist.gov, Thomas Roth tom.roth@nist.gov, Edward Griffor edward.griffor@nist.gov

PRELIMINARY AGENDA

[9:00-9:30] Welcome and NIST SGCPs NIST CPS Testbed Effort How testbed fits into research endeavors at SGCPs NIST/Vanderbilt Collaboration – C2WT, Cosimulation, ... NIST/PNNL Collaboration – TE Challenge

[9:30-10:30] Architecture Use Cases Communications Requirements HLA Overview

[10:30-11:30] UCEF Fundamentals Virtual Machine WebGME, Federate types, Interactions, Objects Federation Manager Courses of Action (COA) Experiment orchestration language

[11:30-12:00] Install UCEF Install VirtualBox, VM

[12:00-1:00] Lunch

[13:00-15:30] Hands-on UCEF Exercise Create test federate according to scripted scenario Edit and compile source code Run federation Feedback on the exercise

[15:30-16:30] UCEF Contin'd Eclipse Docker/Uberjar Mongo, MySQL and data acquisition during experiments FIWARE experimental visualization/analysis technology GridlabD Simulink LabView Omnet ++

[16:30-17:30] Collaboration Opportunity Open-Source Community GitHub Issues Forking and Pull Requests Vagrant Archiva, Git

[17:30-17:45] Feedback on Workshop

References

- [1] NIST SP 1500-201, Edward R. Griffor, Christopher Greer, David A. Wollman, Martin J. Burns (June 2017), Framework for Cyber-Physical Systems: Volume 1, Overview, <https://dx.doi.org/10.6028/NIST.SP.1500-201>
- [2] <https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#5664b318292d>
- [3] Cyber-physical systems: the next computing revolution, Raj Rajkumar, Insup Lee, Lui Sha, John Stankovic; DAC '10 Proceedings of the 47th Design Automation Conference, Pages 731-736
- [4] Cyber-physical system development environment for energy applications, Roth, Song, Burns, Neema,Emfinger, Sztipanovits, 2017 Proceedings of the ASME 2017 11th International Conference on Energy Sustainability (ES2017)
- [5] 1516-2010 - IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)-- Framework and Rules