DEFT Consortium

Developing research infrastructure in support of R&D to secure national critical infrastructure

Terry Benzel USC-ISI (tbenzel@isi.edu), David Manz PNNL (David.Manz@pnnl.gov) David Nicol UIUC (dmnicol@illinois.edu) and Laura Tinnel SRI (laura.tinnel@sri.com)

Summary:
The DEFT consortium seeks to enable research and development to improve and secure vital national critical infrastructure like energy, oil & gas, water, and transportation. Academic and industry users from across the country can utilize the DEFT federation of testbeds to conduct cyber-physical experimentation & testing. DEFT combines the assets and capabilities of multiple research partner institutions, including the Information Sciences Institute (ISI), the Pacific Northwest National Laboratory (PNNL), and the University of Illinois Urbana-Champaign (UIUC). Through these partners, the federated DEFT testbeds provide access and support to a unique combination of virtual, simulated, emulated, and physical systems for users of all sizes and resources. Researchers and companies can utilize the expertise, equipment, and facilities of the combined consortium members. In the end, DEFT enables novel research and development to address the pressing national problems for our critical infrastructure.

Wide-Area situation Awareness (WASA) Scenario:

The DEFT consortium developed a preliminary use case analysis that focuses on power grid wide-area situational awareness (WASA) as a first step toward understanding the needs, challenges, and limitations of experimentation for cyber physical systems research. The WASA use case study leveraged: 1) the existing DETER testbed technology to provide automated, highly reconfigurable and repeatable experiment control and accessibility to the research community; 2) virtualization, simulation, and a federation of three geographically distributed testbeds to achieve scalability; and 3) individual member cyber and control system capabilities to provide a set of heterogeneous cyber-physical assets, accessible to the research community. The final demonstration was presented at the 2012 IEEE Homeland Security Technology Conference.

In this use case analysis, a portion of a regional power grid was represented, and necessary information was shared between sites in a distributed situational awareness framework, enabled by ISI's DETER testbed federation software and domain-specific extensions. Illinois and PNNL provided cyber-physical integration of real, virtual, and simulated PMUs for a range of data fidelity, and ISI provided coordinated situational awareness.

The range of fidelity and scale across geographically and capability diverse federated systems in this use case, provided us a unique opportunity to illustrate the constraints that occur in cyber-physical systems and allowed us to showcase some of the research capabilities and technologies available at each partner institution. However, this initial demonstration of capabilities did not address many fundamental issues with respect to scale, complexity and varying time and fidelity dimensions.

Coordinated Distributed Environment Model Scenario:

Work to date has demonstrated the feasibility of leveraging federated testbeds to create a distributed cyber-physical testbed. However, work so far is limited to use cases where the individual testbeds need not be coordinated tightly in time and need not be coordinated at all with respect to the physical processes each observes. These are unrealistic restrictions when the need is to perform an experiment on the logical testbed that one could perform on a sufficiently large physical testbed.

A distributed testbed maps components expressed in an abstract system model to actual devices and/or simulators in different physical testbeds. Couplings between abstracted components needs to be supported by that generalization. The distribution of the testbed introduces a severe time coordination problem when directly-coupled components are mapped to different physical testbeds. For example, an abstract model of a substation might have a breaker and a phasor measurement unit (PMU) that is observing points on the (simulated) power flow within the substation. The physical processes observed at those points will be highly coupled in value and in time. Physical validity would be lost if the distributed cyber-physical testbed mapped the model's breaker to a physical breaker in one physical testbed but mapped the model's PMU to a device in a completely different physical testbed. Our challenge is to keep power flow observations and system networking activity coordinated in value and in time, by means of Coordinated Distributed Environment Models.

The next step is to make significant progress in the area of coordinating physical observations and network traffic flows, in realistic experimental scenarios, for example, where system components decompose naturally in space so that the model itself has geographic gaps between components that are mapped to different physical testbeds. It is only by beginning to address these hard questions that we can develop tools, methodologies and approaches for experimental cyber science applied to cyber physical systems.