ABSTRACT

With growing concerns for cyber security of critical infrastructures like the power grid, Cyber-Physical Systems (CPS) security testbeds are essential in providing controlled testing environments for evaluating and validating novel CPS security tools and technologies, thereby accelerating the transition of research to industrial practice. The engineering of such testbeds requires significant investments in money, time and modeling efforts to provide a scalable, high-fidelity, realistic attack/defense platform. Therefore, there is a strong need in research community, academia and industry to create remotely accessible testbeds that enable access to a broader user community through frameworks that support a range of use-cases such as vulnerability assessments, impact analysis, product testing, attack-defense exercises, and operator training. This thesis will focus on remote access framework that has been implemented on PowerCyber - CPS security testbed for Smart Grid at Iowa State University.

Firstly, this thesis introduces the motivation and need for enabling remote access on PowerCyber by providing current state-of-art work in the area. Secondly, the thesis elaborates on fundamental building blocks that enable remote experimentation, such as front-end user interface, backend experiment automation and describes the architecture, overall design flow and story-board constructs of the remote access framework. Thirdly, the thesis captures a case study of coordinated cyber-attack/defense experimentation on Remedial Action Scheme using PowerCyber remote access framework with screenshots. Details of how the remote access framework facilitated versatile user community engagement is included with survey results, use-case studies and user feedbacks. Finally, the thesis also includes a detailed discussion on practical engineering challenges that are faced in the development of scalable, multi-user, remote access CPS security testbeds.