CYPRESS

Deliverable 1.4 - Specification of a cyber-physical real-time test environment

Tohid Behdadnia, Nadia Boumkheld, Geraint Chaffey, Rick Loenders
KU Leuven / EnergyVille

Date: October 28, 2022

Executive Summary

It is clear that there is an ever increasing cyber threat to power systems worldwide. In order to mitigate this threat and ensure systems remain resilient and performant in the face of evolving adverse cyber events, simulating both the physical power system and the cyber system that provides control, protection and automation is increasingly essential. Numerous studies rely on standalone simulation, however, performing a co-simulation of both the physical system and the cyber system is essential when considering the impact of one system on the other (e.g. the impact of a cyber attack on the physical system).

In addition to simulating the cyber system and the physical system, there is also the possibility of integrating real hardware into the simulation using a real-time simulation and laboratory setup. Such a configuration allows for testing of the response of the hardware to simulated events, and allows for the system-level impact of hardware to be evaluated. As part of the CYPRESS project a real-time co-simulation environment will be developed, allowing for the simulation of electrical power systems, simulation of cyber networks and systems, and laboratory testing of power system protection, control and automation systems. This real-time co-simulation environment will allow for the testing of the interactions and co-dependence between the different system elements.

This document describes the design specifications of the cyber-physical real-time test environment, including detailed description and motivation for the choices made for each of the elements as well as their interfacing.

The power system simulation will use selected benchmark networks - in common with the rest of the CYPRESS project - in order to show the power system impact of adverse cyber events. The simulation will be performed in real time on an RTDS simulator such that real hardware can be interfaced to the simulation, and complemented with Electro-Magnetic Transient (EMT) simulation in order to represent all power system phenomena - from steady state to very fast transients.

A cyber simulation will be performed to allow simulation of a range of adverse cyber events - malicious attacks as well as unintentional faults. Two types of cyber simulation are chosen for the studies - firstly traffic (information flow) modification using SNORT and Linux traffic control, and secondly an advanced simulation platform NS-3 in order to model the elements of a modern cyber system. The cyber simulations will be connected to the power system simulator such that control actions can be taken on the power system, and that measurements from the power system are passed to the cyber simulation.

Physical industrial control and protection hardware - identical to that used in real power systems - will be integrated into the cyber-physical co-simulation. This setup will use a wide range of industrial devices, including protection Intelligent Electronic Devices (IEDs/relays), Remote Terminal Units (RTUs) and industrial networking equipment. The use of this hardware 'in-the-loop' allows the stud-

ies performed in this part of the CYPRESS project to move beyond pure simulation studies - allowing analysis of the cyber security and system impact of industrial solutions. This configuration allows for a highly powerful and reconfigurable test system, for example looking at *vulnerabilities in devices that are in use in real power systems*, and *examining the possible power system impact of a variety of cyber attacks on the devices*. The aim is to have a test setup as close as possible to that in place in real world power systems. Coupled with the cyber simulation and the power system simulation, the overall test setup allows for realistic cyber attacks to be simulated, and propagated to the in-lab network to examine device and system impact.

The connection between cyber simulation, power system simulation, and the industrial hardware will require an interfacing arrangement. An interface will be provided between the NS-3 cyber simulator and the RTDS power system simulator for signals that require a direct connection between the cyber and physical simulations. The NS-3 simulator will also have a standard Ethernet interface for communicating with the in-lab industrial networks and devices. The SNORT and Linux traffic control packet manipulation is designed for connection within an Ethernet network and therefore requires no additional interfacing.

Summarizing, this document describes the specification, motivation and design for the real-time cyber-physical co-simulation environment. In the next phases of the project, the designs detailed in this deliverable will be implemented, for in depth testing of cyber attacks, penetration testing on real industrial devices, and examination of power system impact and possible mitigation.