Extensible Cyber-Physical Systems (CPS) are loosely connected, multi-domain platforms that “virtualize” their resources to provide an open platform capable of hosting different cyber-physical applications. These cyber-physical platforms are extensible since resources and applications can be added or removed at any time. However, realizing such platform requires resolving challenges emanating from different properties; for this paper, we focus on resilience. Resilience is important for extensible CPS to make sure that extensibility of a system doesn’t result in failures and anomalies.

Since extensible CPS have dynamic resources and applications, resilience mechanism should be autonomous. To achieve this, we are currently working on a platform called CHARIOT (Cyber-pHysical Application aRchI-tecture with Objective-based reconfiguraTion). As shown in Figure 1, CHARIOT comprises design-time and runtime entities. CHARIOT-ML is a modeling tool used at design-time. Applications are modeled as components with functionalities. Systems are modeled using goal-based system description, which allows them to have mission goals that can be satisfied by functionalities. This results in a generic description of system requirements, which is later used at runtime to provide autonomous resilience.

Runtime aspect of CHARIOT comprises a distributed infrastructure that implements a self-reconfiguration based autonomous resilience mechanism. This mechanism is implemented as a closed loop comprising (a) monitoring infrastructure, (b) a Satisfiability Modulo Theories (SMT) based resilience infrastructure that computes new configuration points at runtime, and (c) application managers. It is important to note that any resilience mechanism provided should be predictable as CPS have strong timing requirements. Figure 2 presents preliminary result to show predictability of the Configuration Point Computation (CPC) algorithm used to compute new configuration points.