# Common (high level) activities implemented

* Reachability to an assets (containment): considering that we target the angle of topology we expect that the modelling of a system (i.e. CPS) contains locations that an activity initiator would traverse through to reach a certain location containing the target asset.
  + For example, a visitor entering the *hallway* (location2) from *entrance area* (location1), then enters a *reception office* (location3). Then we can define an activity which has the containers of the initiator to be *entrance area* (location1) and *reception office* (location3).
  + Current criteria for when this is applied:
    - Activity initiator in the first activity is contained by different entities in the precondition and postcondition.
    - Container of initiator in the second activity should be different from the container in postcondition of the first activity.
    - Connection between the containers of the postconditions in the first and second activity should exist.
  + This type of activity is not associated with a specific vulnerability or attack.
* Connectivity to an asset: similar to the containment we consider connectivity to be a part of the topology as we present both containment and connectivity of a topology.
  + For example, a visitor connects to smart light in toilet, then connects to a hvac in the server room. Then we can create an activity that has the initiator connected to the hvac (target asset) through a smart light (exploited asset).
  + Current criteria for when this is applied:
    - Check basics (same action name, same initiator, same activity type).
    - Activity initiator in the first activity contains an entity that has connections that increases from pre to post. These connections should be associated with the target asset.
    - In the second activity, the same entity in the postcondition has new connection different from that in the post of the first activity postcondition.
  + This type of activity is not associated with a specific vulnerability or attack. On the contrary of other attack patterns stated in other resources such as CAPEC.

Others (mainly inspired from CAPEC)

* Collect data (main source: <https://capec.mitre.org/data/definitions/150.html>): collect data from a target asset in the system