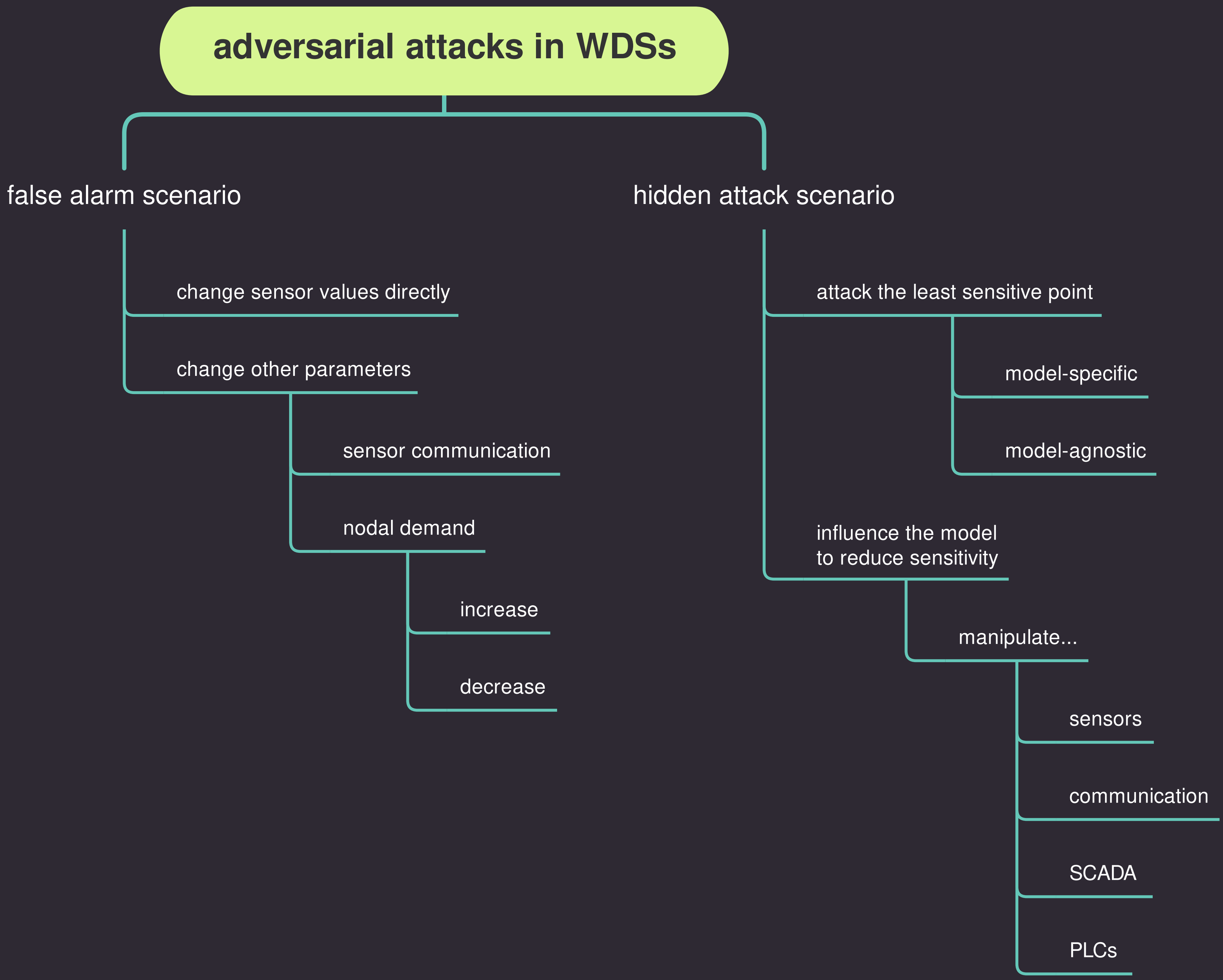

adversarial attacks in WDSs

- false alarm scenario
  - change sensor values directly
  - change other parameters
    - sensor communication
    - nodal demand
      - increase
      - decrease
- hidden attack scenario
  - attack the least sensitive point
    - model-specific
    - model-agnostic
  - influence the model to reduce sensitivity
    - manipulate...
      - sensors
      - communication
      - SCADA
      - PLCs