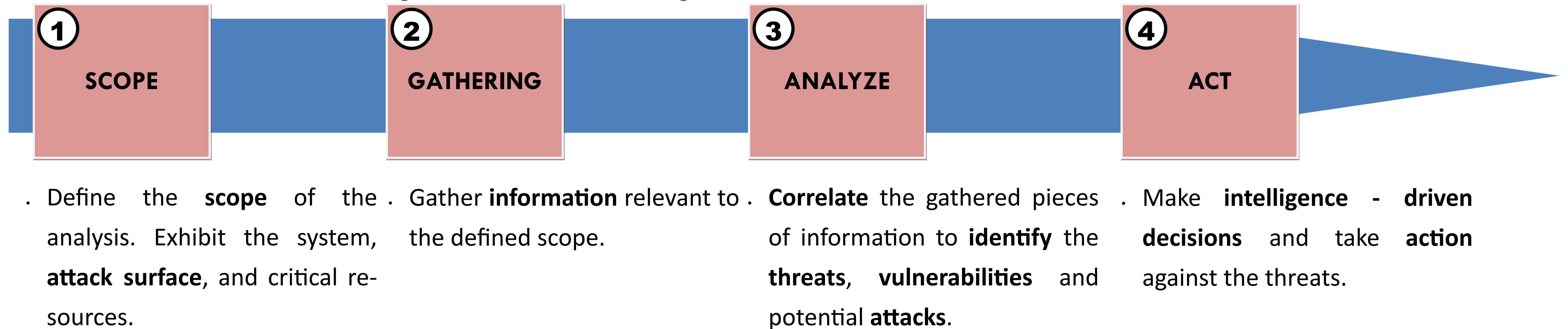


## Threat-Driven Cyber Security



## Dynamic Attack-Defense Model

How to model and build a **dynamic simulation** of a **running system** in a **cyber security** context ie in an environment where **threat actors** evolve ?

### Attack Surface Reification

**Concepts** identification and description. Relevant **structures** and **abstractions** choices.

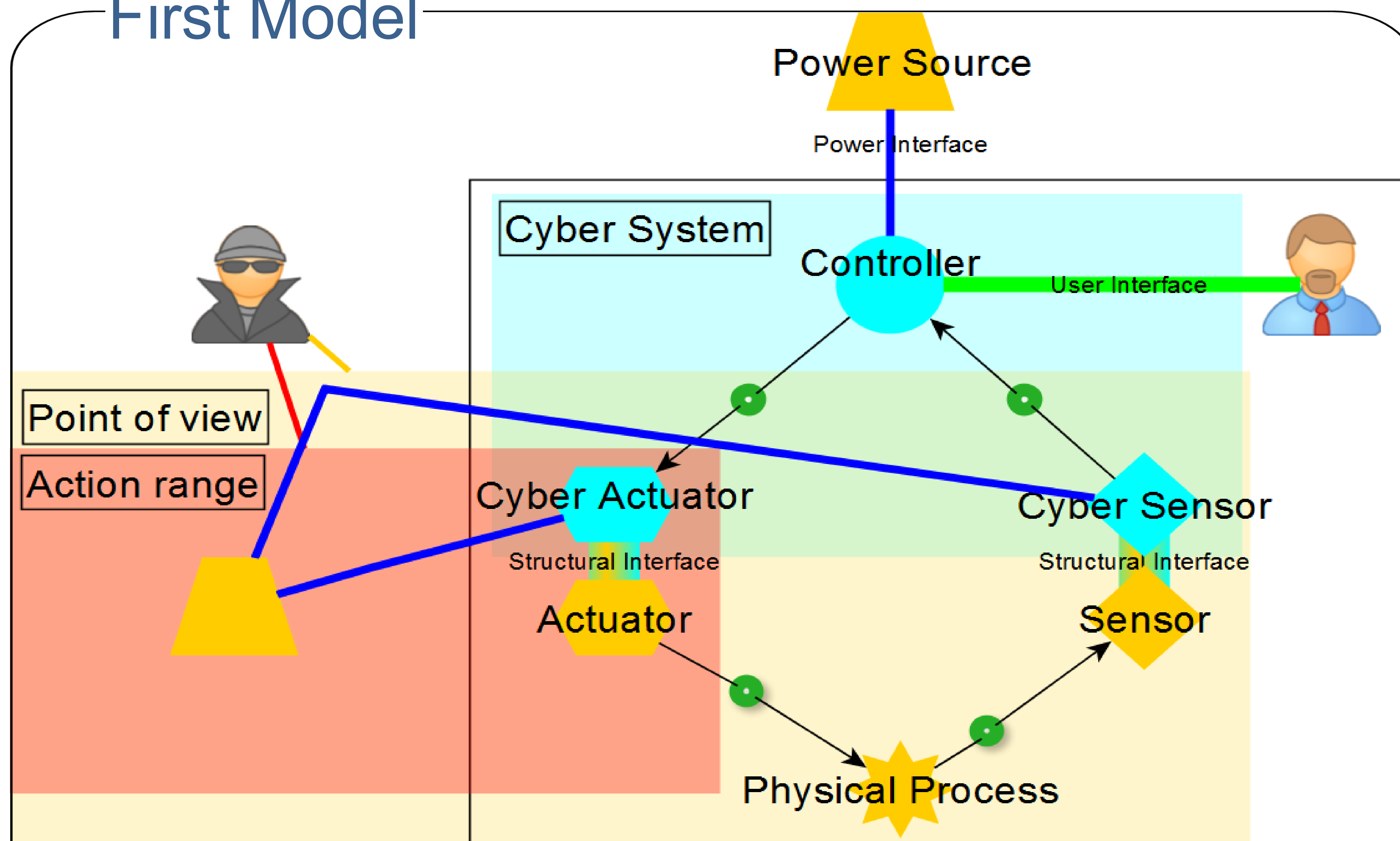
### Dynamic Model

**Lifecycle** of the system. **Temporal** dimension, **interactive** system and evolving **attackers** and **defenders**.

### Implementation & Simulation

**Runnable** and non-cyber-agent-**user-friendly** simulation. **Compatibility** with other security **tools**.

## First Model



**Cyber Physical System:** Group of interacting entities. Target of the attackers. Definition in an **environment**.

**Actor:** **Attacker** or **defender** of the system. Interactions with the system through an evolving **point of view** and **action range**.

**Actions:** Available **evolution** attempts of an actor's interactions with the system. (modification, insertion, deletion)

## Research Directions

### Cyber Threat Intelligence

Cyber-related vocabulary

### Operational Design

Military operation planning

### Embedded Systems

Cyber physical system modeling

### Attack Trees

Step-by-step attack modeling

### Model-Checking

Formal verification method

### Game Theory

Multiplayer scenarii modeling

### Temporal Graphs

Evolving data structure

### Automata

Conditional state-machines

### Composite Structure

Both textual and graphical