





**Formal Methods**

# Specification

**`Formally express the goal'**

# Verification

**`Ensure controller satisfies the  
goal'**

# Reactive Synthesis

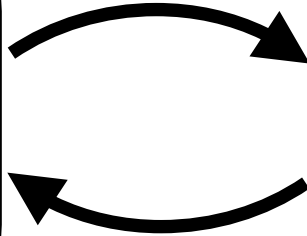
**`Design correct-by-construction  
controller'**

# Higher Logical Layer

**logical control loop**

**logical  
context**

**logical  
controller**

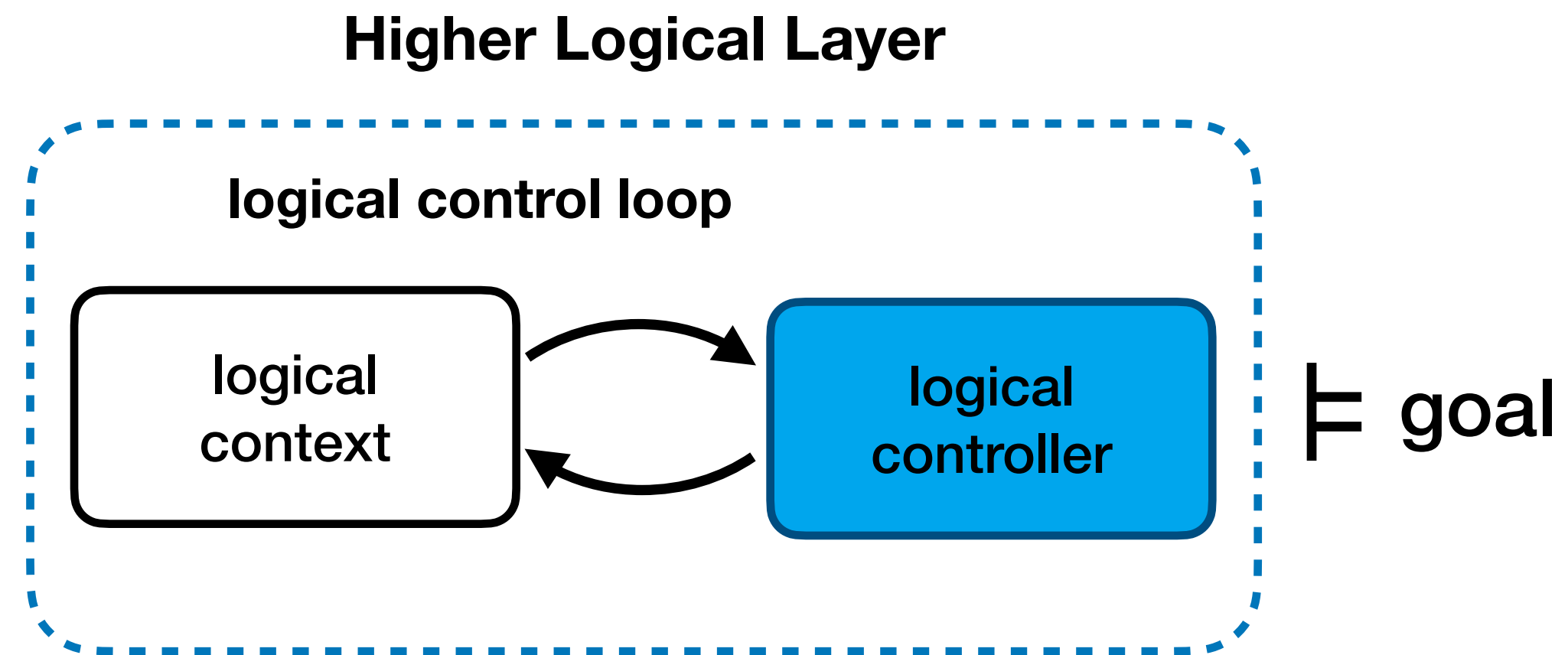


**$\vdash$  goal**





# Formal Methods



## Specification

‘Formally express the goal’

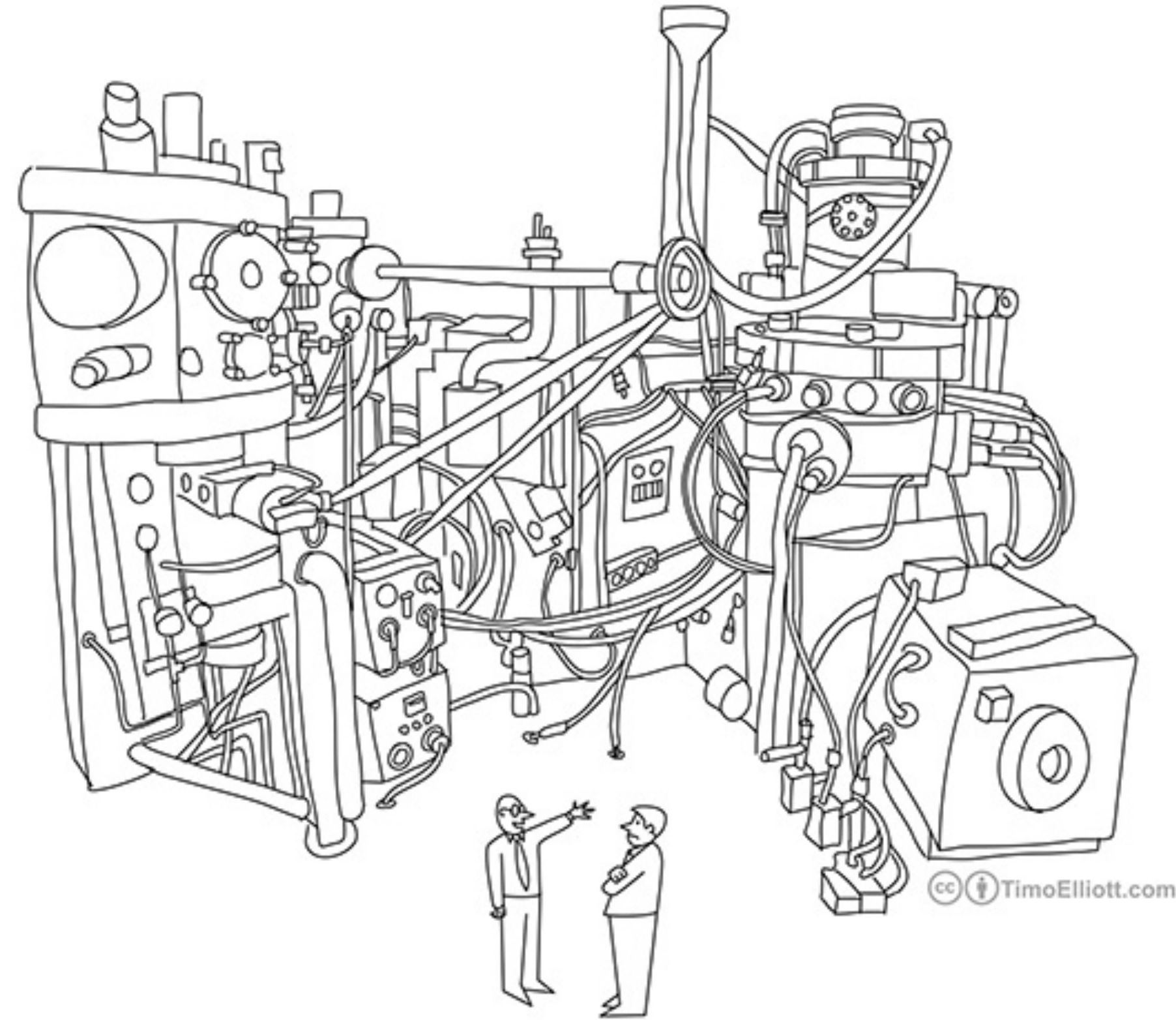
## Verification

‘Ensure controller satisfies the goal’

## Reactive Synthesis

‘Design correct-by-construction controller’

# Specification Inference: Explainability



*“Well, sure, it looks complicated...”*