UNIVERSITY OF Southampton

Prototyping the Smart Ballot Box

Robert Thorburn

HD-Sec Workshop, 16th September 2021

Agenda

- The SBB and Capability Hardware
- SysML model
- Potential SBB designs
- Demonstrator and attack

The SBB and Capability Hardware

- The SBB using off-the-shelf components
  - Easy to swap components out
  - Rapid prototyping
  - Reduced functionality per component:
    - Lends itself to compartmentalisation
    - Fail to stop as opposed to fail to vulnerable
    - Can derive localised threat model

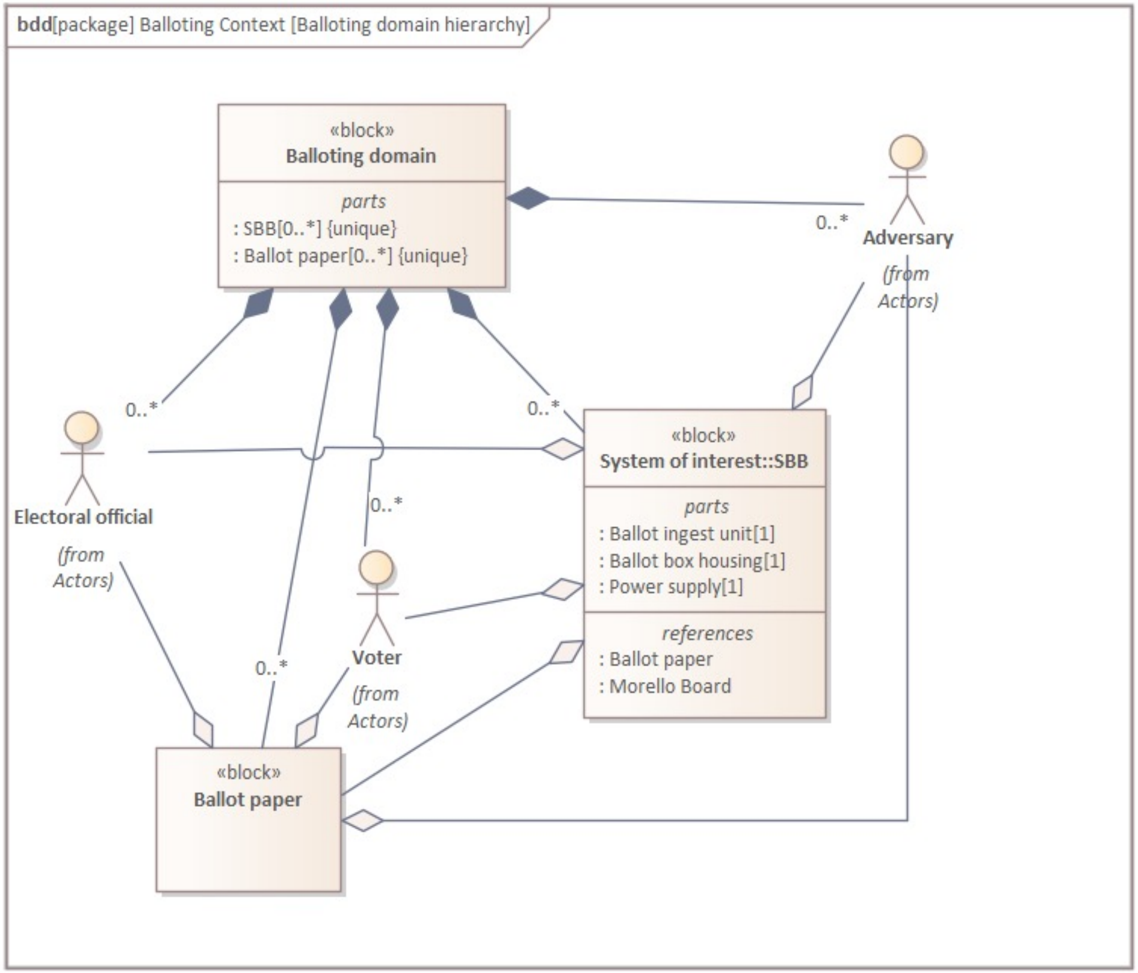
The SBB and Capability Hardware

- Is capability hardware needed for an air gaped device?
  - Yes, air gapping can be bypassed
    - Stuxnet – human failure to follow procedure
    - SolarWinds – supply chain hack
  - Yes, elections are significant targets
  - Yes, air gapping interrupted for data up/down load
- The mix of a highly secure bespoke system with off-the-shelf components allows for the development of new best practice

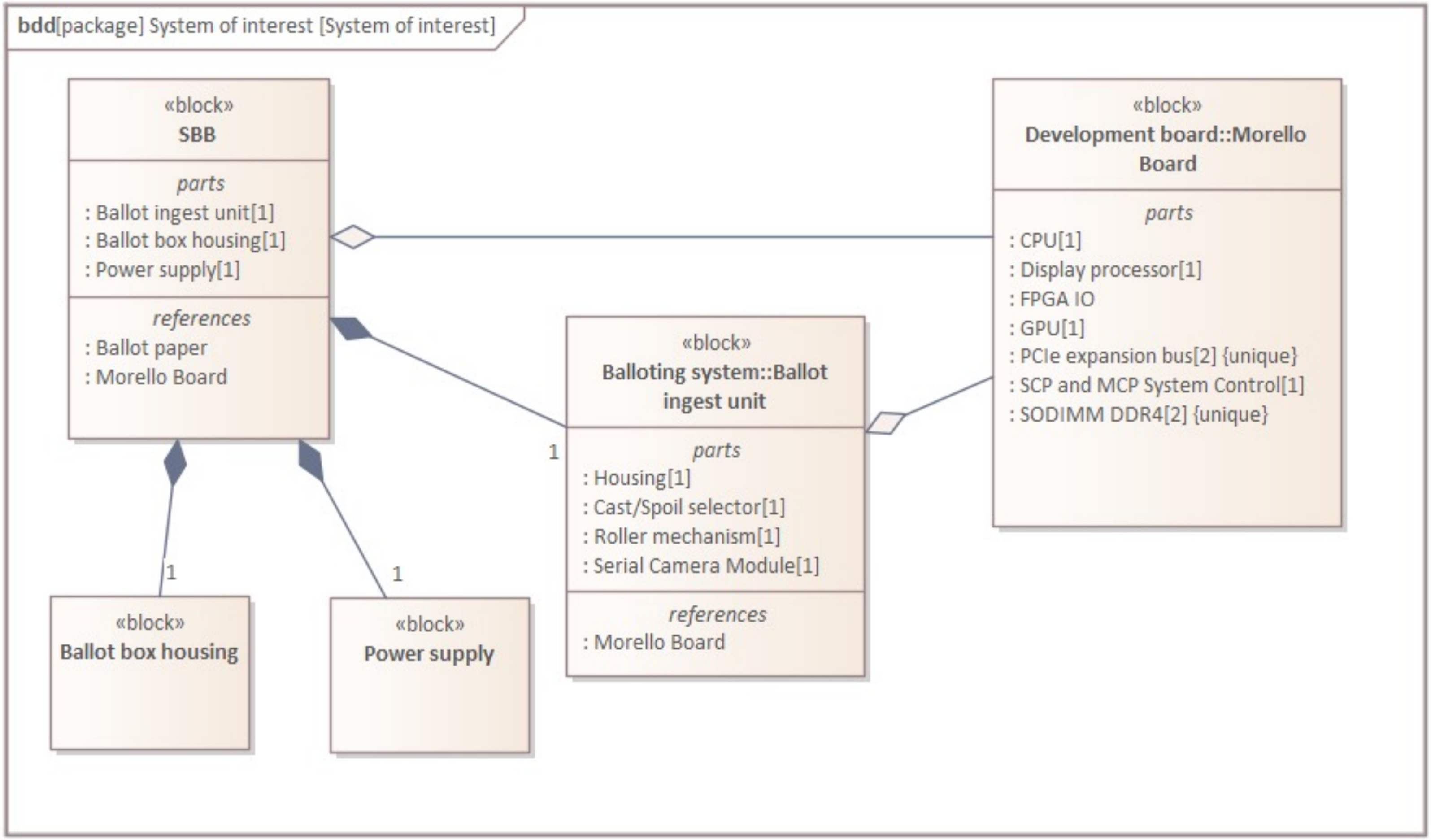
The SBB and Capability Hardware

- Building a physical prototype allows for extensive testing
  - Security includes both software and hardware elements
  - Components are not standard and well understood, which undermines software simulation
- Morello capabilities used in final prototype
  - SBB System Model Refinement Strategy as requirements
  - Compartmentalisation to build on MAC advantage
    - Least privilege: only the rights needed to operate
    - Control flow deviation and software state manipulation

Domain context



System of Interest



bdd[package] System of interest [System of interest]

«block»
SBB

parts
: Ballot ingest unit[1]
: Ballot box housing[1]
: Power supply[1]

references
: Ballot paper
: Morello Board

«block»
Development board::Morello Board

parts
: CPU[1]
: Display processor[1]
: FPGA IO
: GPU[1]
: PCIe expansion bus[2] {unique}
: SCP and MCP System Control[1]
: SODIMM DDR4[2] {unique}

«block»
Balloting system::Ballot ingest unit

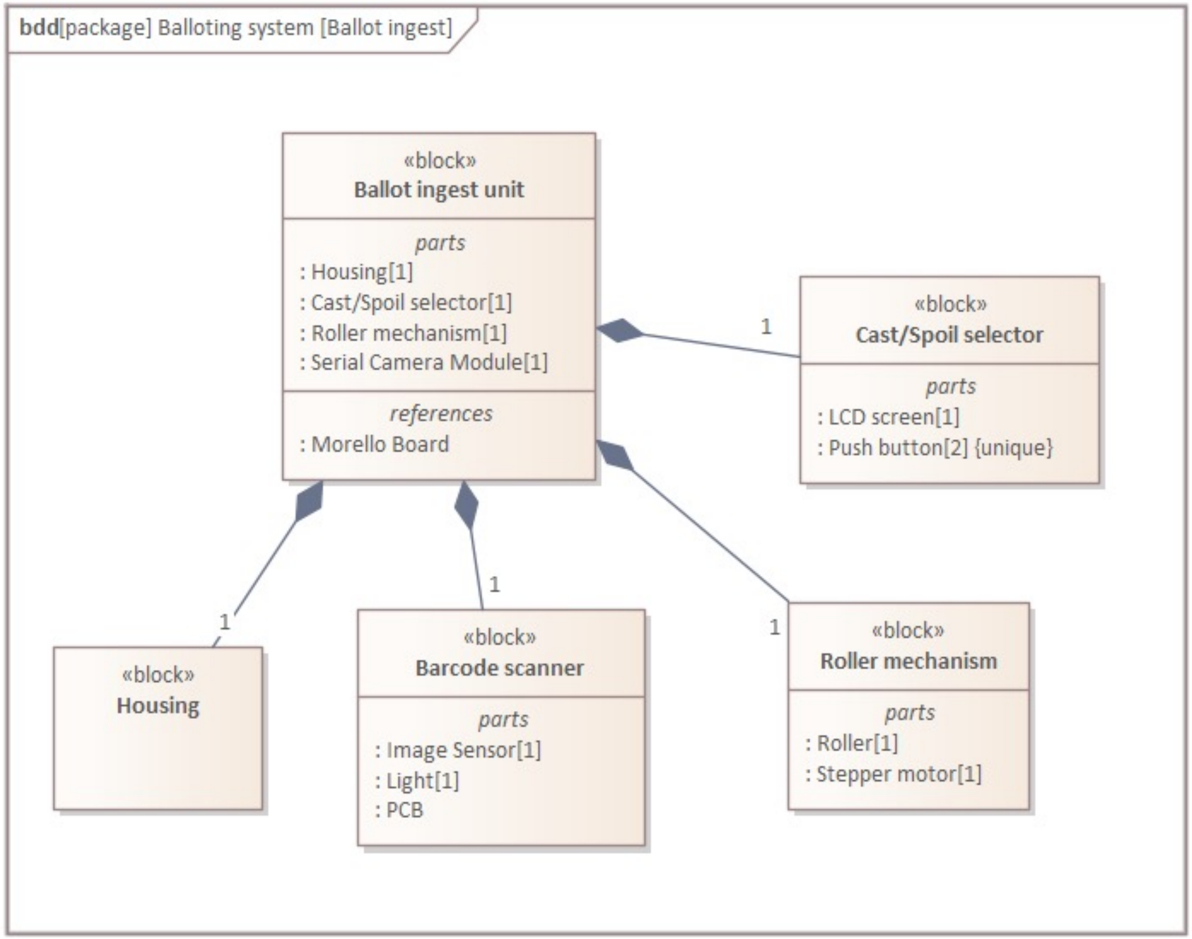
parts
: Housing[1]
: Cast/Spoil selector[1]
: Roller mechanism[1]
: Serial Camera Module[1]

references
: Morello Board

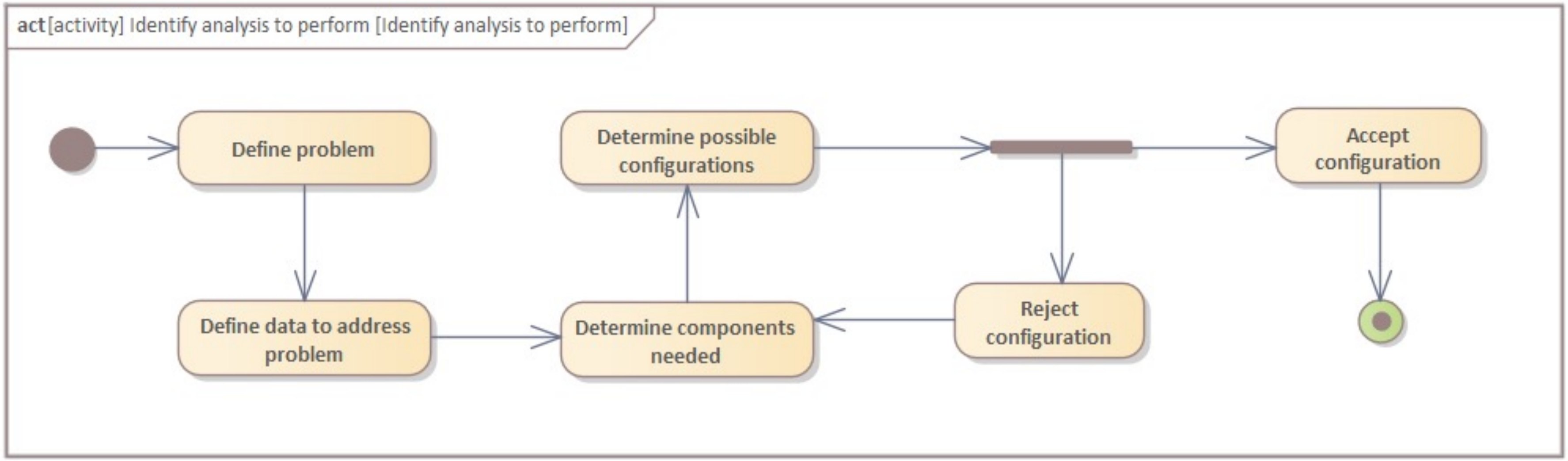
«block»
Ballot box housing

«block»
Power supply

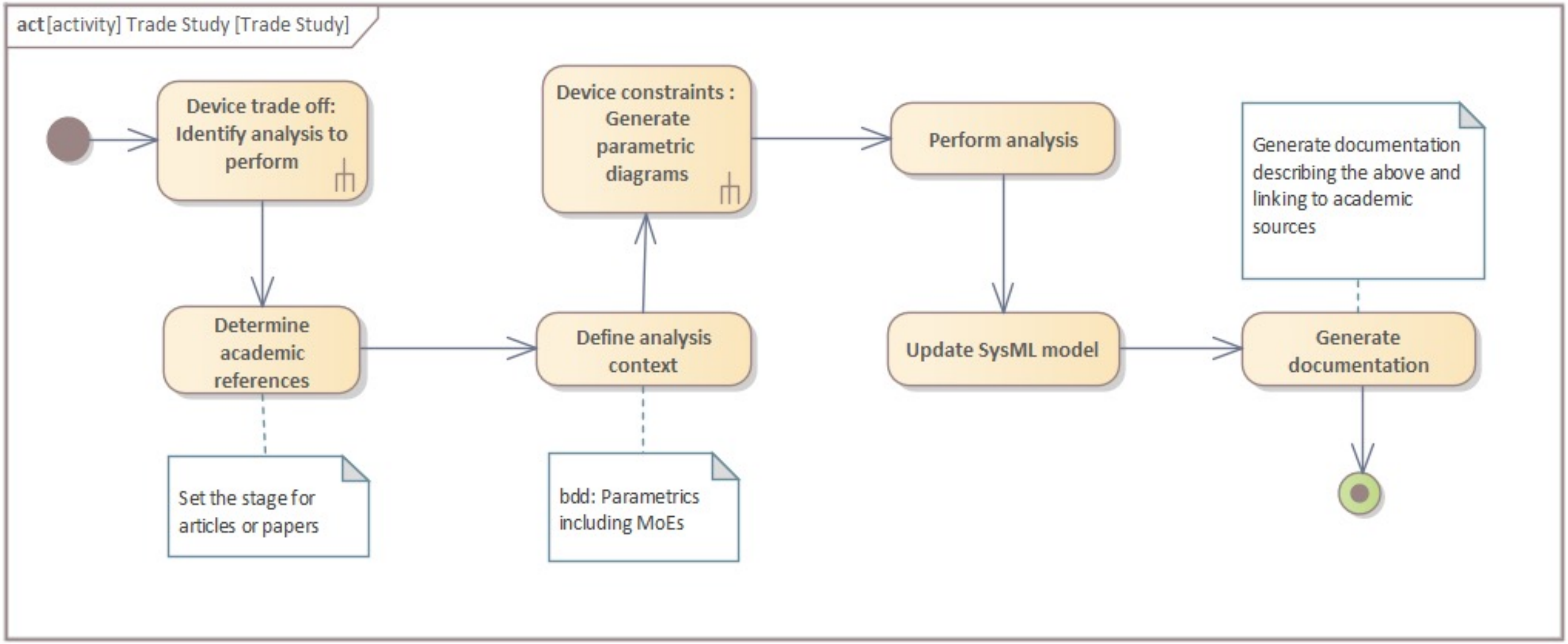
Balloting system



Trade study: analysis


act [activity] Identify analysis to perform [Identify analysis to perform]
Define problem
Define data to address problem
Determine components needed
Determine possible configurations
Reject configuration
Accept configuration

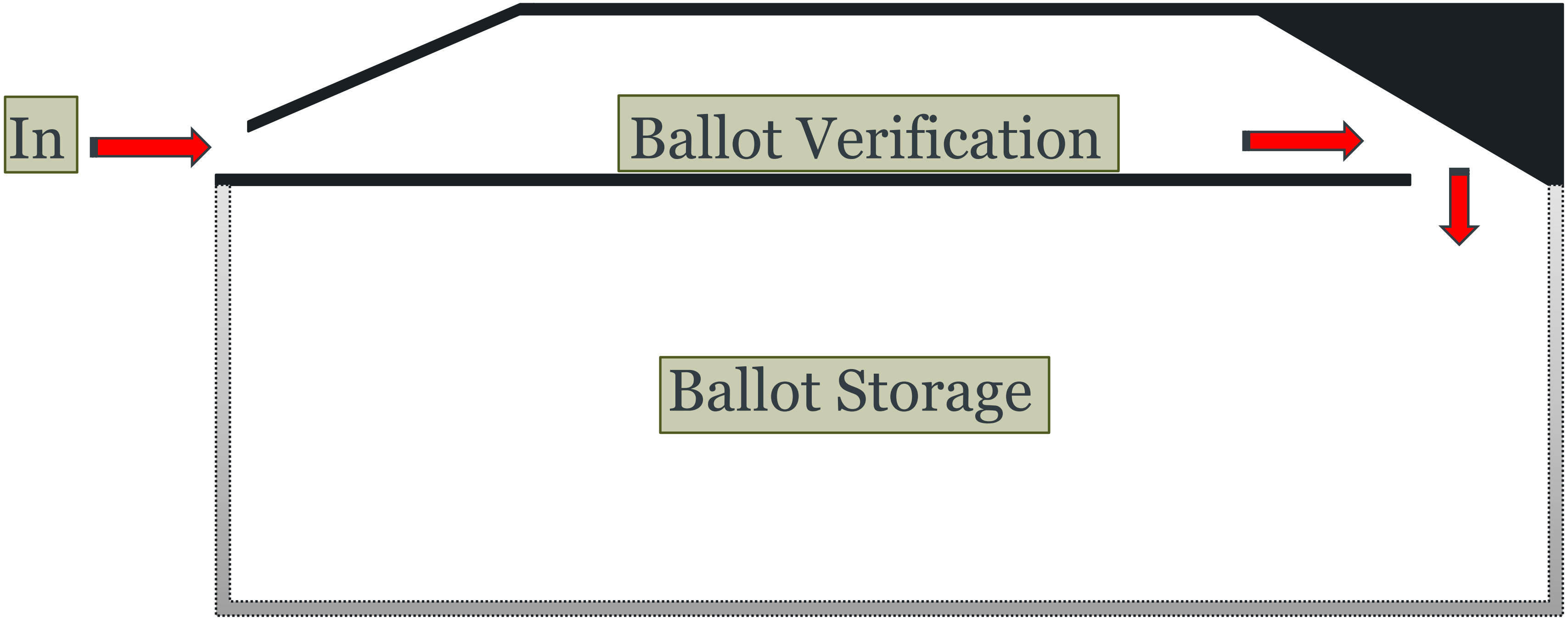
Trade study



act [activity] Trade Study [Trade Study]
Device trade off: Identify analysis to perform
Determine academic references
Set the stage for articles or papers
Define analysis context
bdd: Parametrics including MoEs
Device constraints : Generate parametric diagrams
Perform analysis
Update SysML model
Generate documentation
Generate documentation describing the above and linking to academic sources

System of Interest

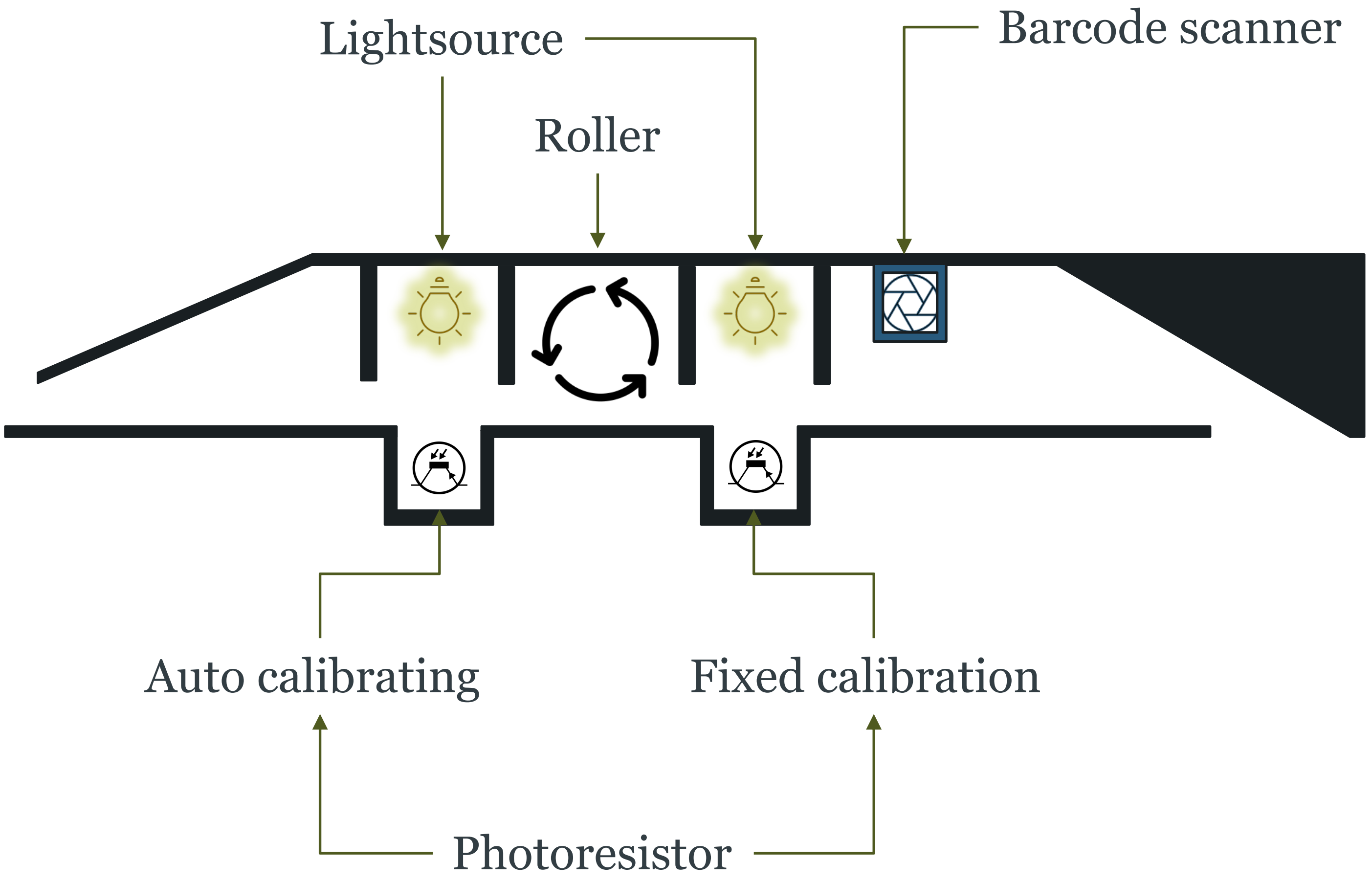
- **Black box :** Internals not yet specified



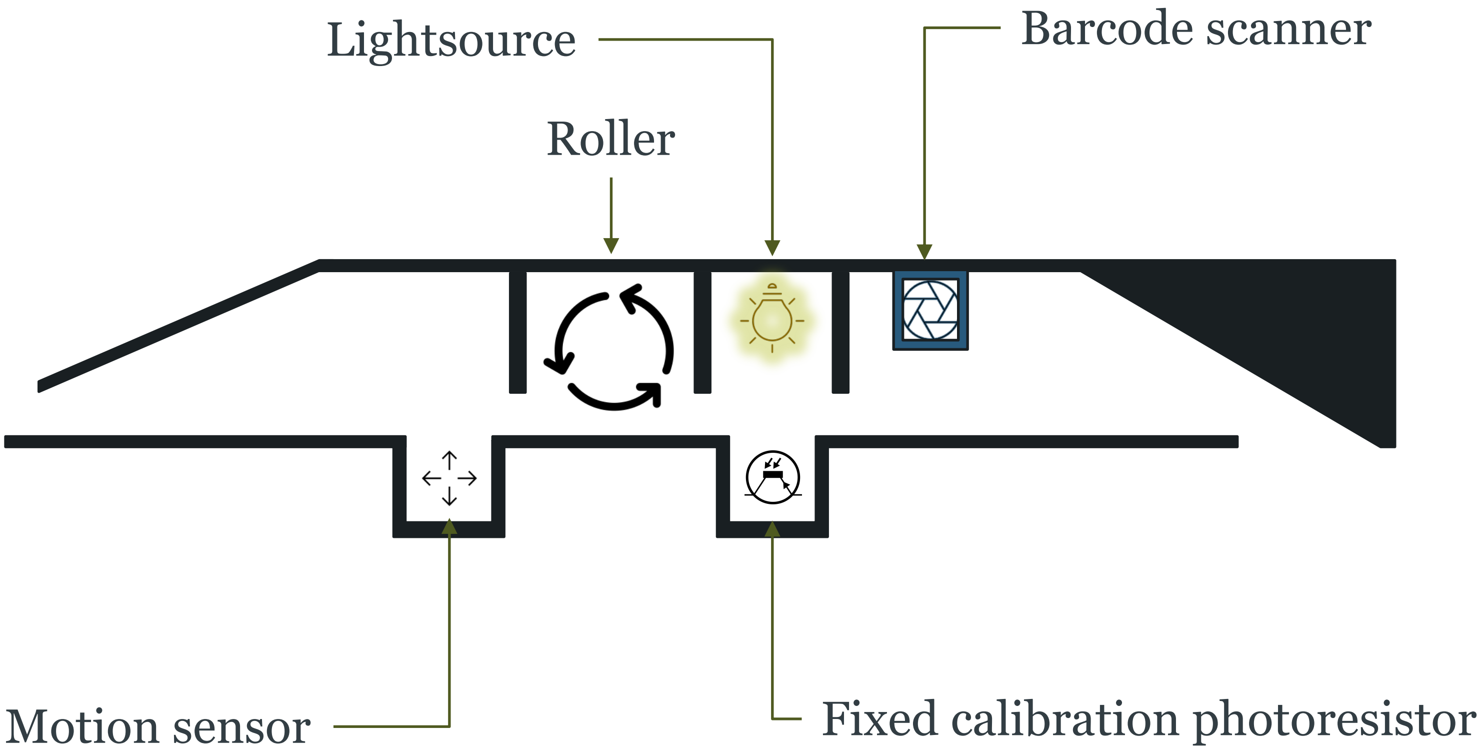
White box

- Logical subsystem
- Too many possibilities without further testing
- The need to better understand components
- Five potential designs
  - Balloting system::Ballot ingest unit
  - Off-the-shelf sensors and actuators
  - Foamboard and upcycling for testing, then prototyping with 3D printed housing and parts

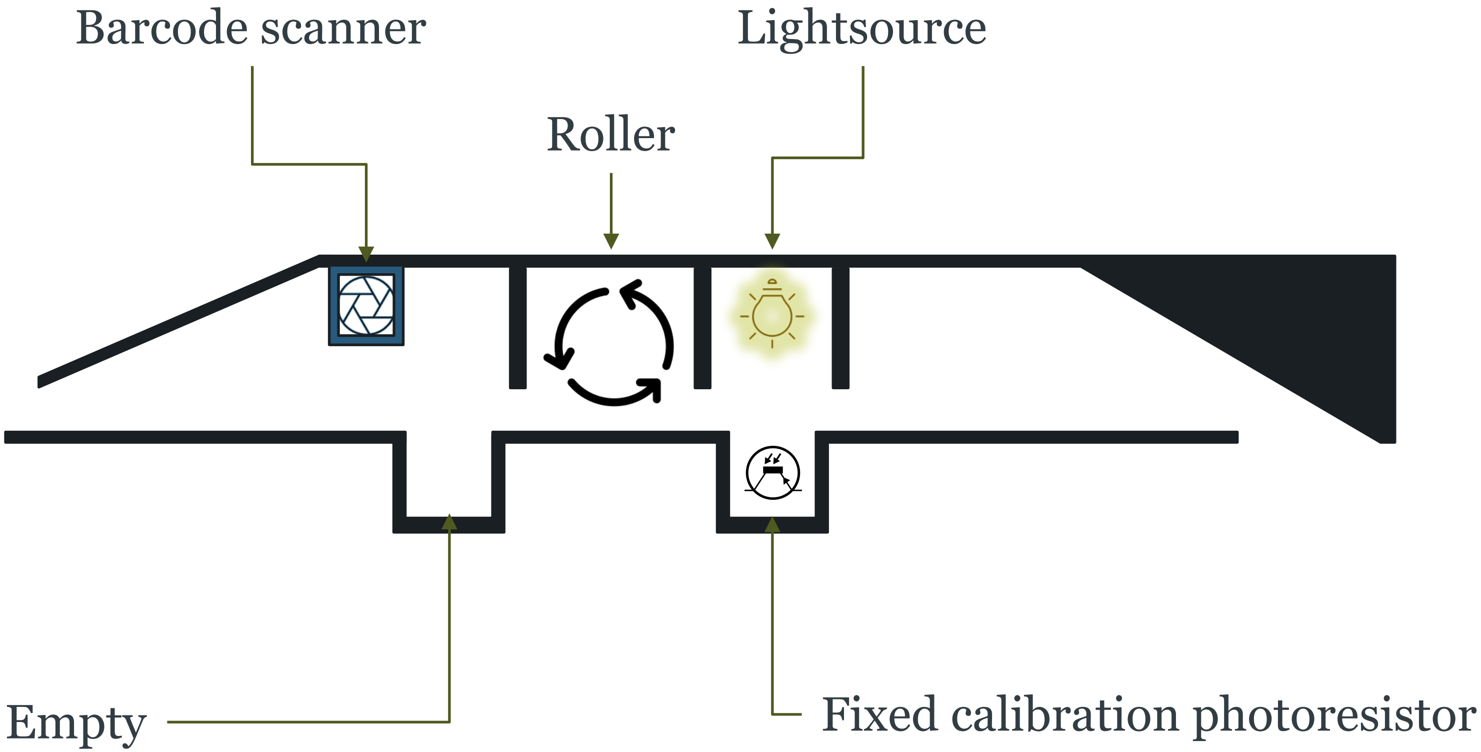
Design 1


Lightsource
Barcode scanner
Roller
Auto calibrating
Fixed calibration
Photoresistor

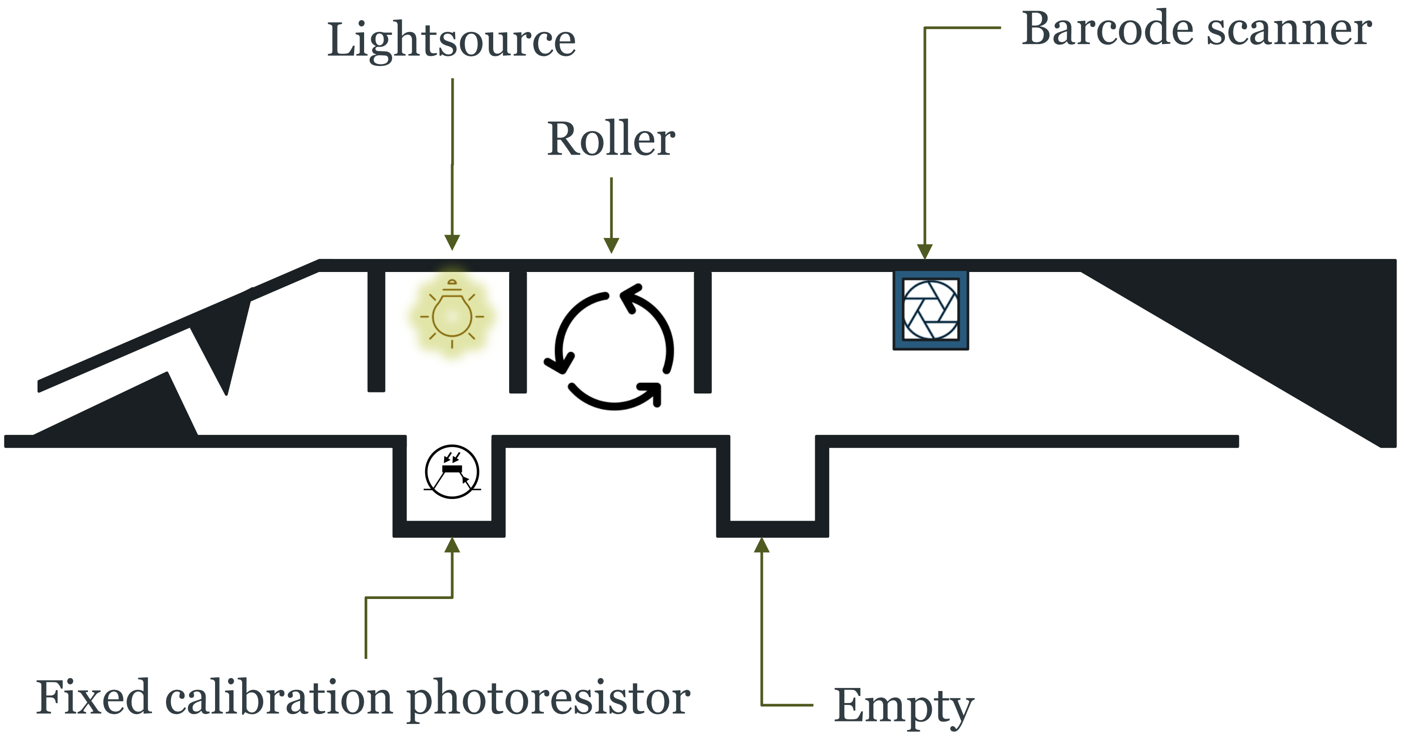
Design 2


Lightsource
Barcode scanner
Roller
Motion sensor
Fixed calibration photoresistor

Design 3


Barcode scanner
Roller
Lightsource
Empty
Fixed calibration photoresistor

Design 4



Lightsource

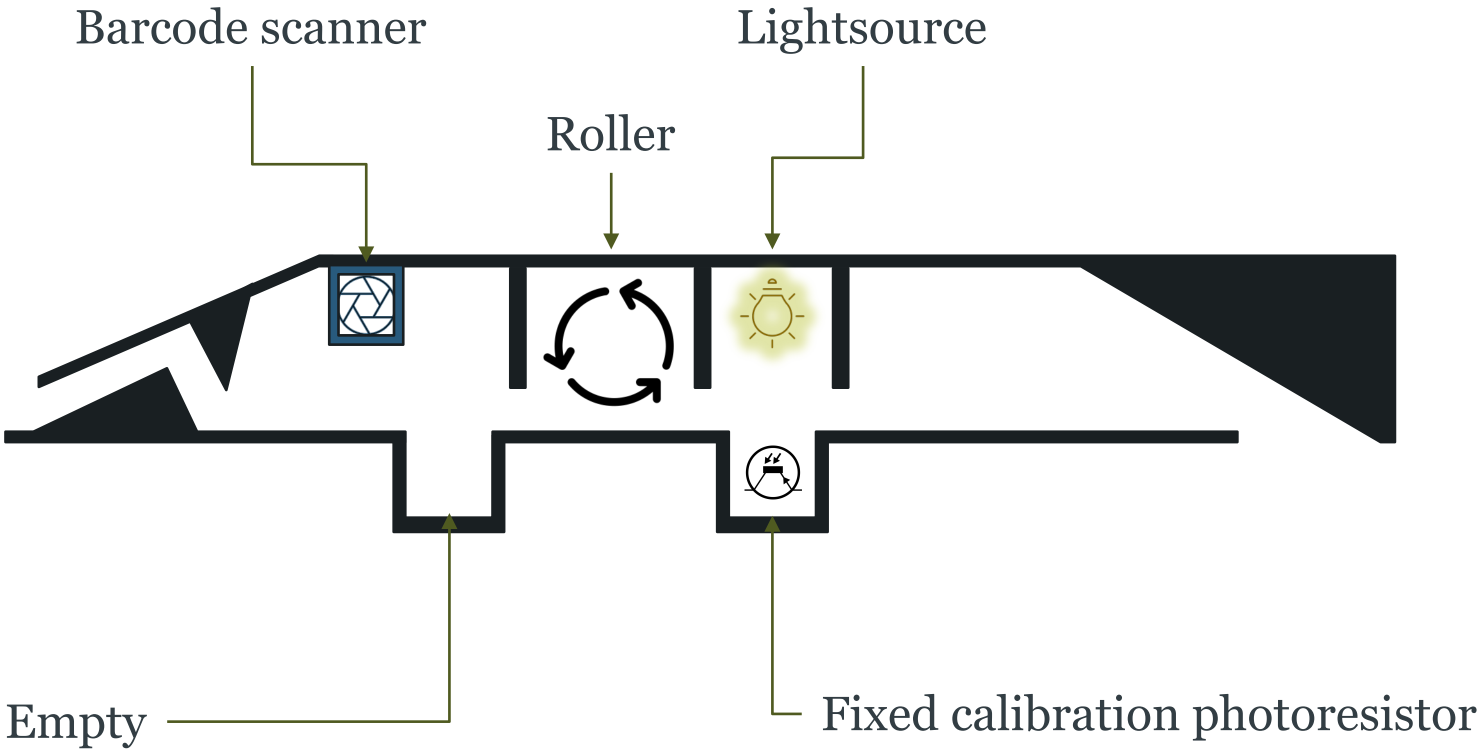
Roller

Barcode scanner

Fixed calibration photoresistor

Empty

Design 5


Barcode scanner
Lightsource
Roller
Empty
Fixed calibration photoresistor

Thank you

Questions?