

HD-Sec: Holistic Design of Secure Systems on Capability Hardware

<https://hd-sec.github.io>

Asieh Salehi, Robert Thorburn, Dana Dghaym, Michael Butler, Thai Son Hoang, Leonardo Aniello, Vladimiro Sassone
University of Southampton, UK {a.salehi-fathabadi, r.h.thorburn , d.dghaym, m.j.butler, t.s.hoang, l.aniello, vsassone}@soton.ac.uk

DSbD

Digital Security by Design



University of
Southampton

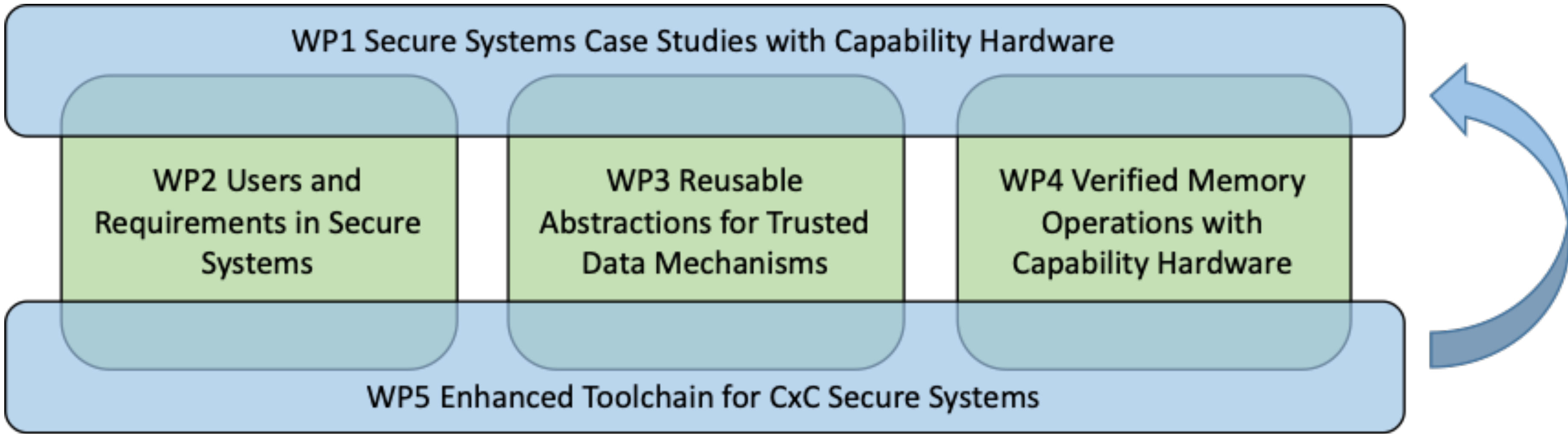


Engineering and
Physical Sciences
Research Council

Overview

Transformation of security-critical software development

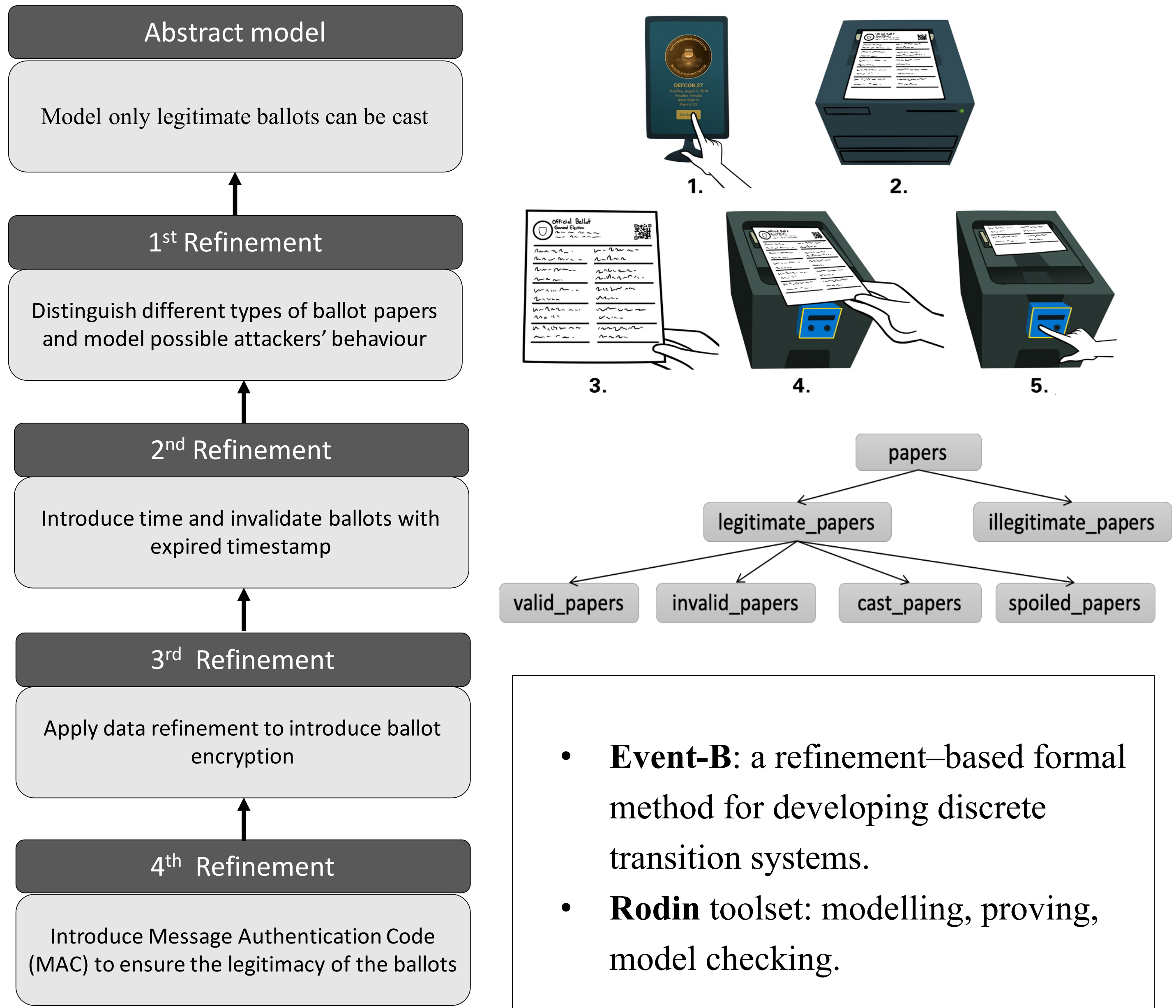
- From an expensive iterative test-and-fix approach
 - To a correctness-by-construction (CxC) approach
- The design of software from requirements to implementation:
 - Formal modelling, Reusable formal abstractions
 - Verification
 - Model transformation
 - CxC tools and running on capability hardware



Formal Modelling and Verification

Case Study: Smart Ballot Box¹ (SBB)

- **Confidentiality** : using encryption of the voter's choices.
- **Integrity**: to only accept valid ballots and reject invalid ballots.
- **Availability**: is guaranteed by not preventing a voter from casting a valid ballot.



- **Event-B**: a refinement-based formal method for developing discrete transition systems.
- **Rodin** toolset: modelling, proving, model checking.

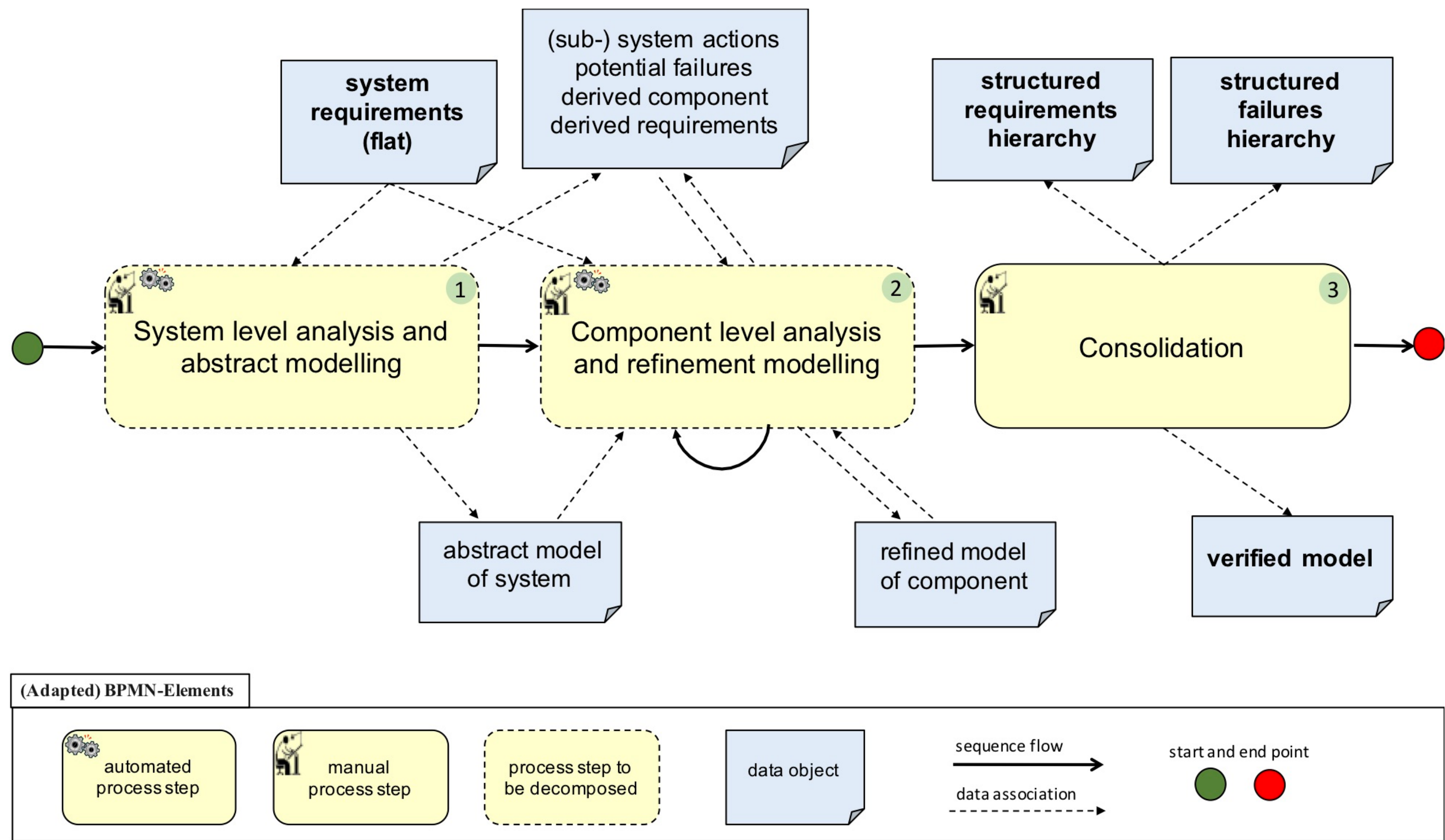
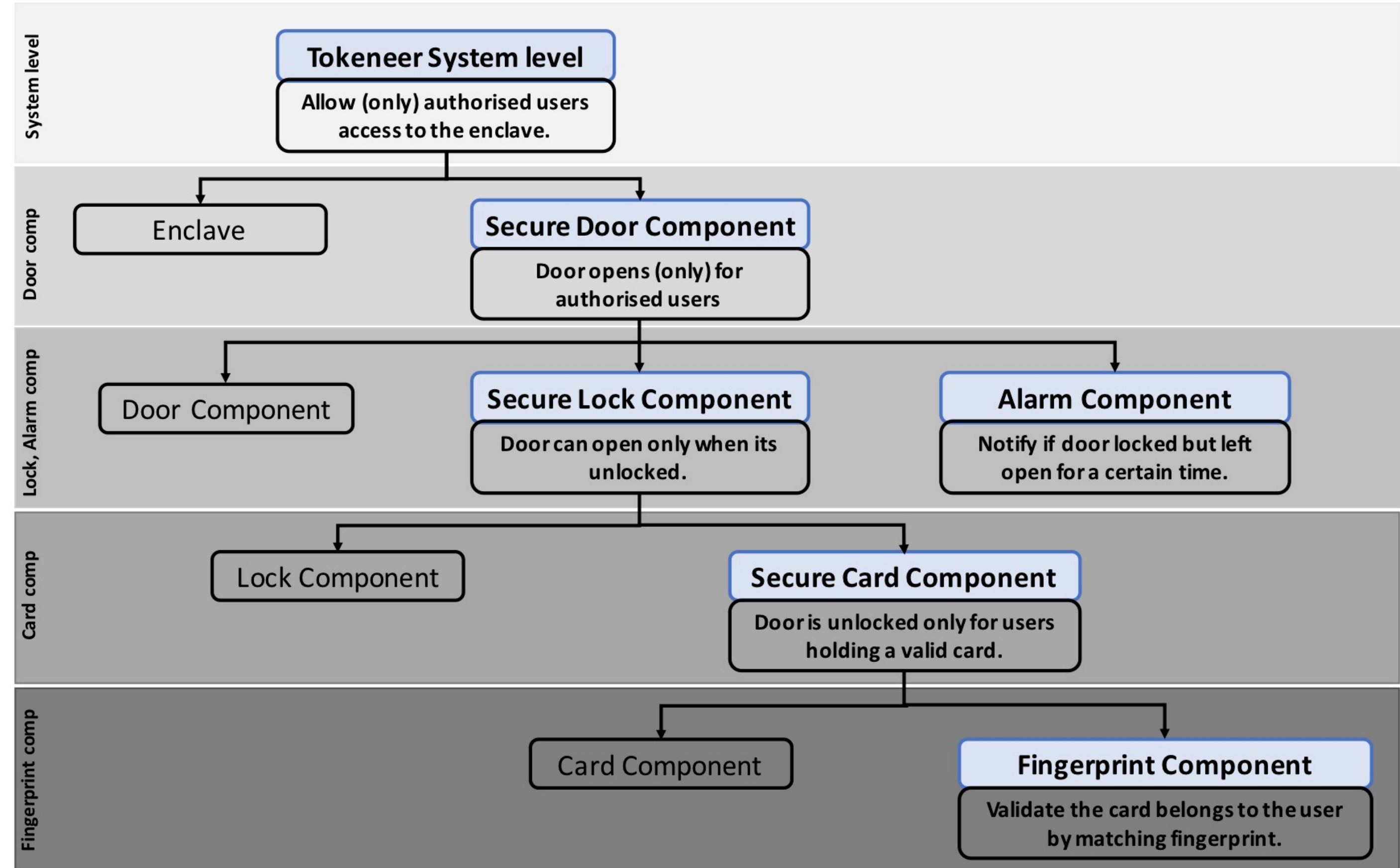
From Event-B to SPARK - Ada Implementation

```
procedure cast(paper : in barcode) with
Global => (Proof_In => (MACKEY, spoiled_arr, curr_time),
In_Out => (cast_arr, vote_count)),
Pre => ( already_cast(paper) = False
and then already_spoiled(paper) = False
and then valid_time (paper) = True
and then validate_barcode(paper) = True
and then vote_count < Max_Votes),
Post => (already_cast(paper)
and vote_count = vote_count' old + 1);
```

SHARCS: Systematic Hierarchical Analysis of Requirements for Critical Systems

Case Study: Tokeneer²

- **Security**: to prevent unauthorized access to the Secure Enclave.
- **Availability**: to allow authorized user entering the Enclave.

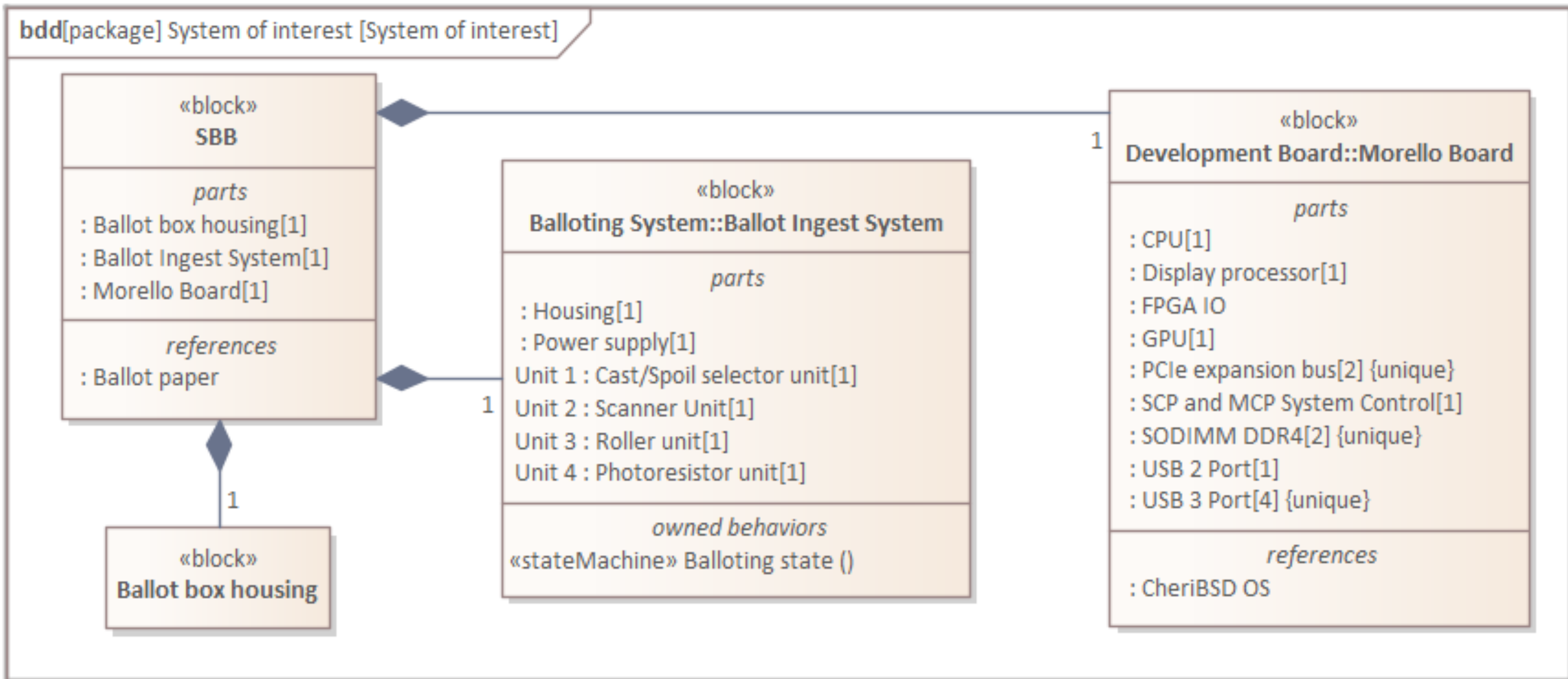


The Morello Fixed Virtualisation Platform (FPV)

- Testing and development in preparation of hardware
- Currently supports CheriBSD, Android, and Linux
- Linux development with capability pointers

Proceeding to hardware testing

- Integrating physical Morello board and test rig
- Testing functionality, cybersecurity, and physical security



References

- [1] Galois and Free & Fair. The BESSPIN Voting System (2019).
- [2] Praxis: Tokeneer. <https://www.adacore.com/tokeneer> (2022).
- [3] D. Dghaym, T.S. Hoang, M. Butler, R. Hu, L. Aniello, V. Sassone (2021) Verifying System-level Security of a Smart Ballot Box. In ABZ 2021- 8th International Conference on rigorous State Based Methods.

Requirement Interchange Specification

- Governs the interaction between SysML and Event-B models
- Iterative improvement potentially ending in code generation
- Ends in a loop as the process stays active across the system lifecycle

