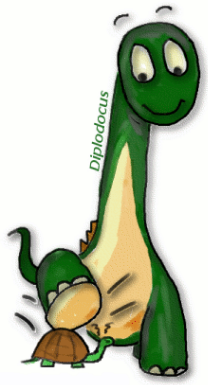
Security-Aware Modeling and Analysis for HW/SW Partitioning

Letitia W. Li, Florian Lugou, Ludovic Apvrille

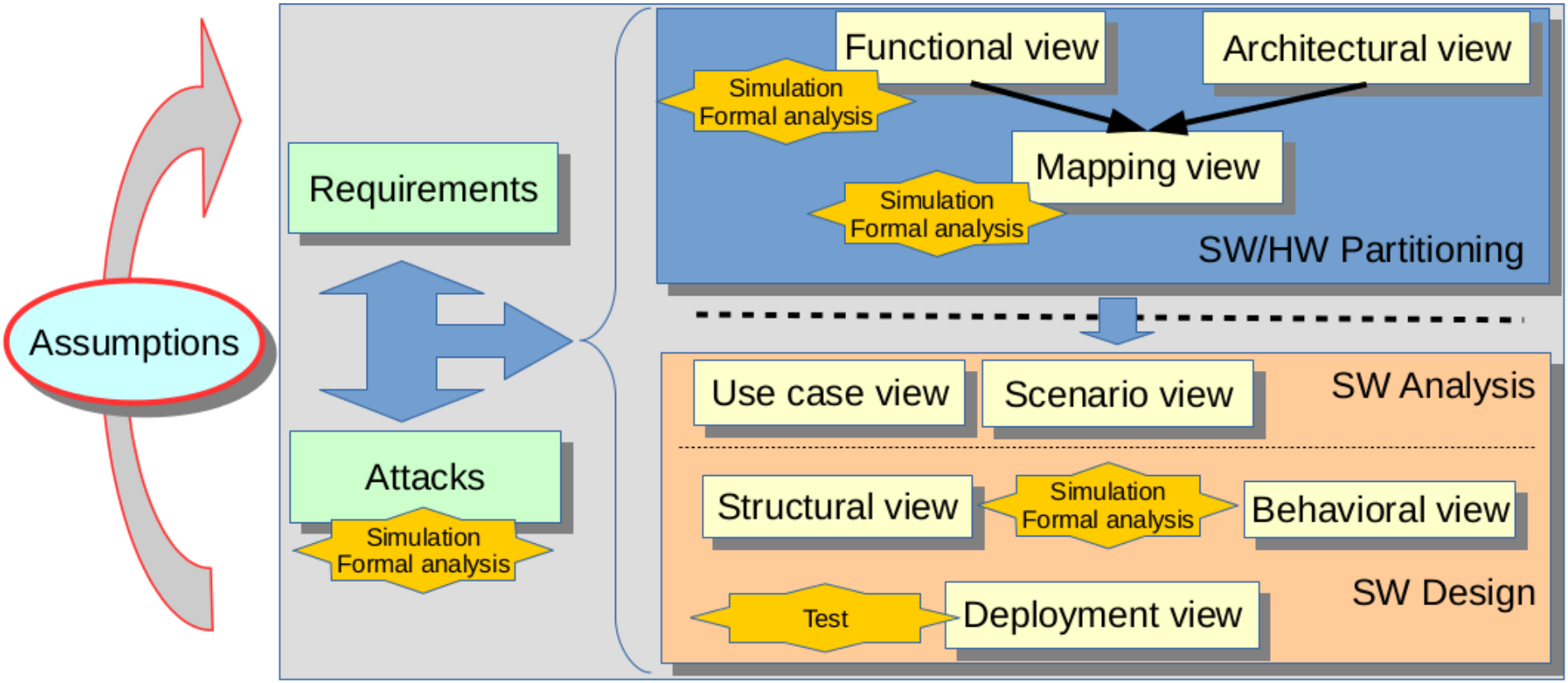
Embedded System Security

SysML-Sec Methodology

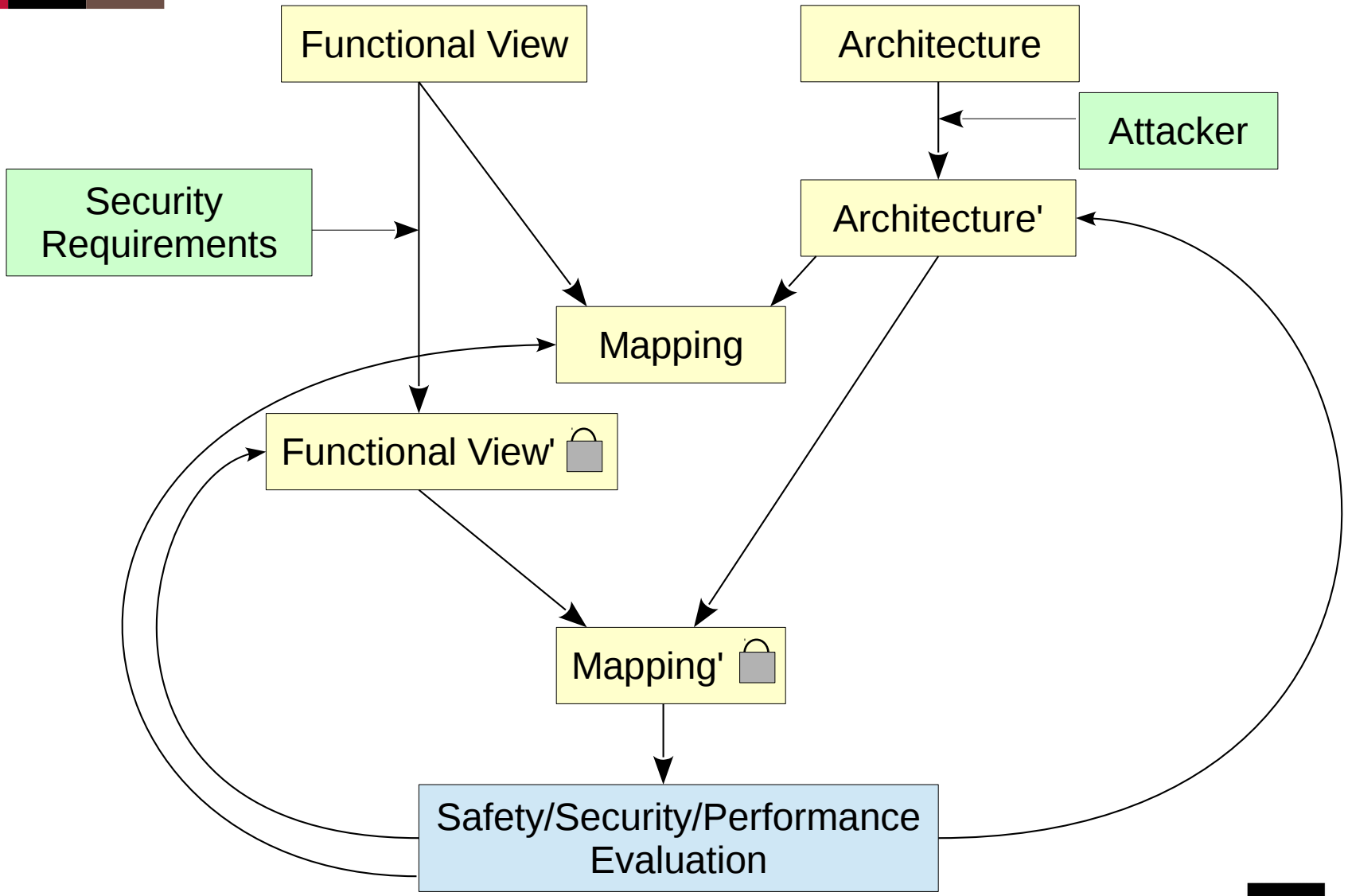


TTool

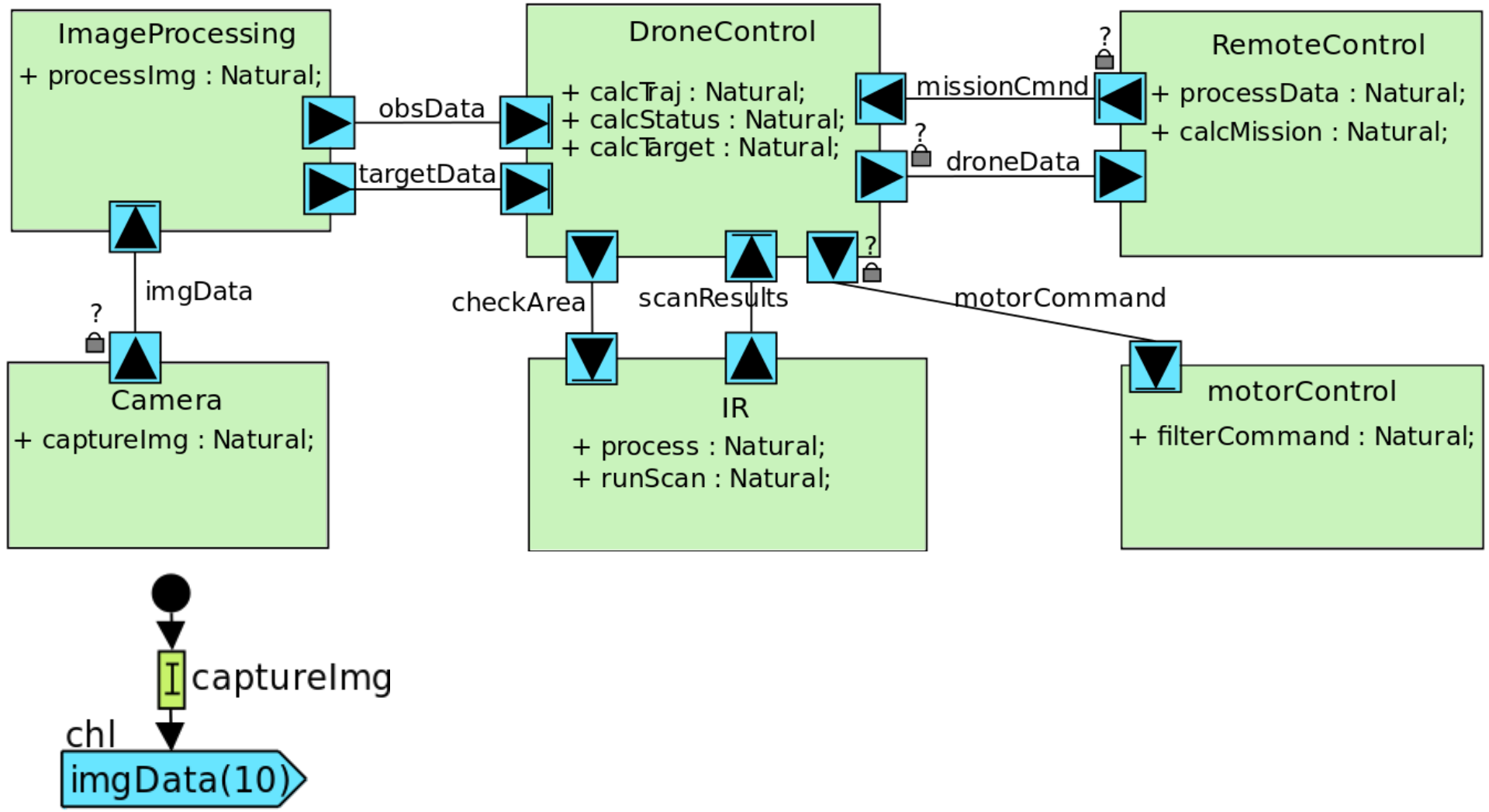
An open source toolkit provided by



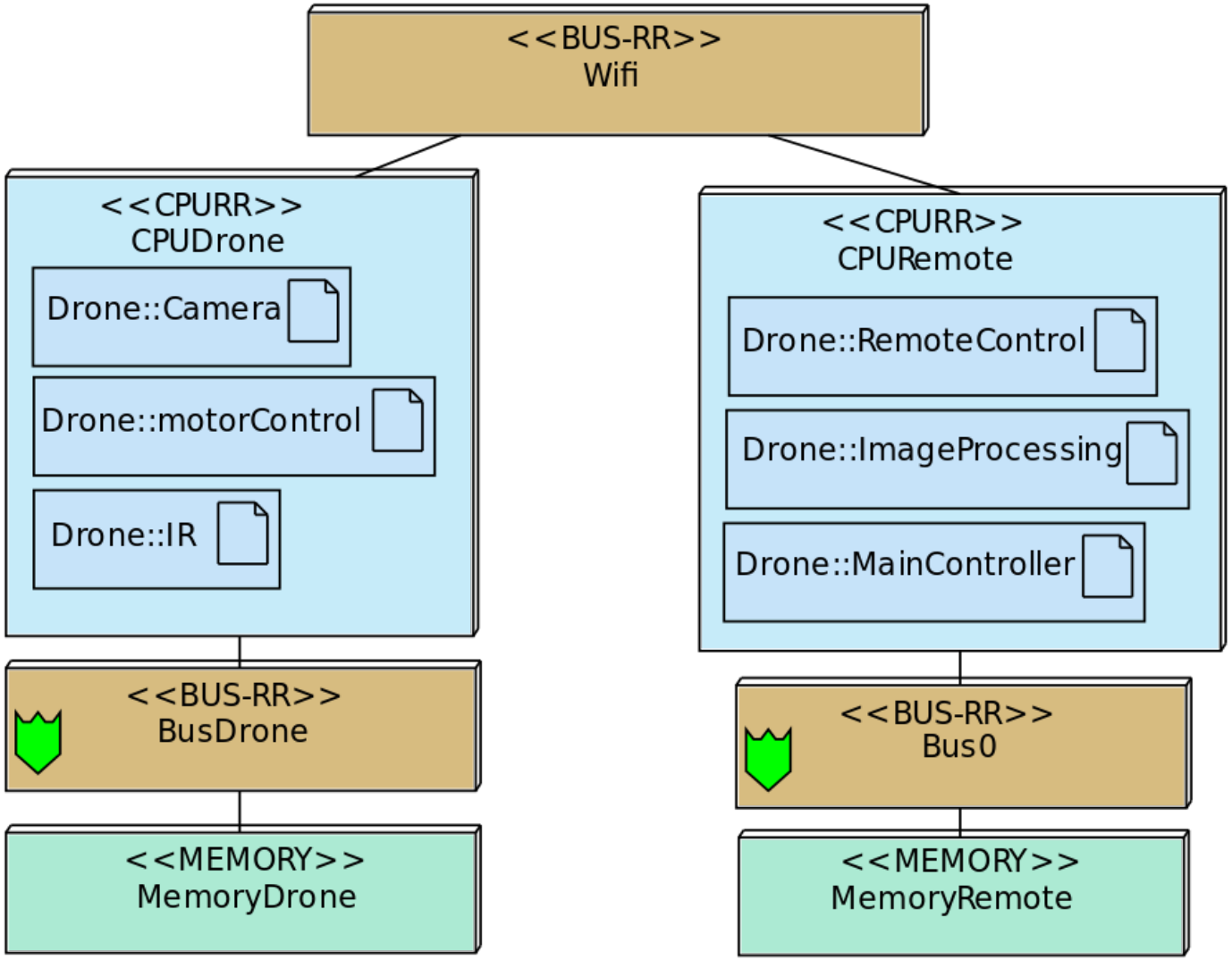
Secure HW/SW Partitioning



Drone Functional View



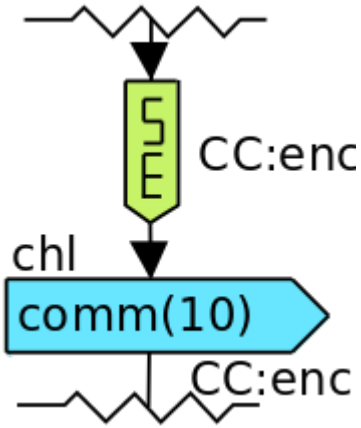
Drone Architecture

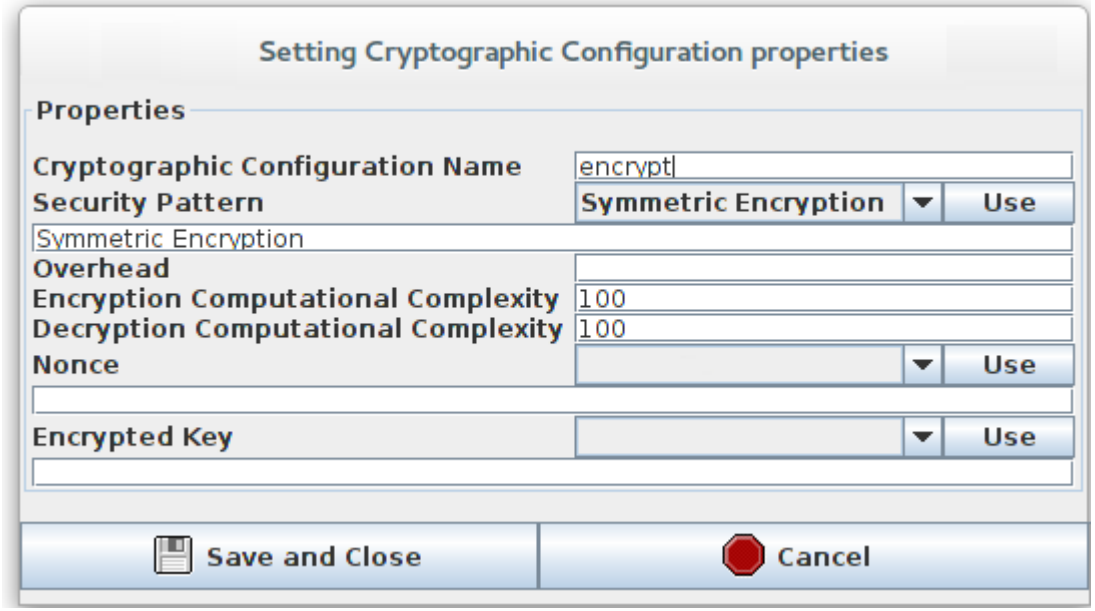


Security Mechanisms

Cryptographic Configurations

- Tag indicating presence of encryption
- Operate on tagged channel
- Occupies computation time in simulation

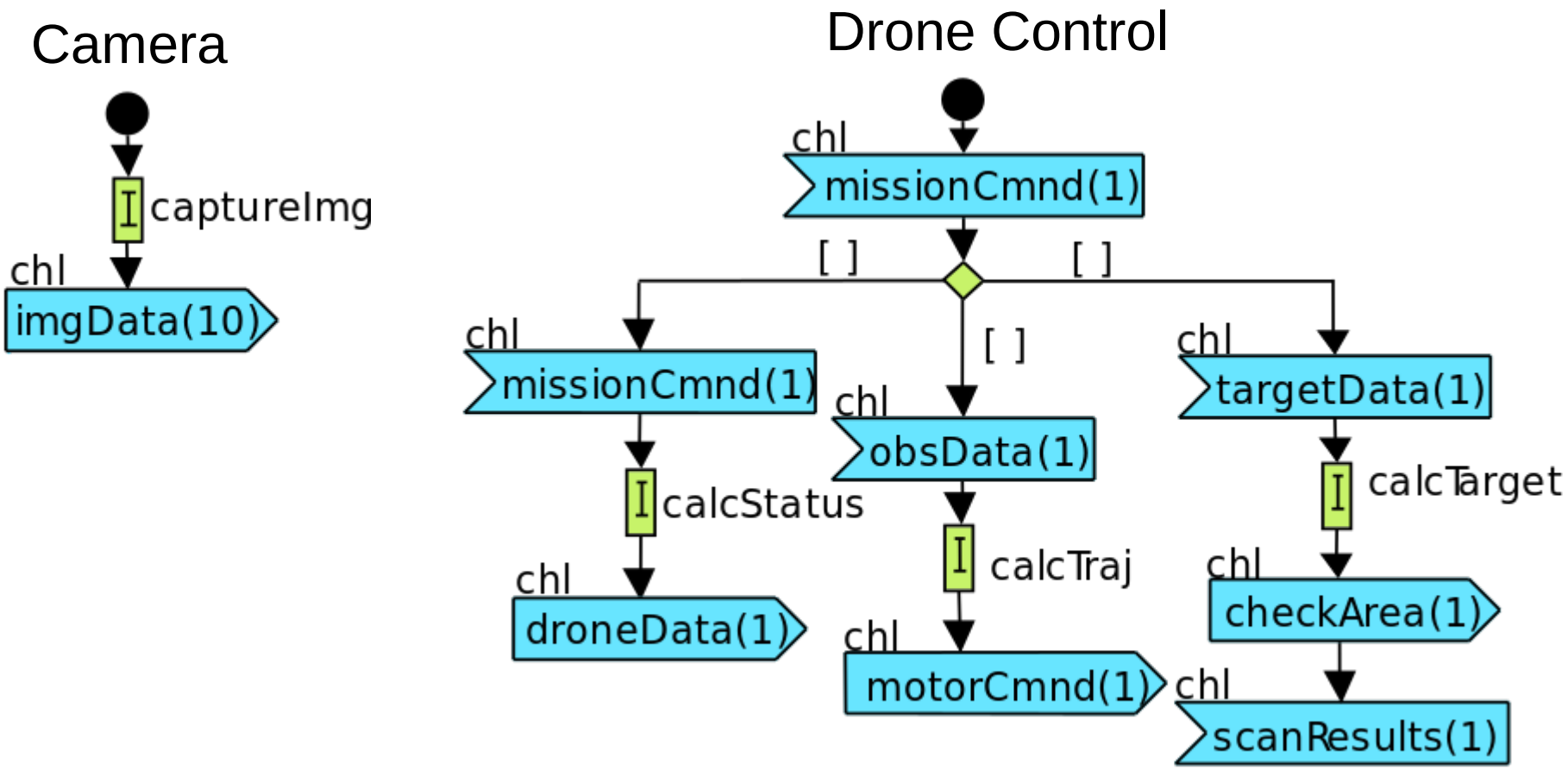




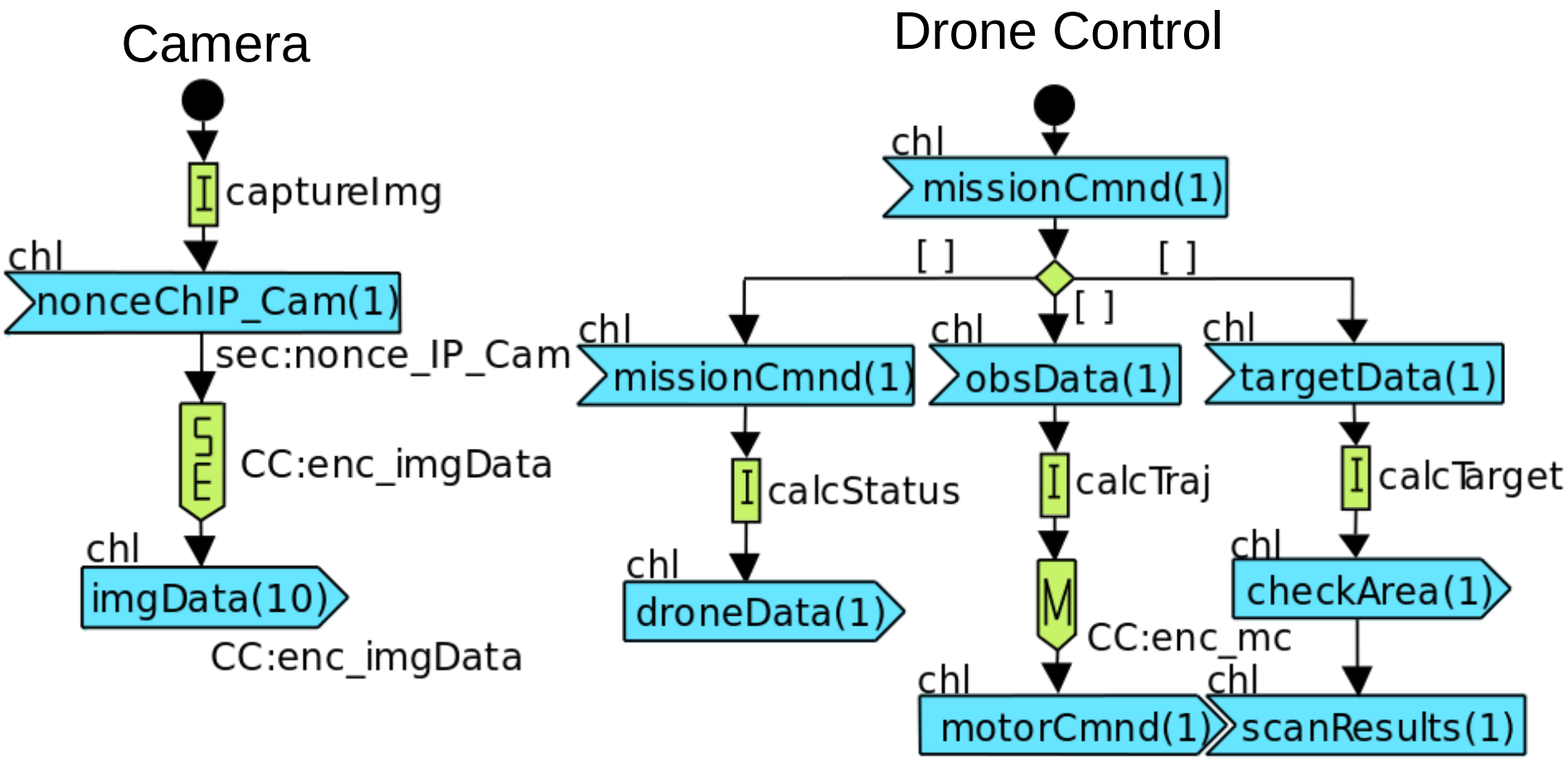
Automatic Generation

- Time-saving and convenient
- Suggestion of basic encryption for user to enhance
- Addition of Nonces, Encryption

Unsecured Model

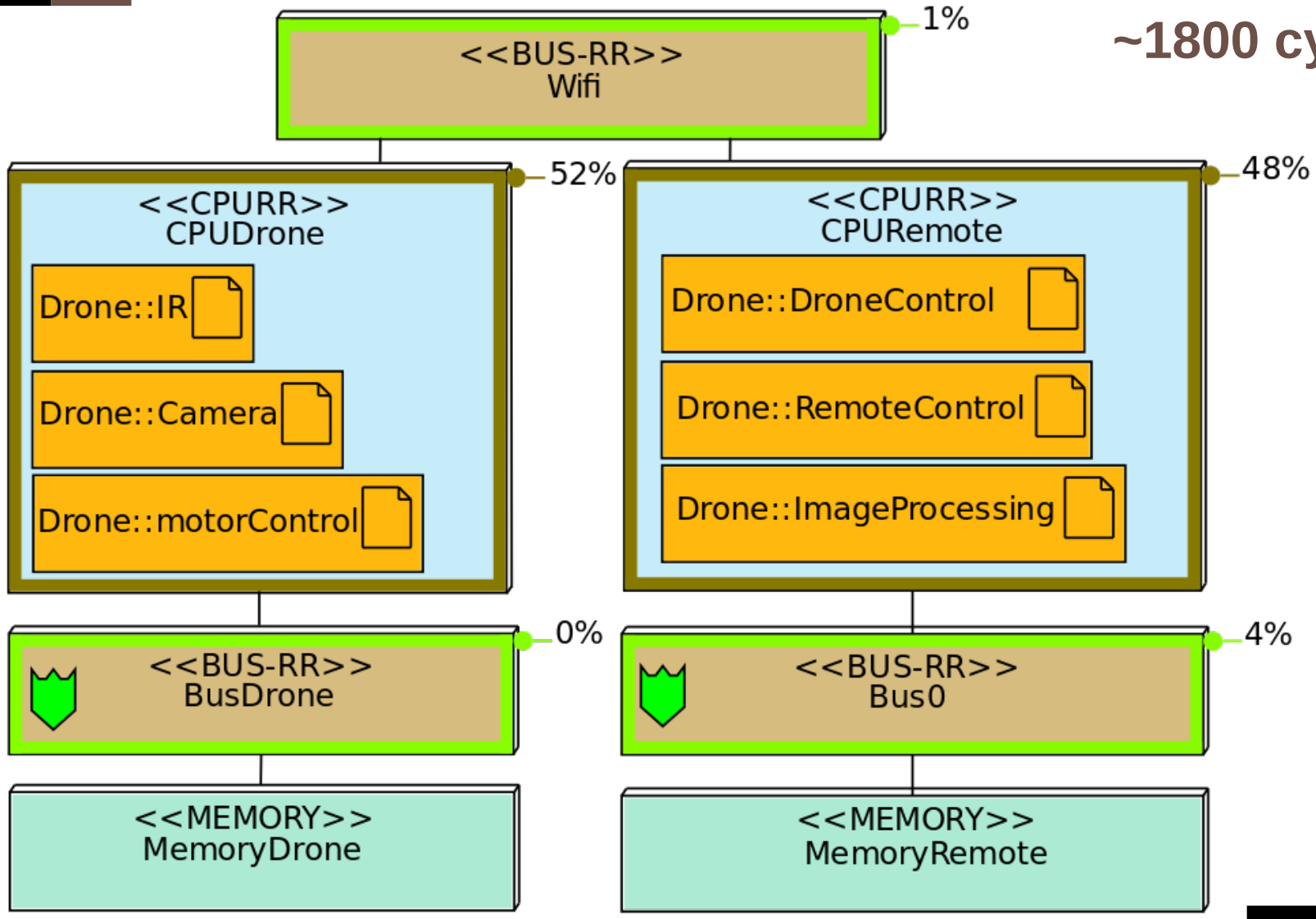


Secured Model



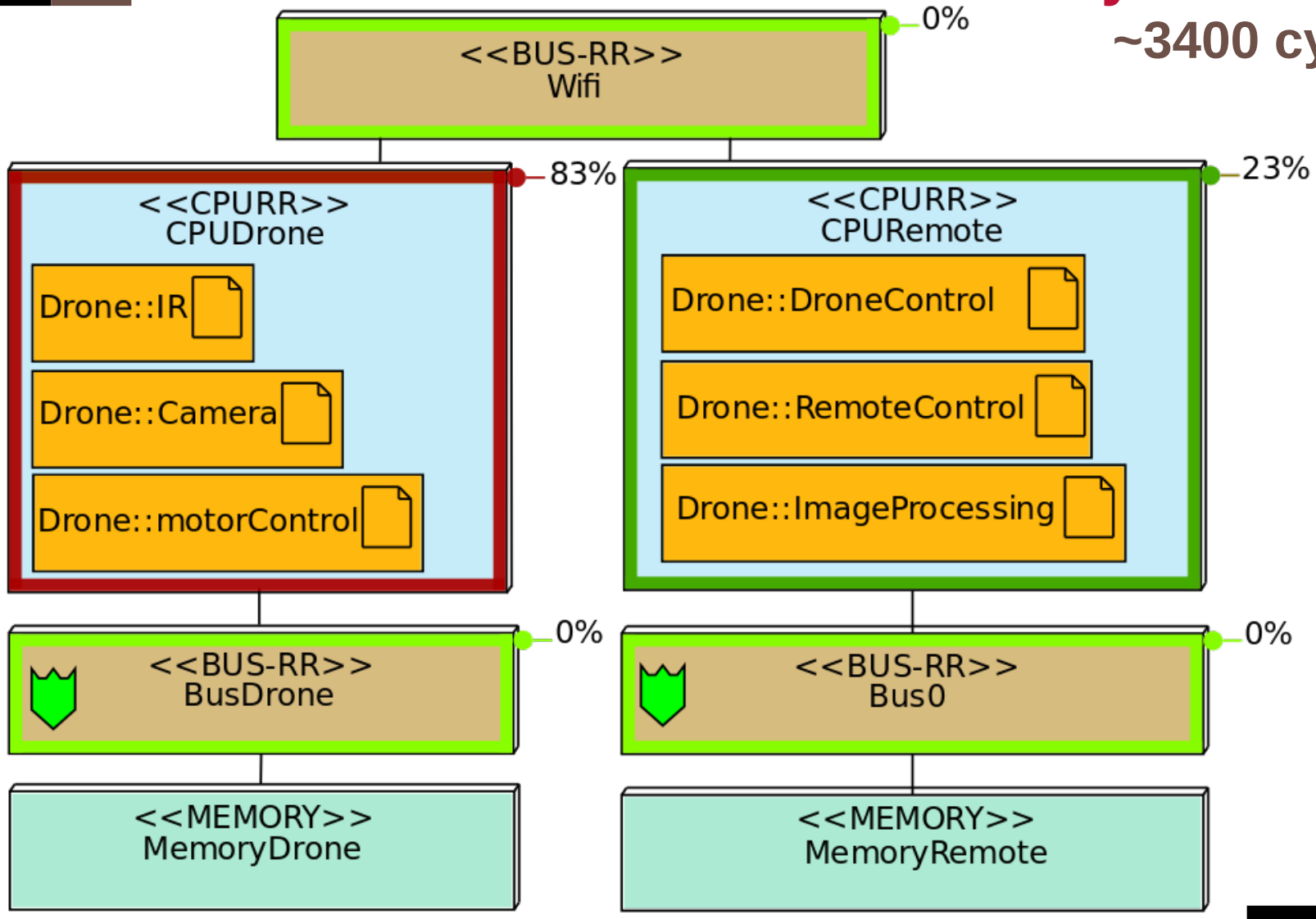
Performance

~1800 cycles



Performance with Added Security

~3400 cycles

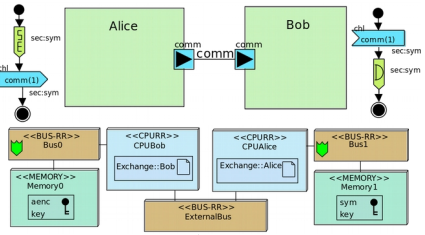


Security Analysis

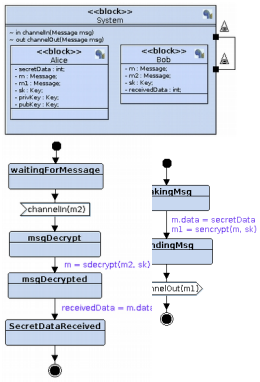
Model Transformation for Security

Lugou Modelsward2016

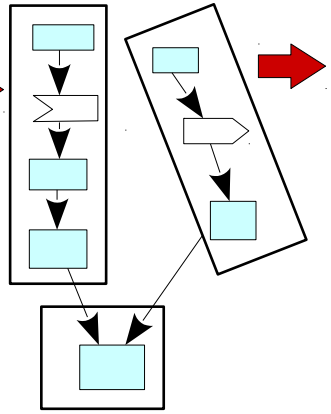
Mapping Model



Intermediate Specification



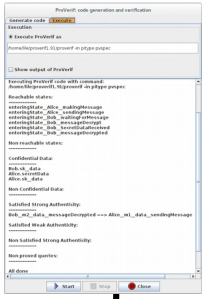
Basic Blocks



Proverif Code

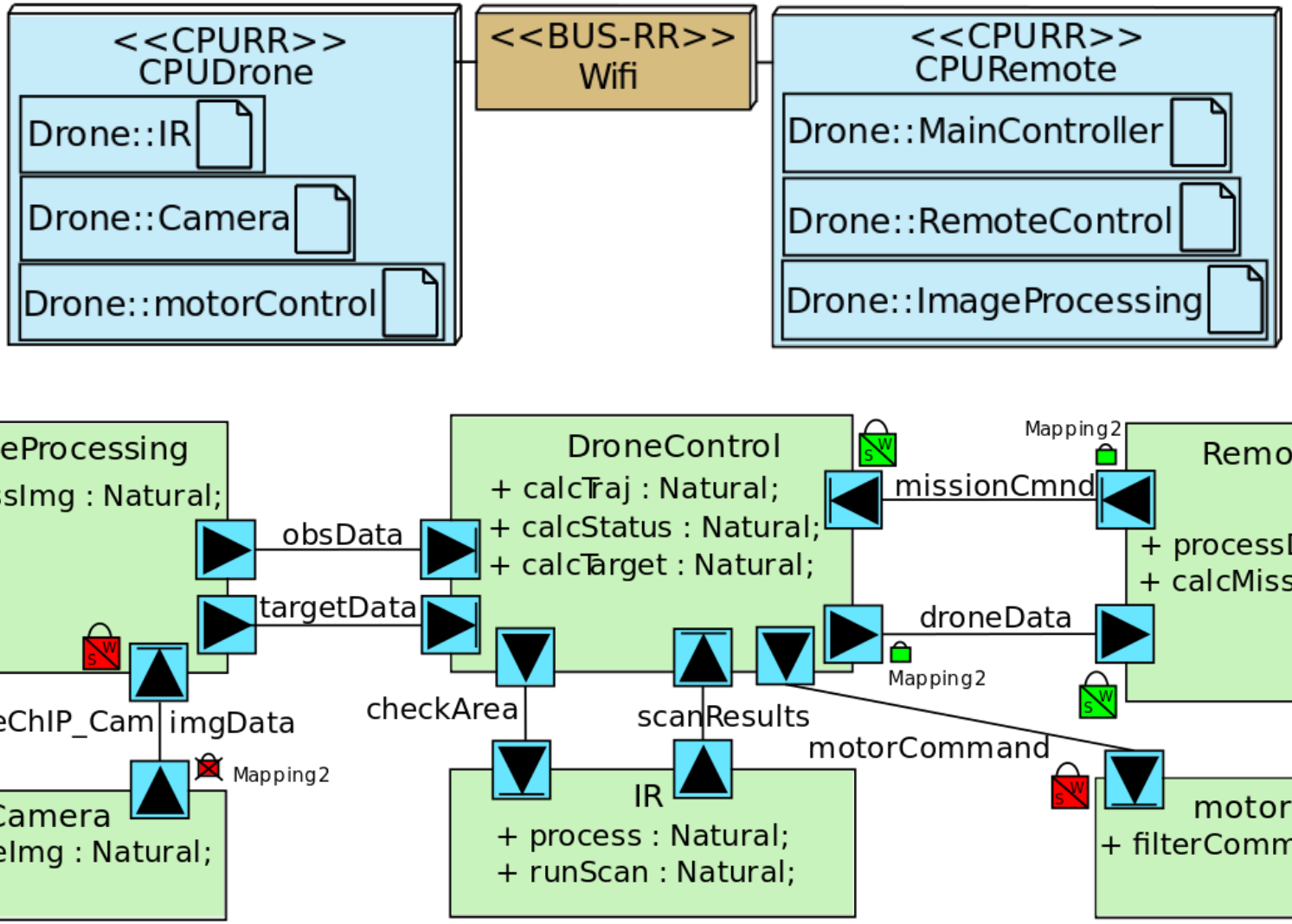
```
(* Generated ProVerif specification *)
(* Queries Secret *)
query attacker(new Alice__secretData).
(* Symmetric key cryptography *)
fun sencrypt (bitstring, bitstring): bitstring.
reduc forall x: bitstring, k: bitstring; sdecrypt
 (sencrypt (x, k), k) = x.
...
let Alice__0 (sessionID: bitstring) =
                    in (chControl, chControlData: bitstring);
                    let (=sessionID, =call__Alice__0,
                    Alice__secretData__1:
...
process
                    ! ( new sessionID: bitstring;((
                    System__0 (sessionID)
                    ) | (
                     Bob__0 (sessionID)  ) | ( Alice__0 (sessionID
                    )) | ((
                    new Alice__sk__data: bitstring;
...
```

Results

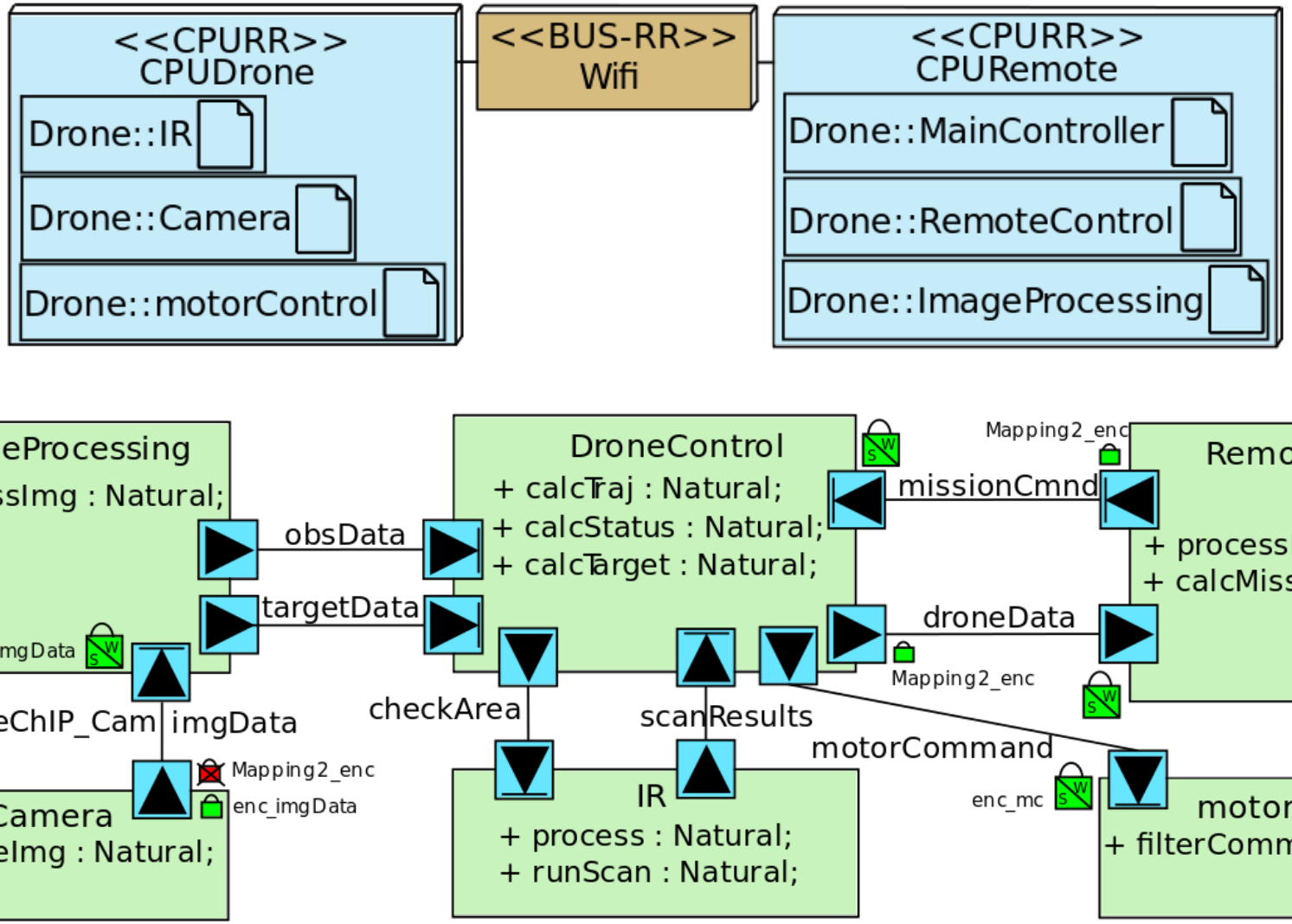


Backtracing to diagrams

Verification of model



Verification of Secured Model



Conclusion

- Modeling and verification of secure architectures
- Evaluation of security and impact of security on performance
- Automatic generation to secure critical communication
- Future support of code integrity, firewalls...

Our work at:

ttool.telecom-paristech.fr

sysml-sec.telecom-paristech.fr

Questions?