Security Modeling for Embedded System Design

Letitia W. Li, Florian Lugou, Ludovic Apvrille

GraMSec 2017

Security


ST. JUDE MEDICAL
Sylmar, CA USA
ANTHEM RF
PM3212 DDDRV

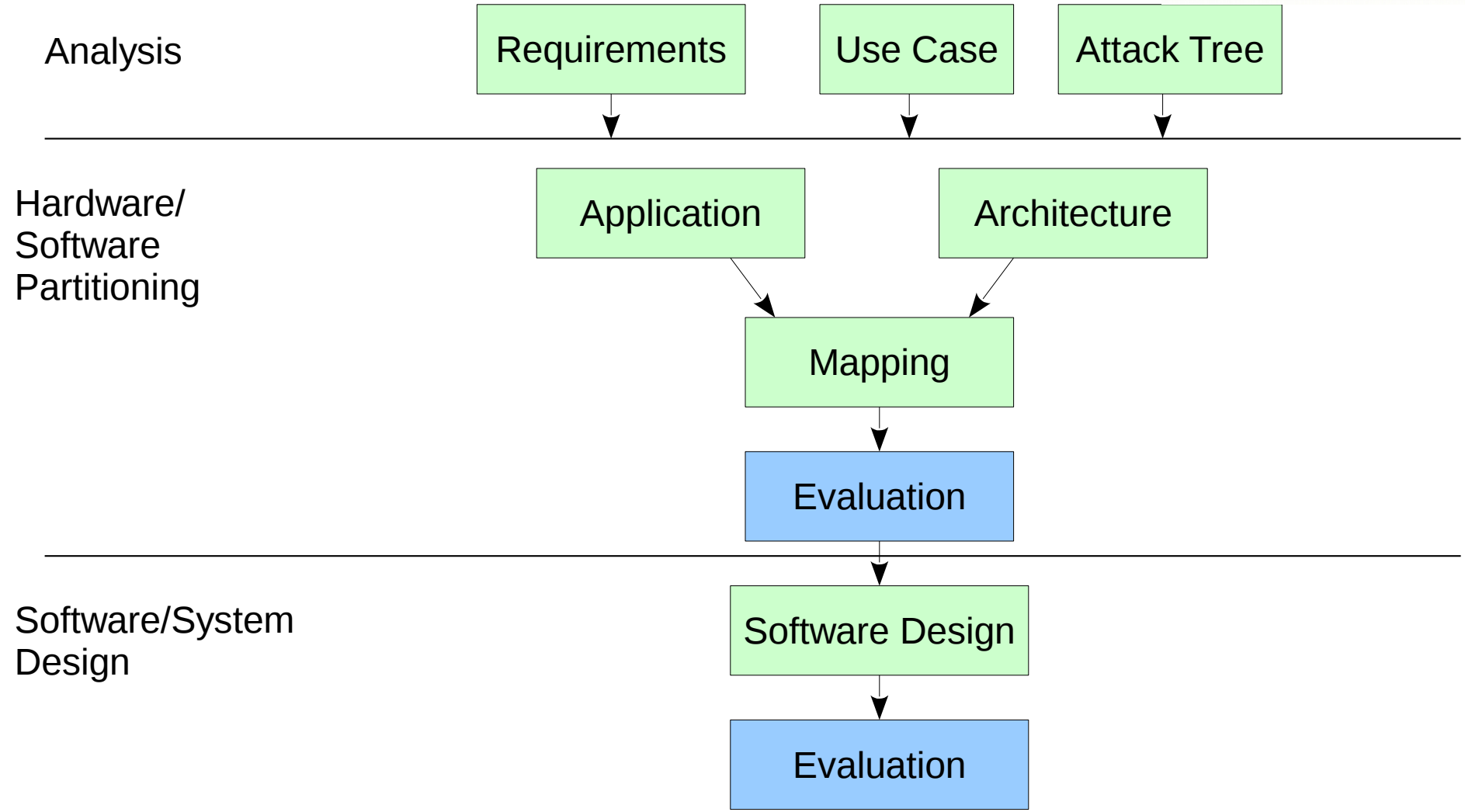

DIEBOLD
ELECTION SYSTEMS
Express Poll System Launcher


Hack into Multiple ECUs
Demonstrate the Unauthorized Xmas Show

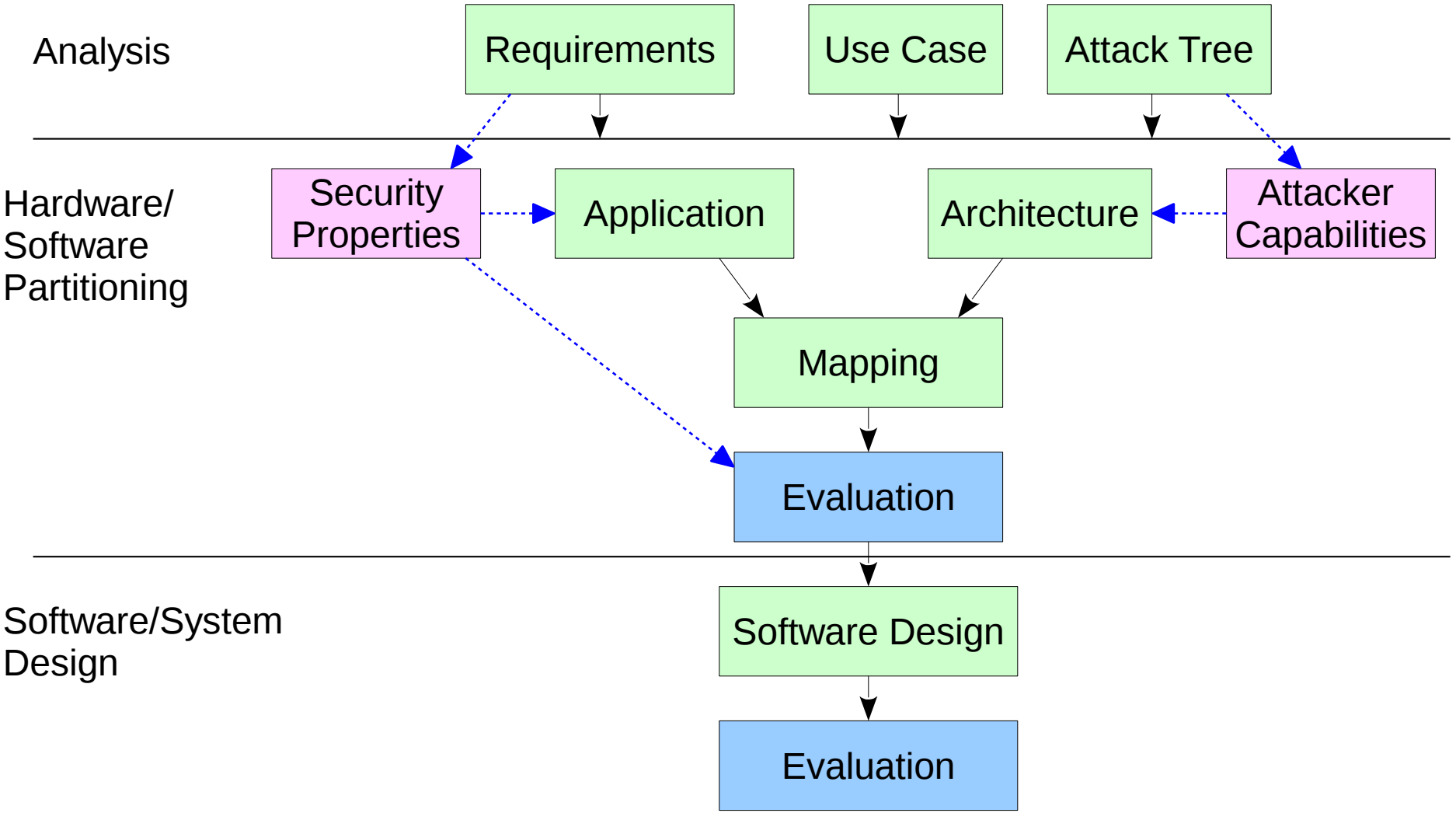
SysML-Sec Methodology

TTool

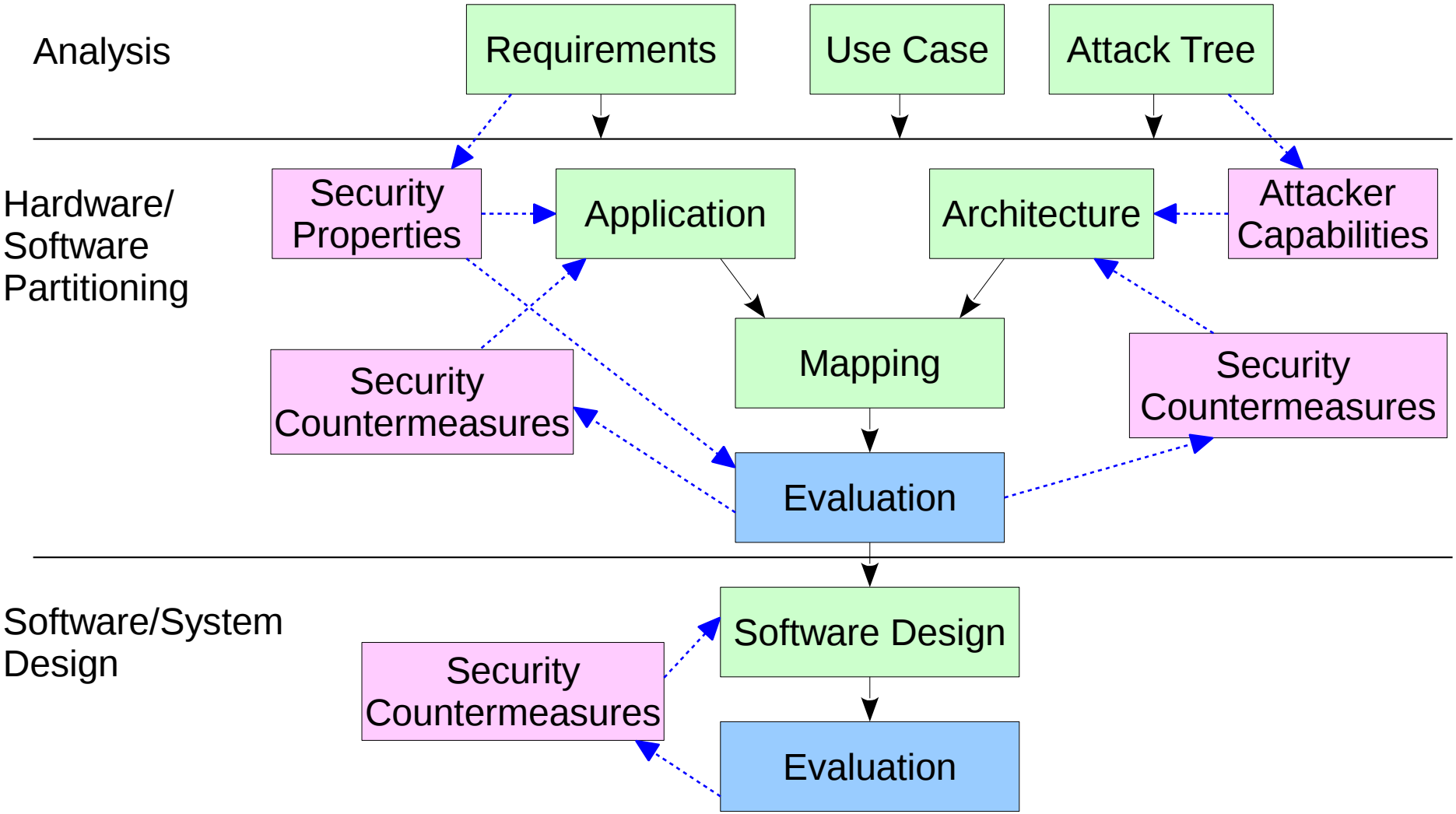
An open source toolkit provided by



Security Modeling

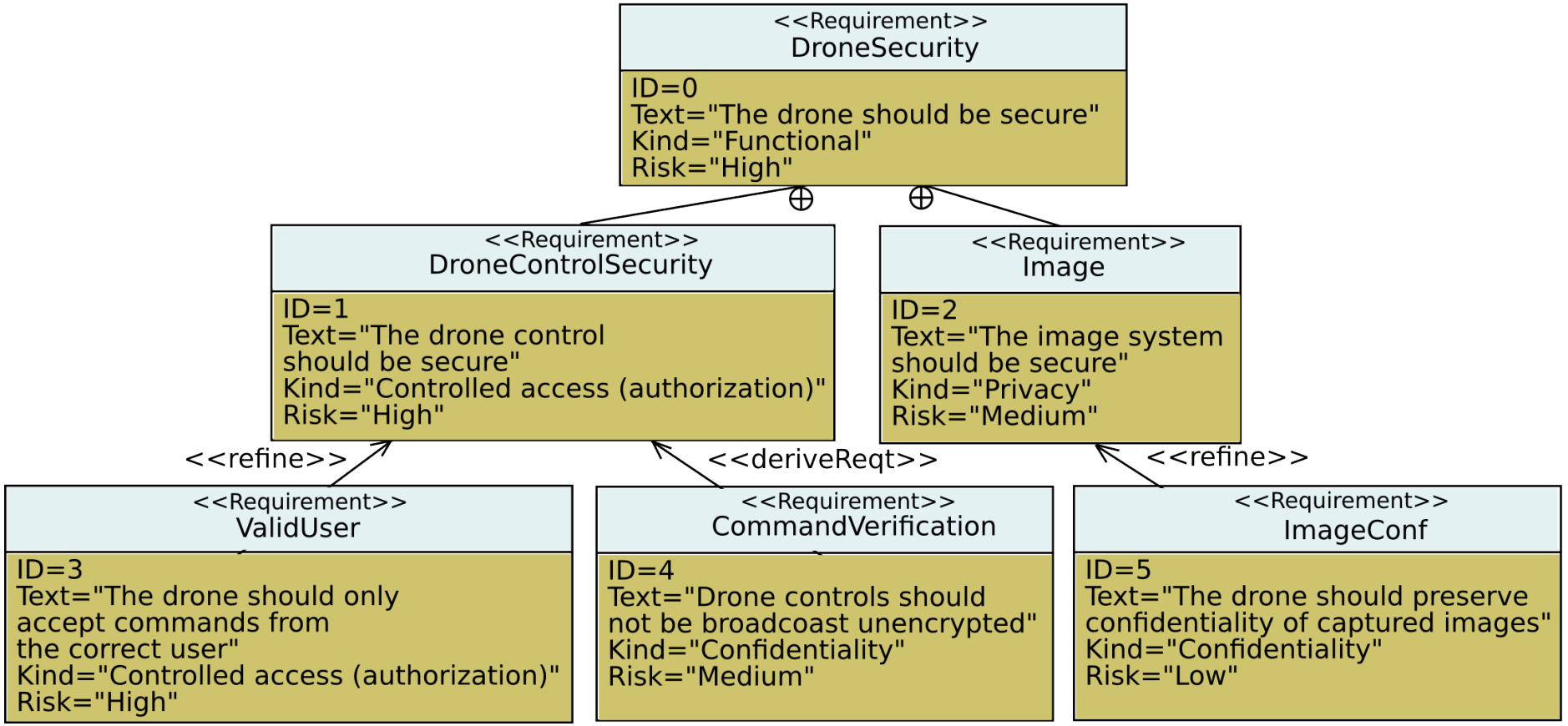


Security Modeling



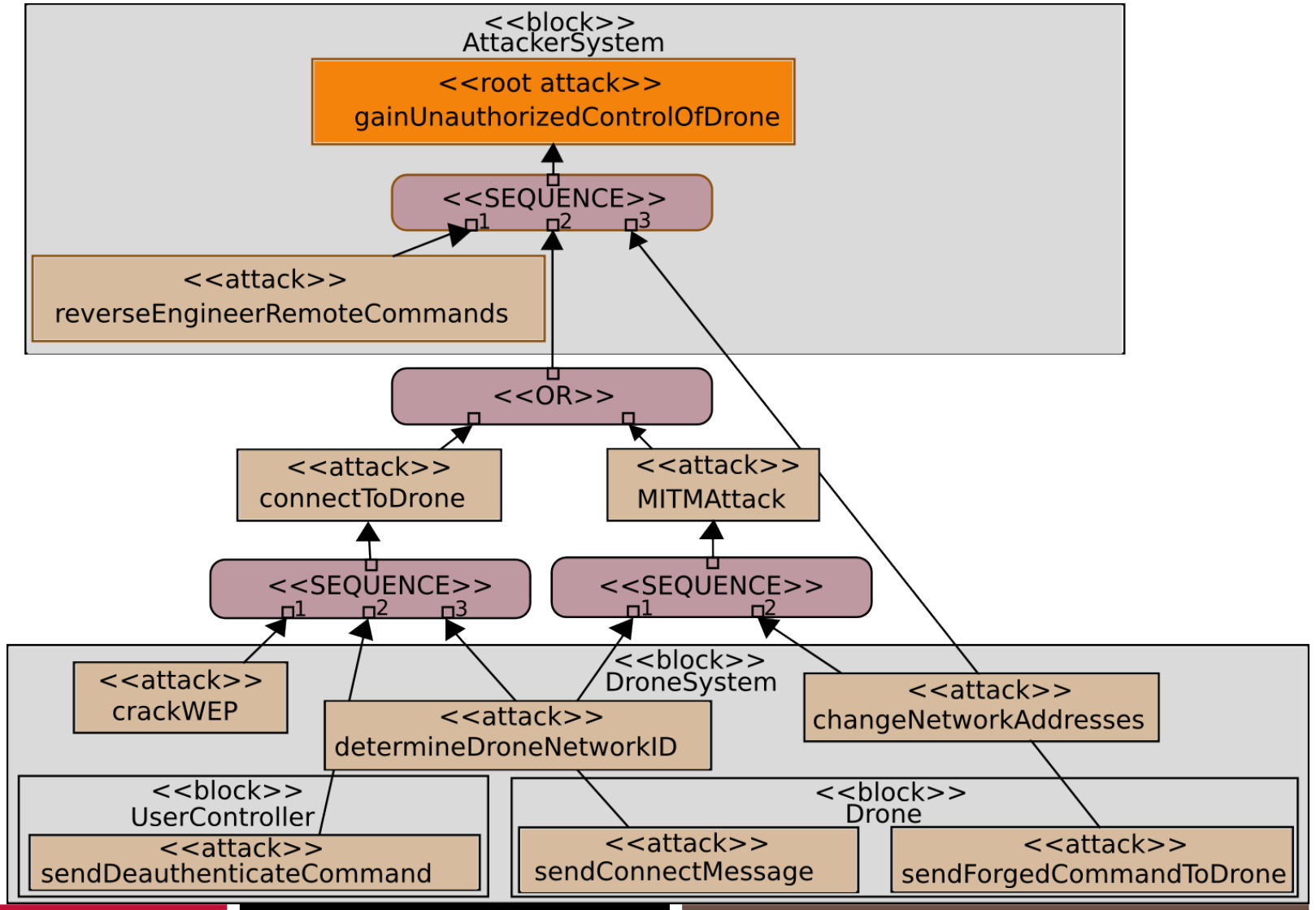
Analysis

Requirements



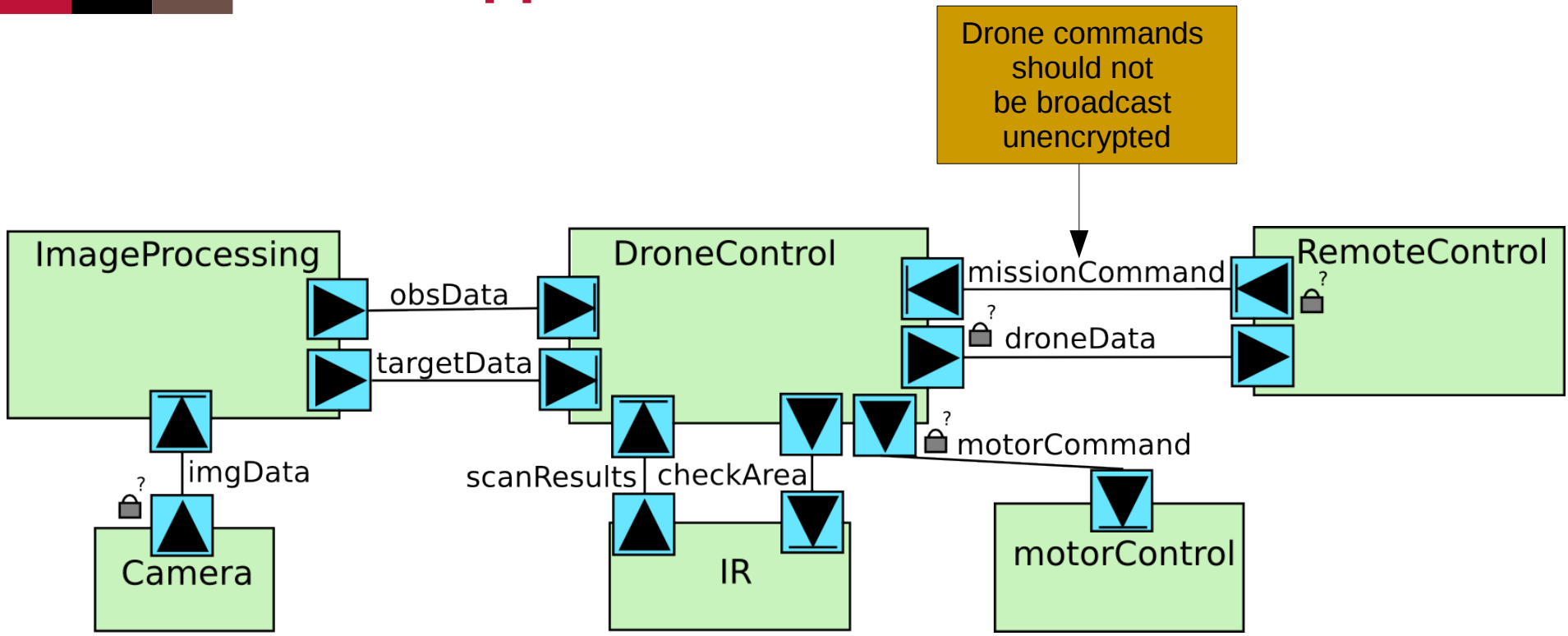
Attack Trees

Apvrille (GraMSec 2015)

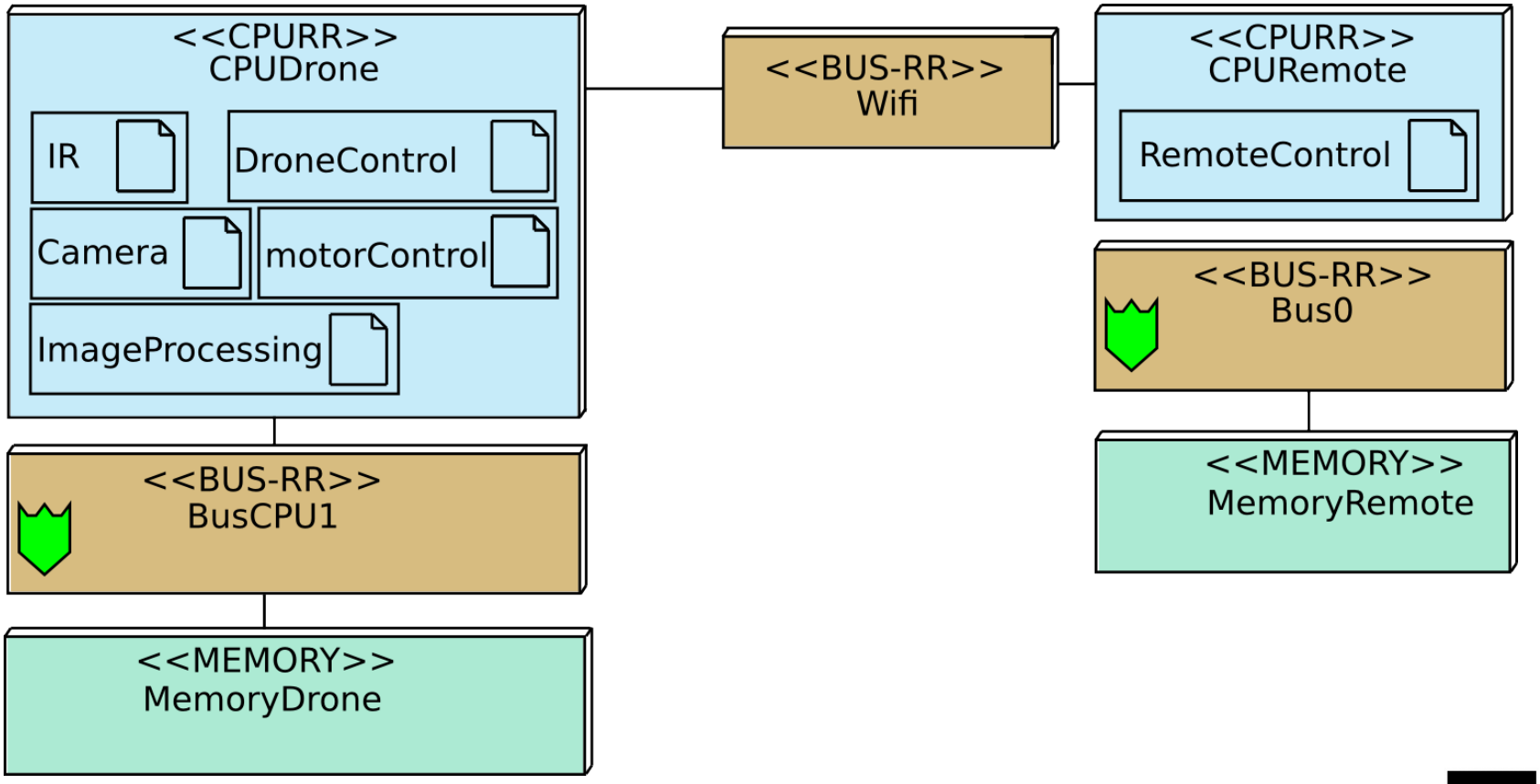


Hardware/Software Partitioning

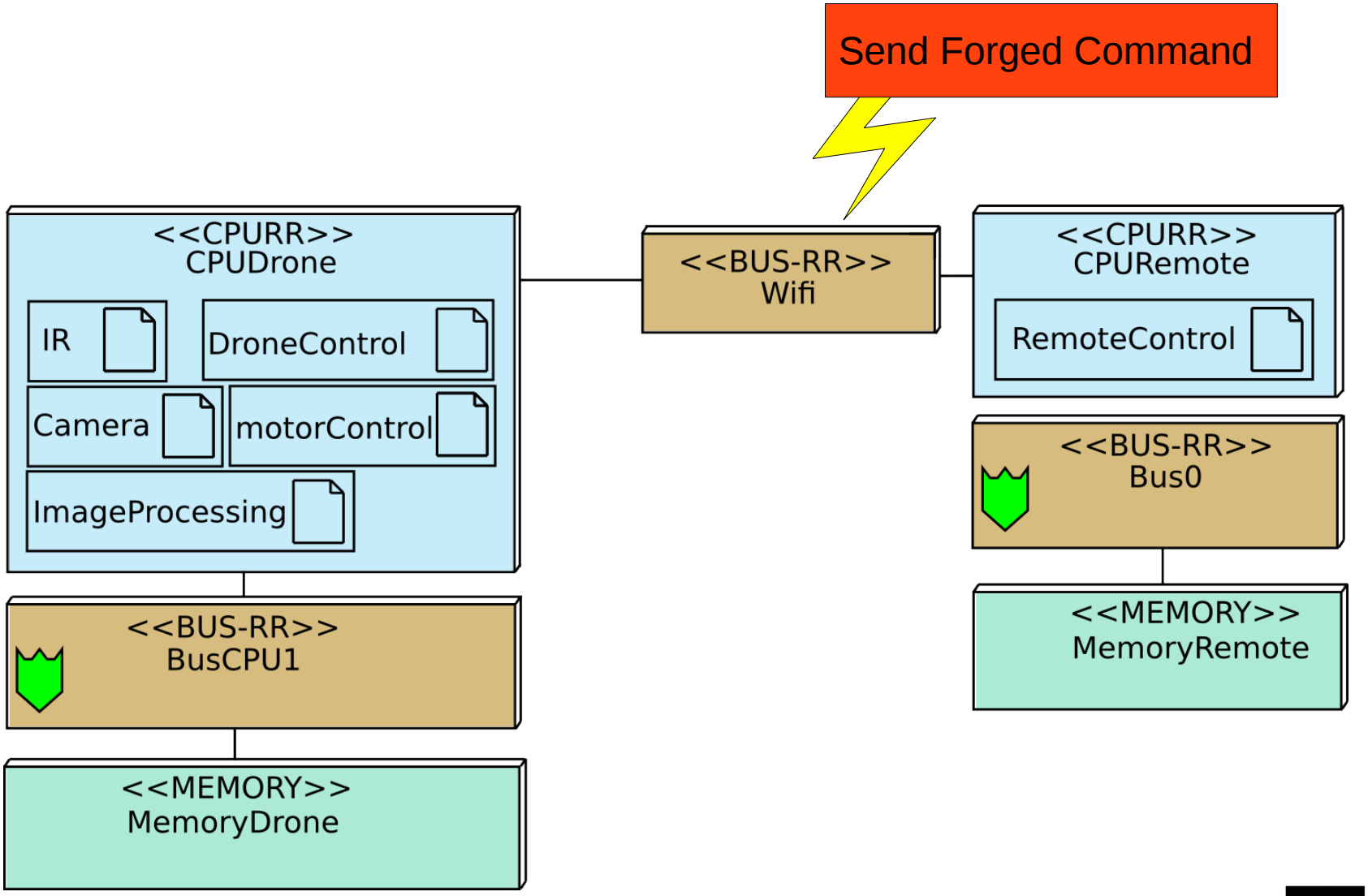
Drone Application



Drone Architecture/Mapping



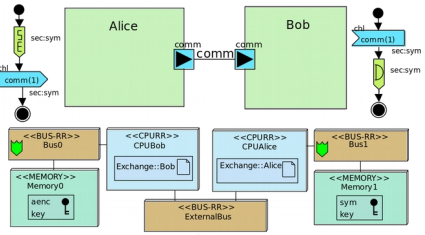
Drone Architecture/Mapping



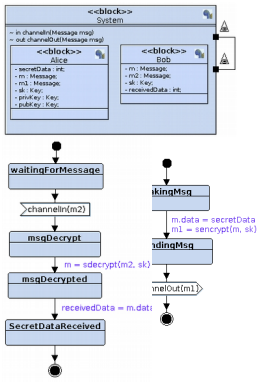
Model Transformation for Security

Lugou (Modelsward2016)

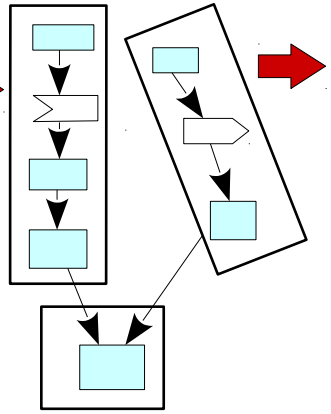
Mapping Model



Intermediate Specification



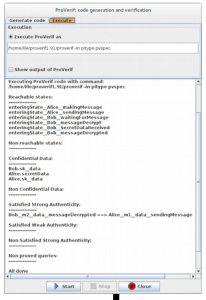
Basic Blocks



Proverif Code

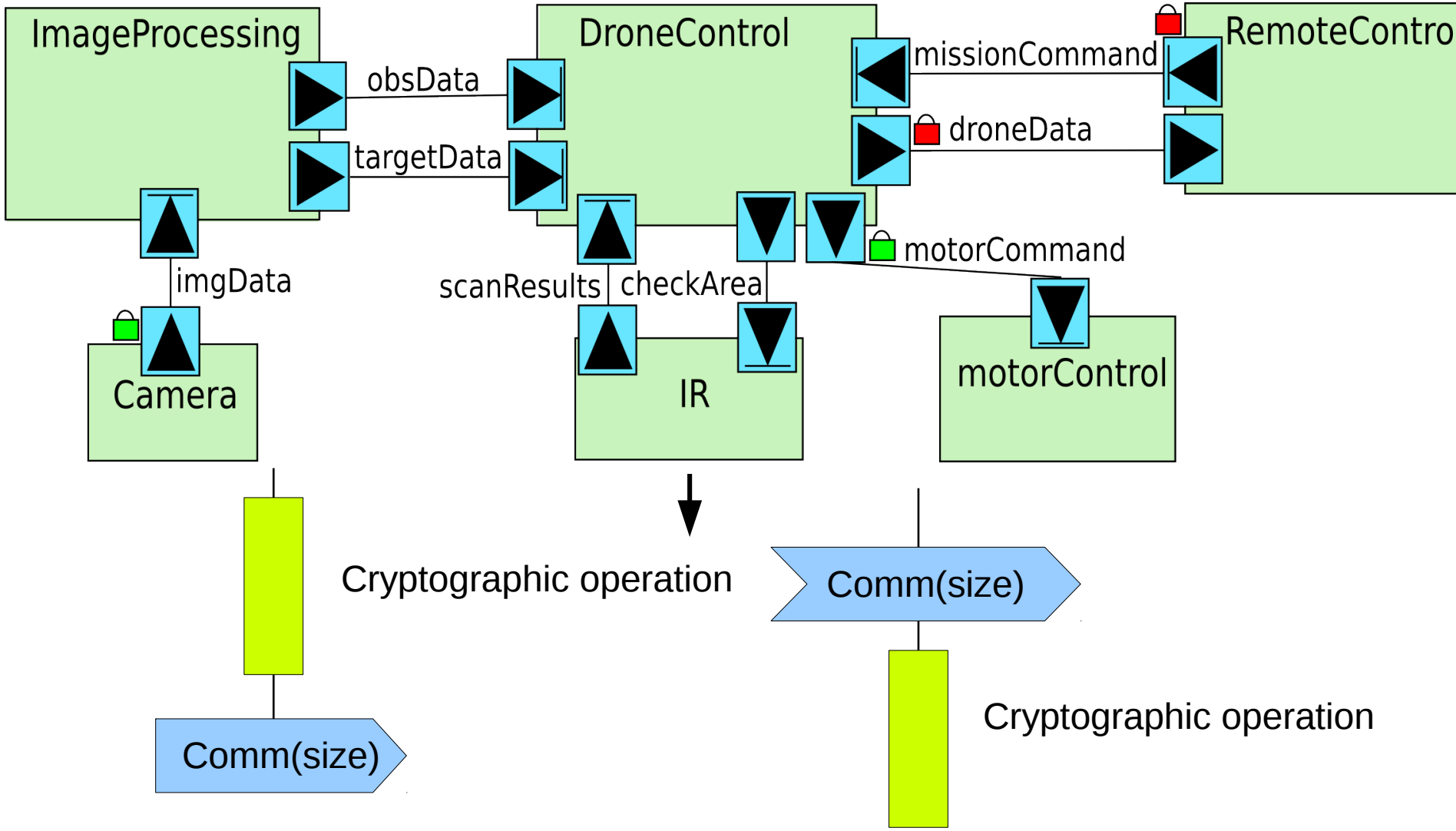
```
(* Generated ProVerif specification *)
(* Queries Secret *)
query attacker(new Alice__secretData).
(* Symmetric key cryptography *)
fun sencrypt (bitstring, bitstring): bitstring.
reduc forall x: bitstring, k: bitstring; sdecrypt
 (sencrypt (x, k), k) = x.
...
let Alice__0 (sessionID: bitstring) =
                    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



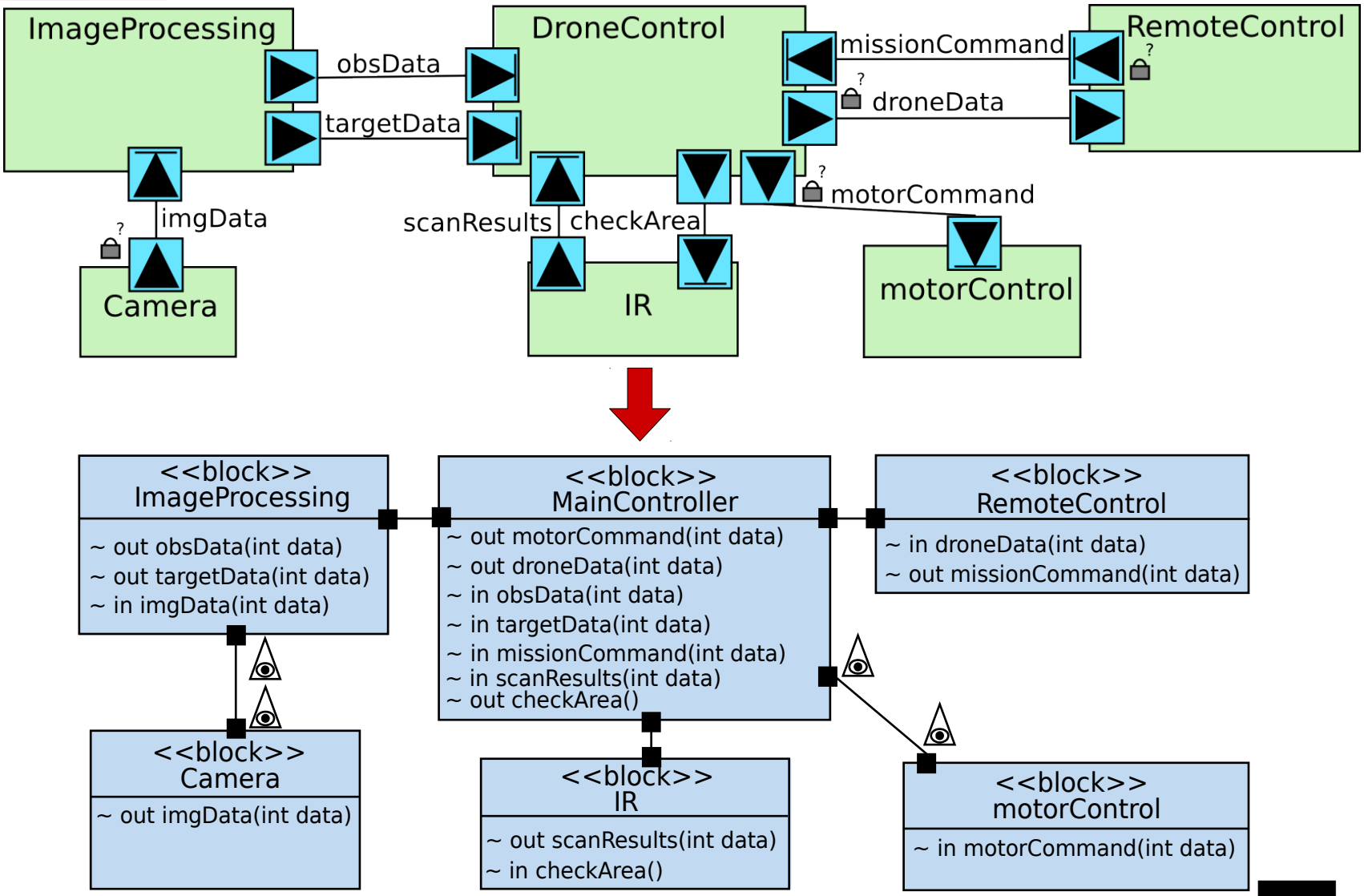
Backtracing to diagrams

Security Countermeasures

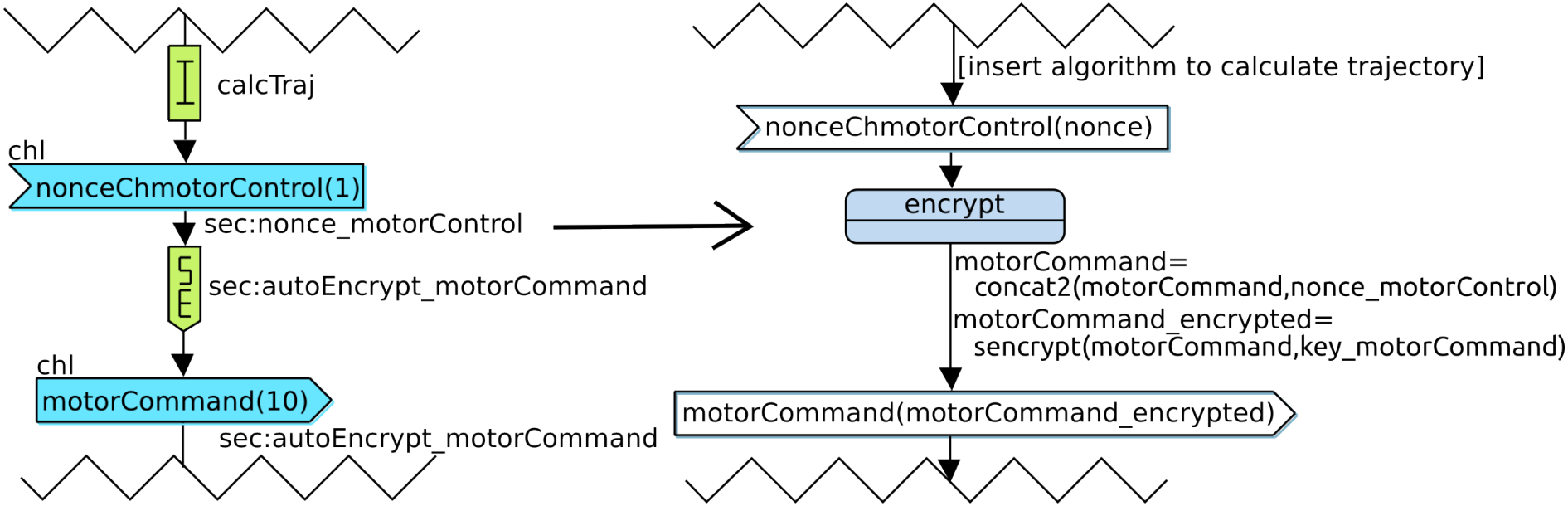


System/Software Design

Software Design



Software Design



Conclusion

- SysML-Sec : Unified methodology for Secure Embedded System Design
- Automated evaluation of Safety, Security, and Performance

- Improve iterations between phases
- Evaluate additional security properties/attacker models

Our work at:

ttool.telecom-paristech.fr

sysml-sec.telecom-paristech.fr

Questions?