Velisarios: Byzantine Fault-Tolerant Protocols Powered by Coq

Vincent Rahli, Ivana Vukotic,
Marcus Völp, Paulo Esteves-Verissimo

April 18, 2018

Bugs and attacks are pervasive

Solutions?

securityandtrust.lu

CritiX

#cloudbleed

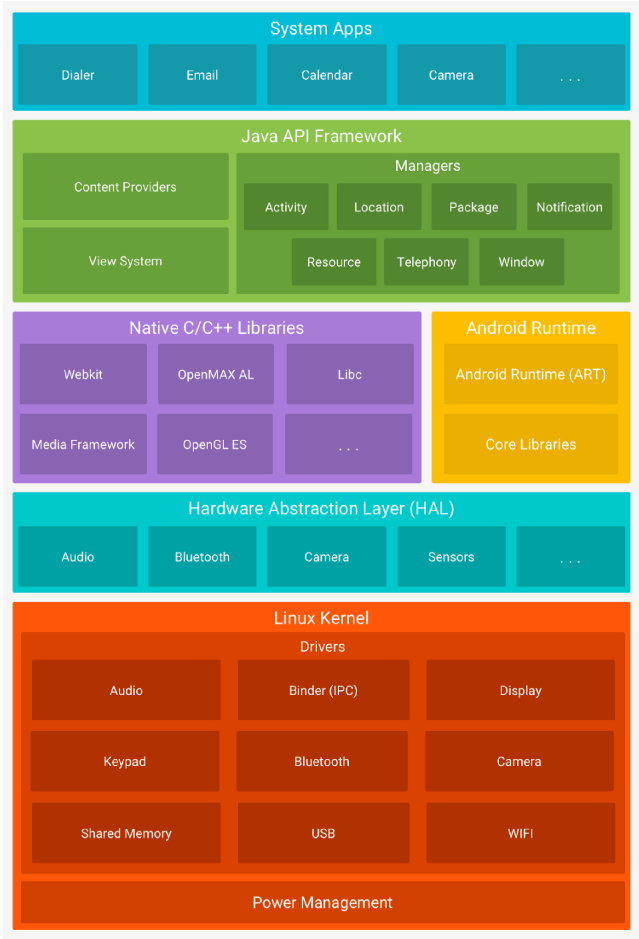
testing?

verification?

Depends on assumptions abt environment

testing?

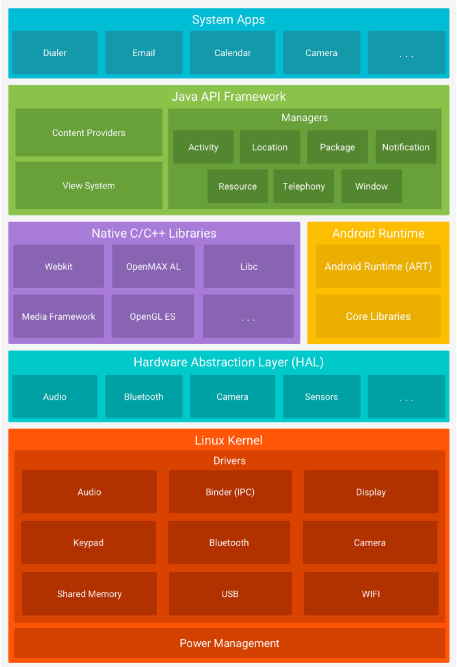
verification?

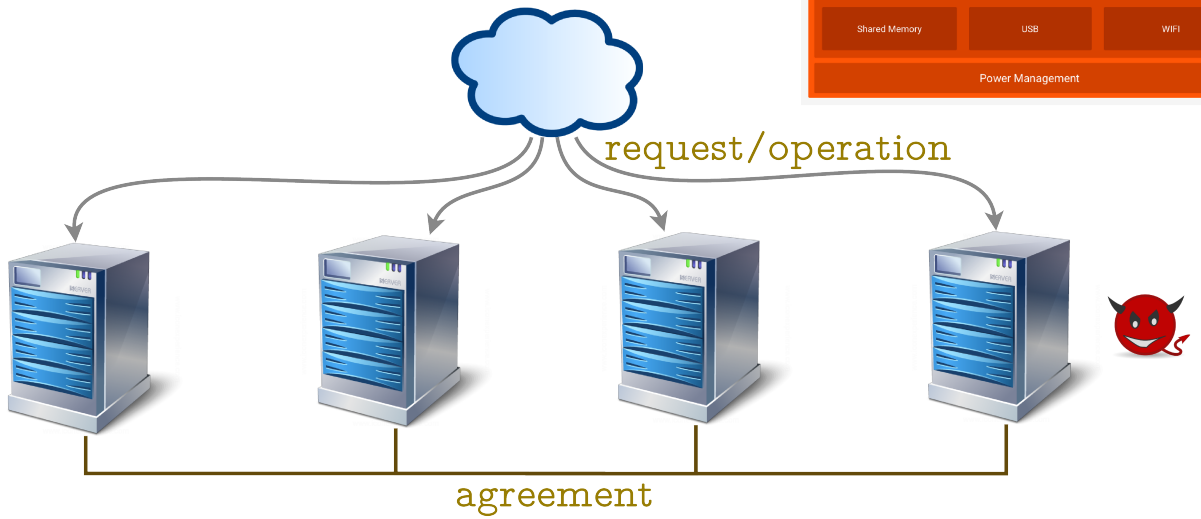


State machine replication

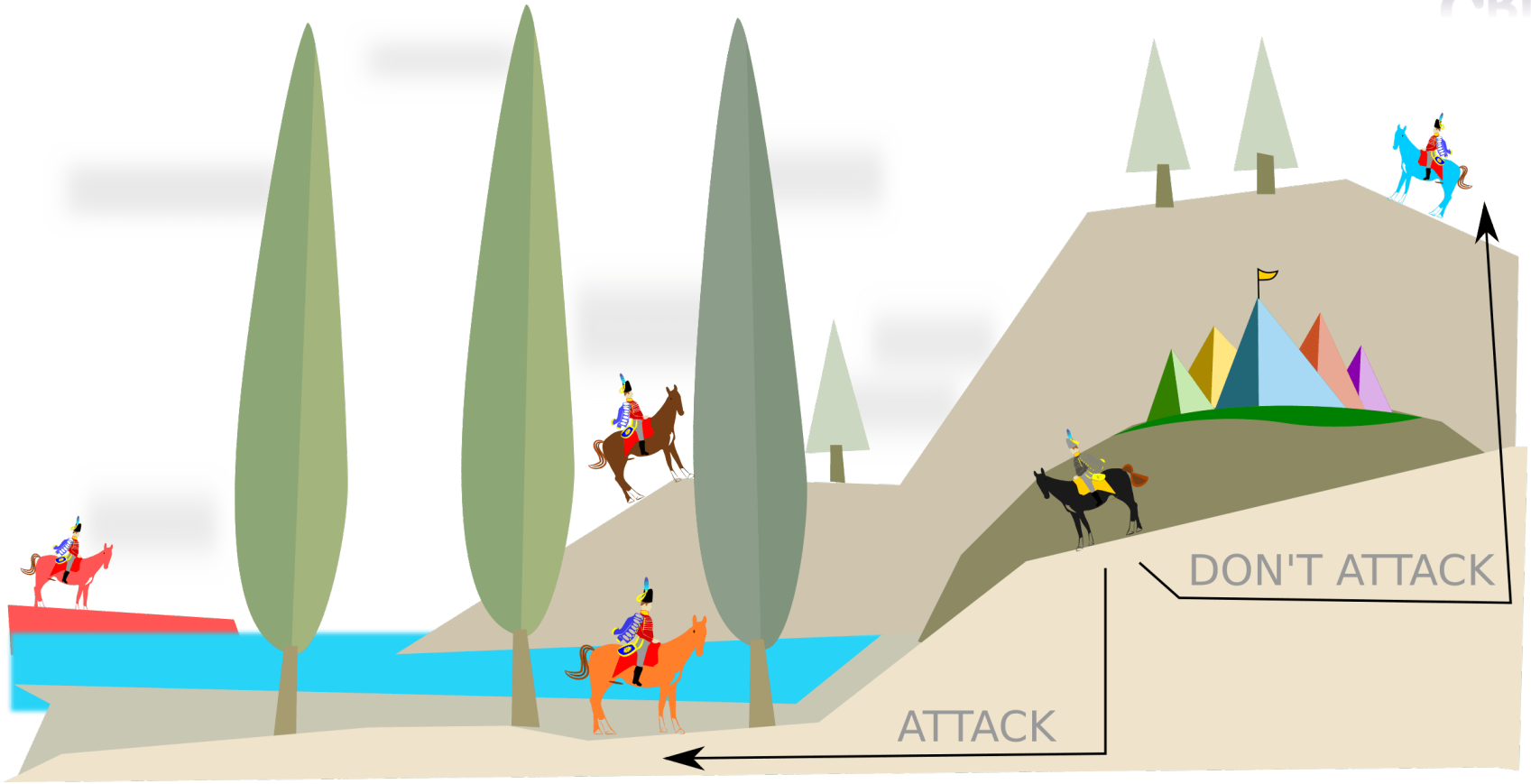
testing?

verification?

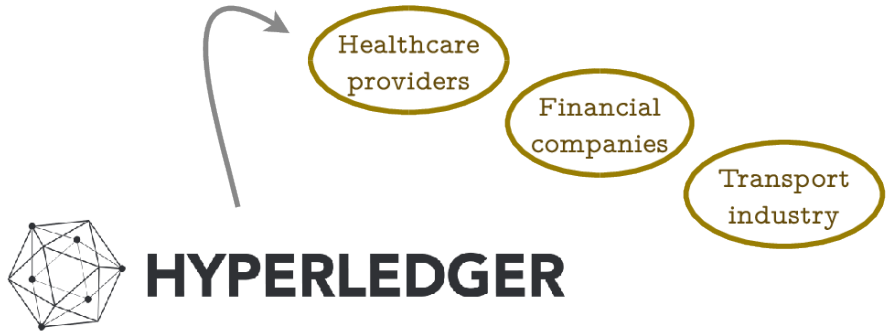




Byzantine Generals



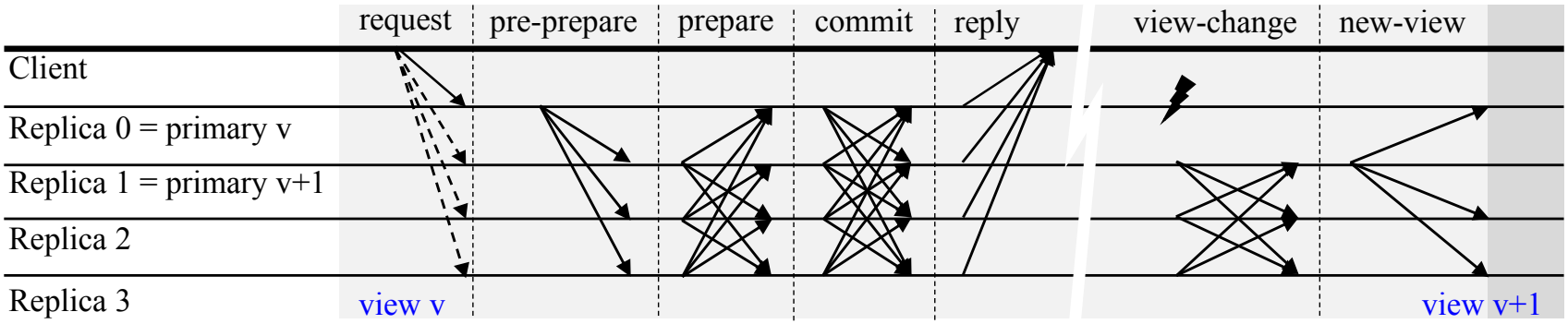
A need for verification



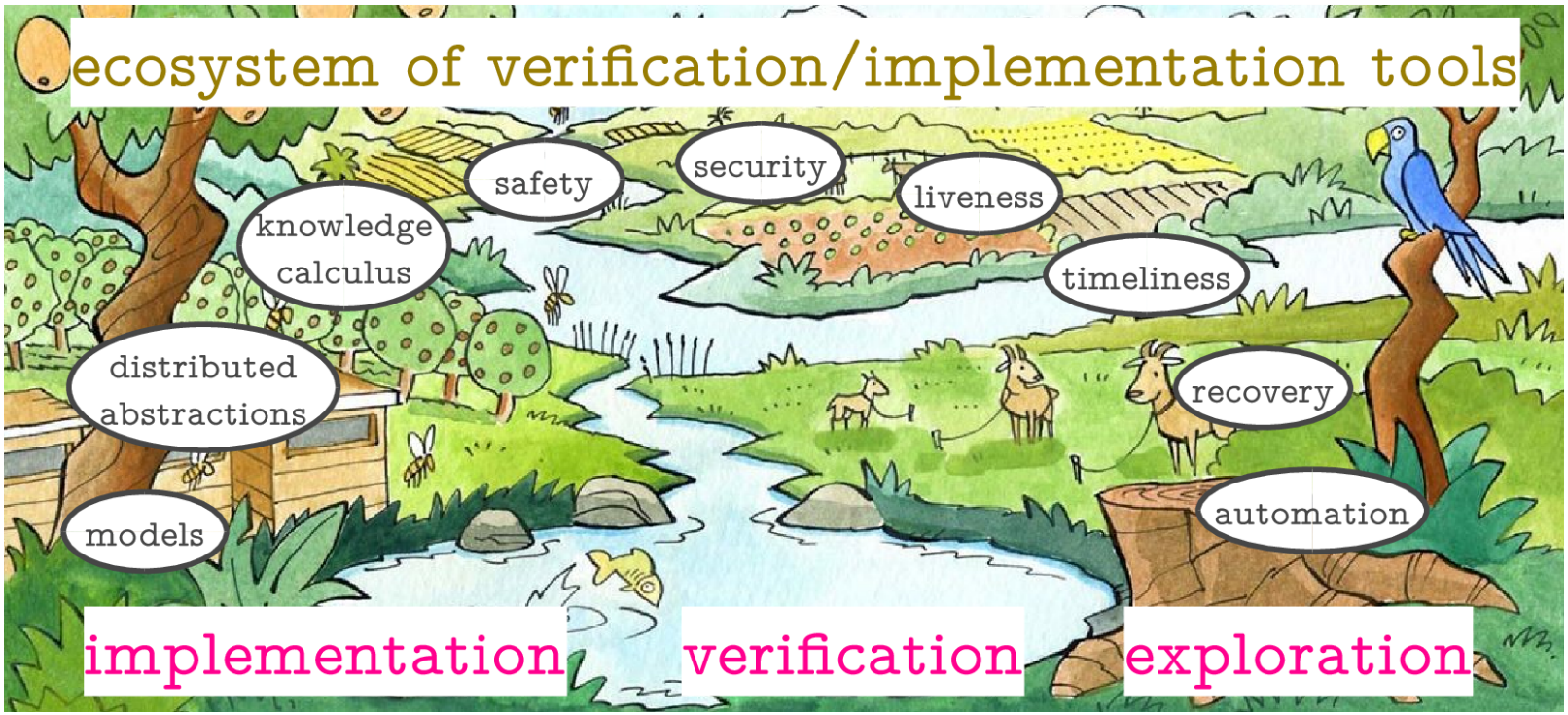
Formal framework to verify implementations of BFT protocols

reference protocol: PBFT

PBFT?


request
pre-prepare
prepare
commit
reply
view-change
new-view
Client
Replica 0 = primary v
Replica 1 = primary v+1
Replica 2
Replica 3
view v
view v+1

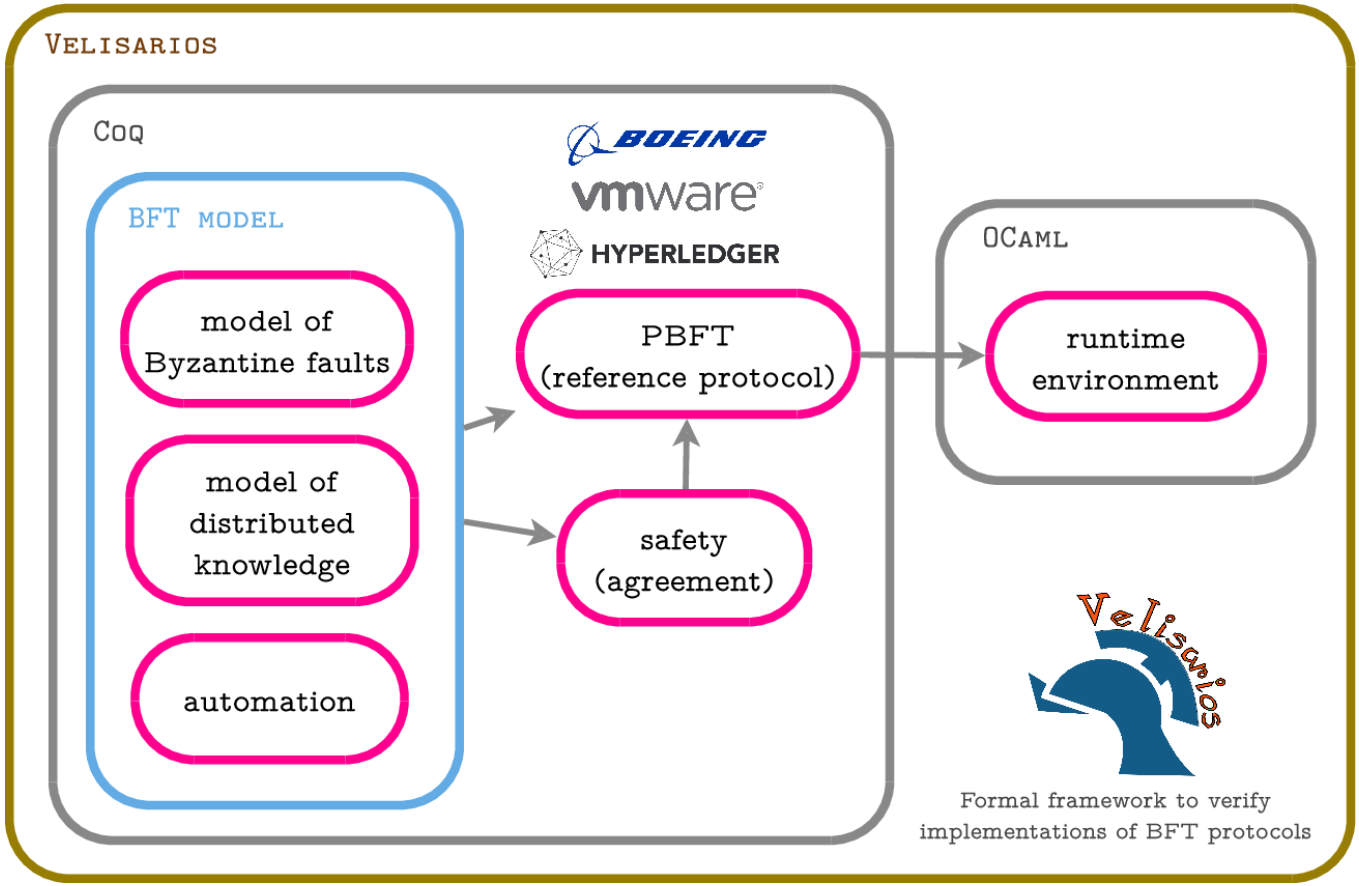
Overarching Goal



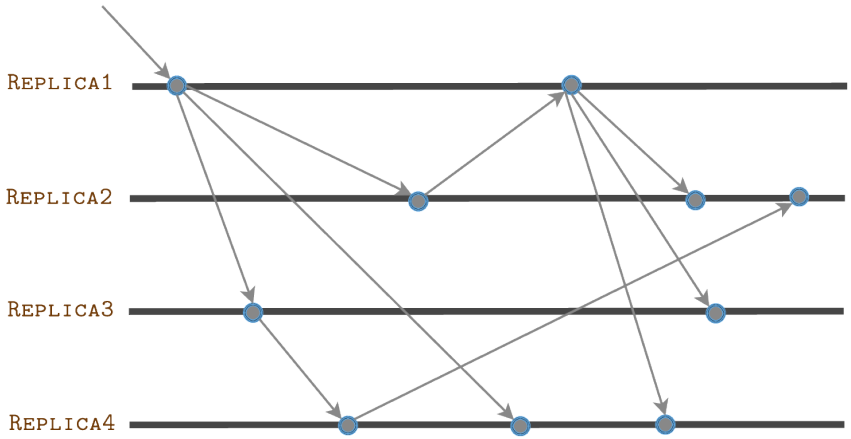
Not the first tool. Where do we fit?

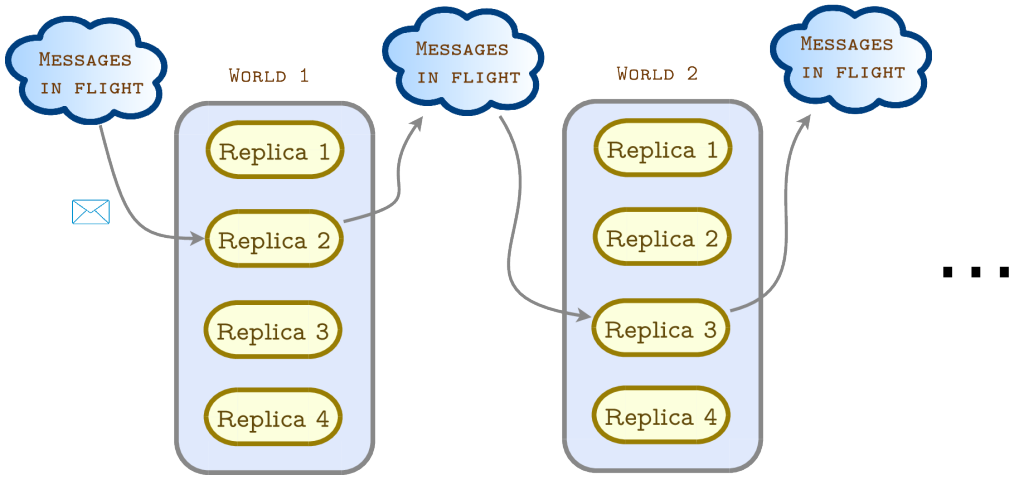
	Running code	Byz. (synch.)	Byz. (asynch.)
IronFleet/EventML/Verdi/Disel/PSync	✓	✗	✗
HO-model/PVS	✗	✓	✗
Event-B	✓/✗	✓	✗
IOA/TLA$^+$/ByMC	✗	✓	✓
Velisarios	✓	✓	✓

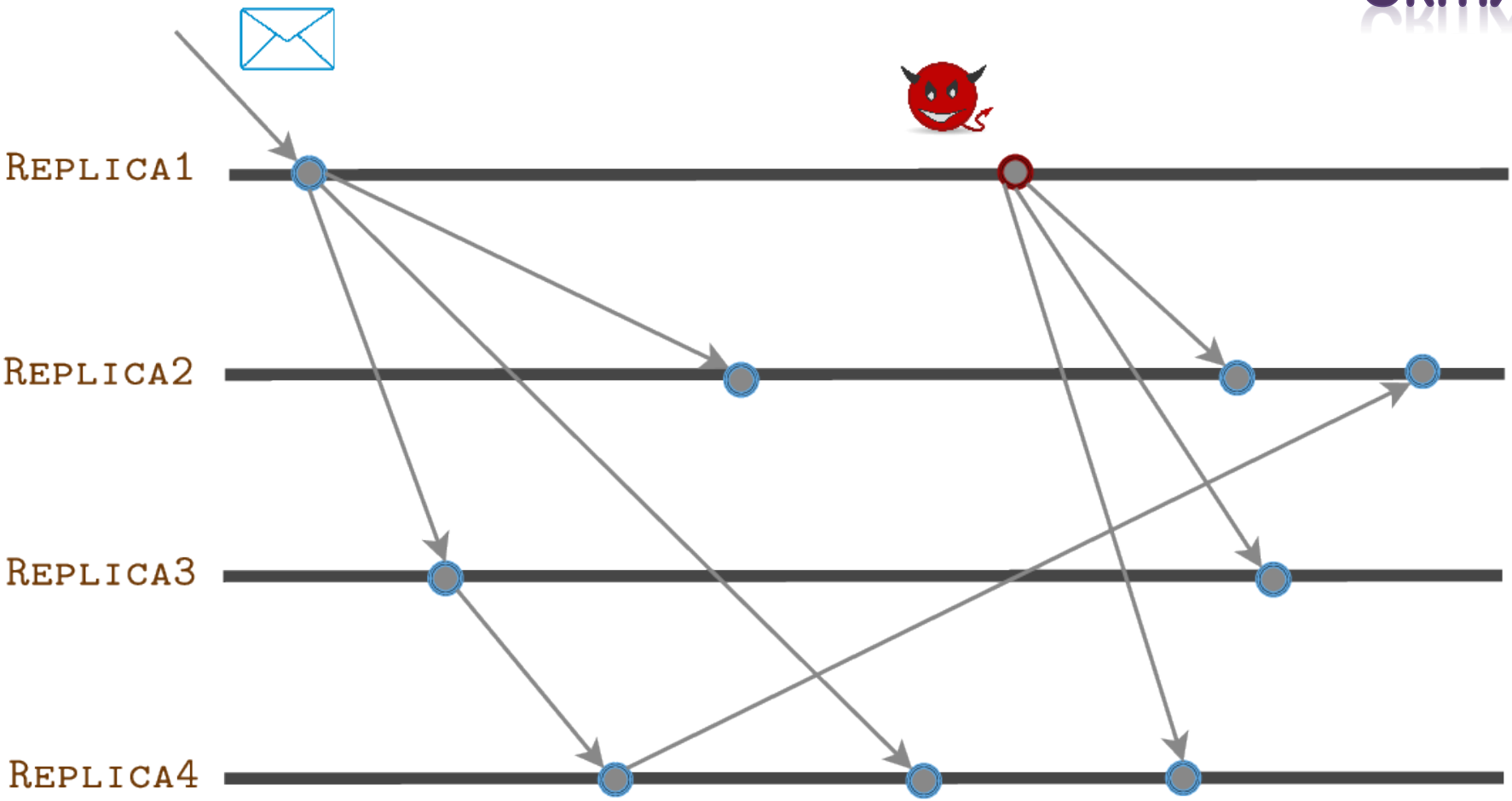
Velisarios overview



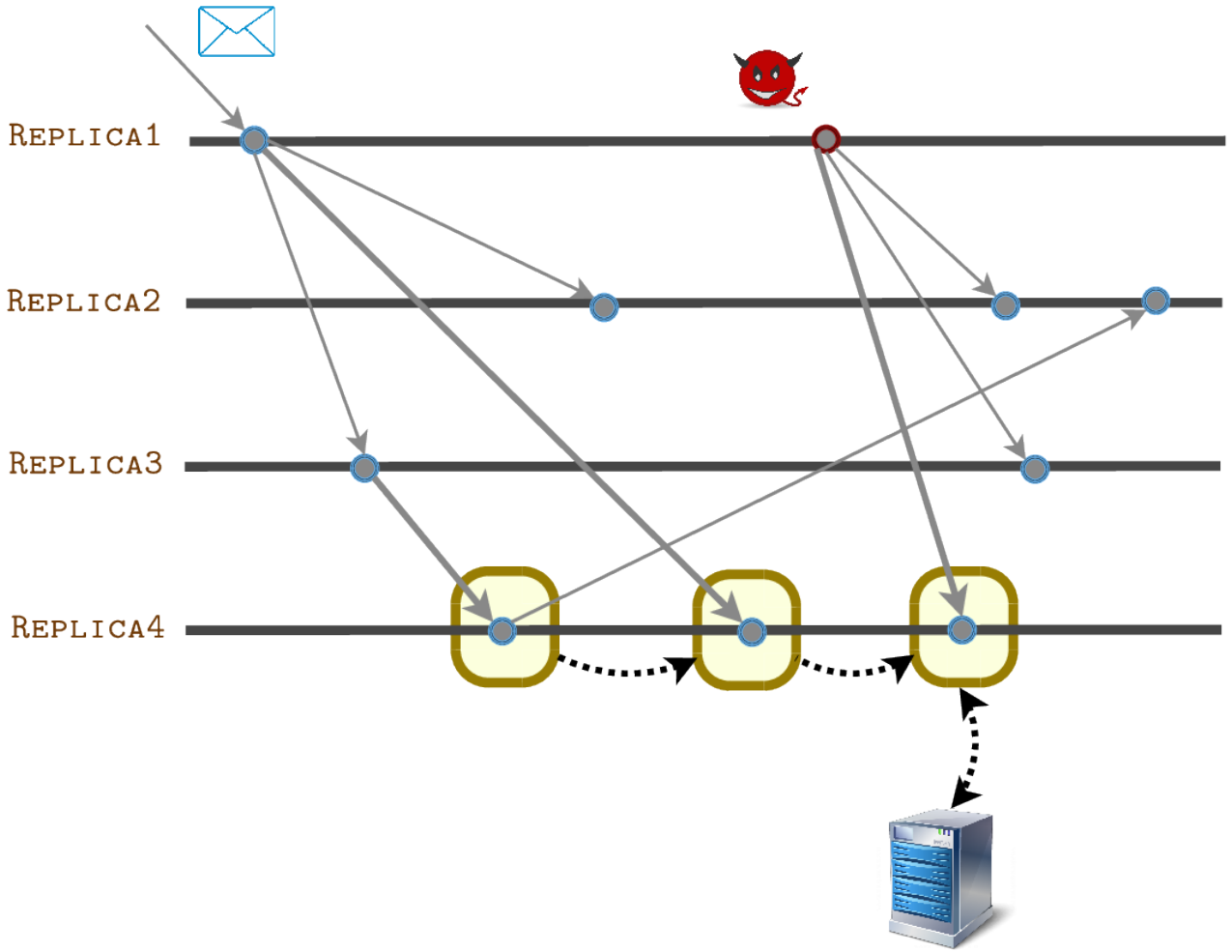
Interlude models of distributed computations



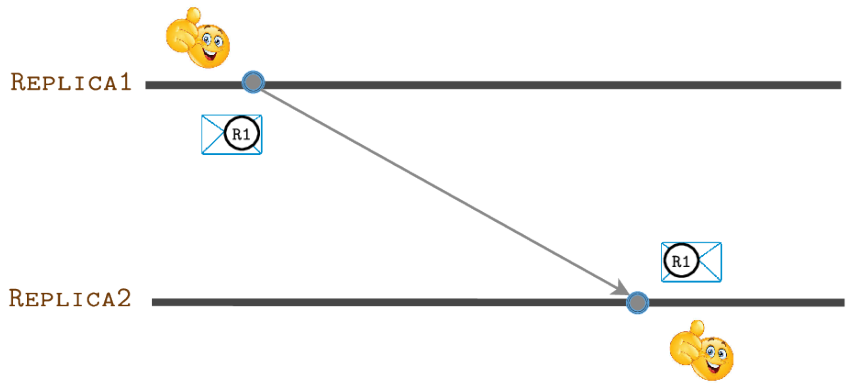



REPLICA1
REPLICA2
REPLICA3
REPLICA4

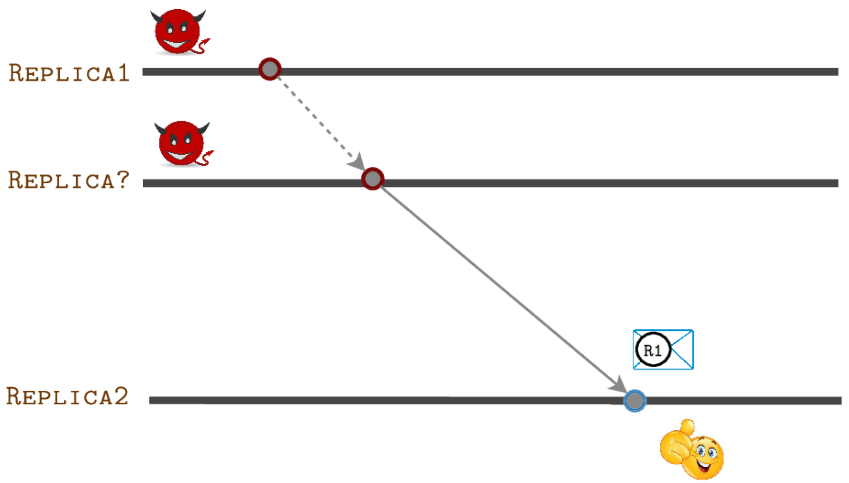
Velisarios computational model



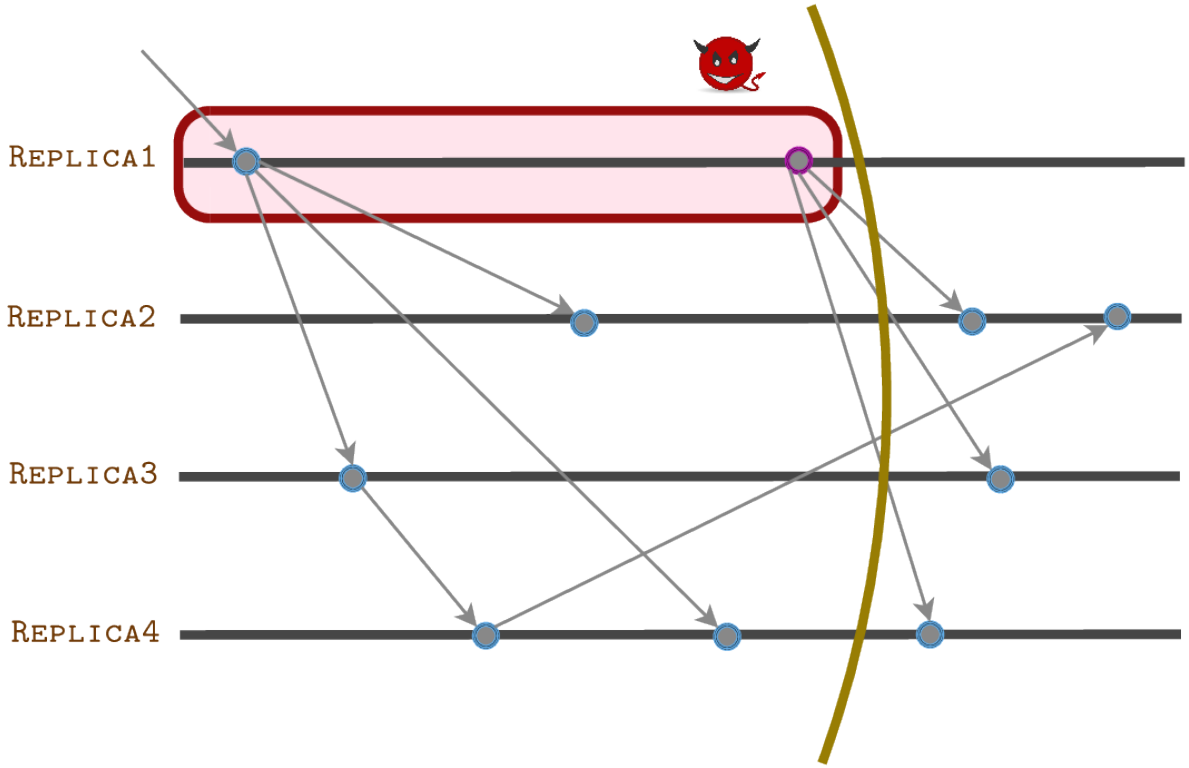
Velisarios typical assumptions



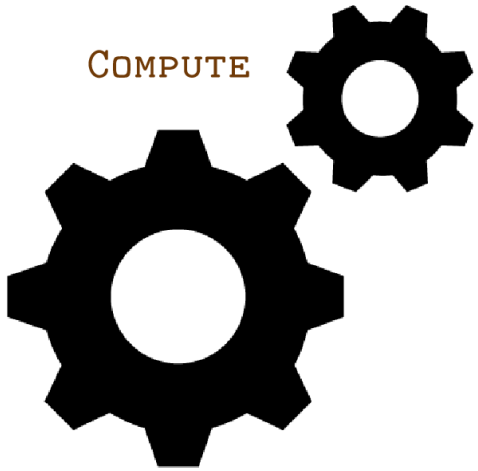
OR

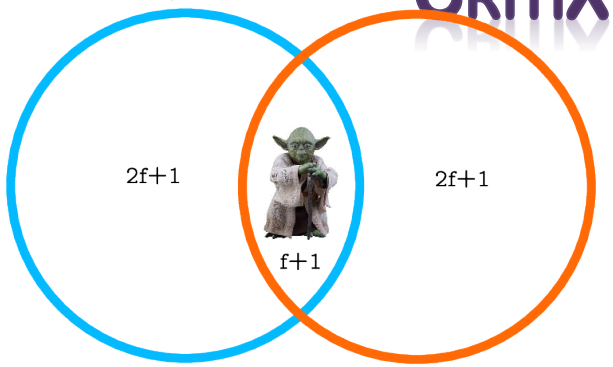


Velisarios typical assumptions

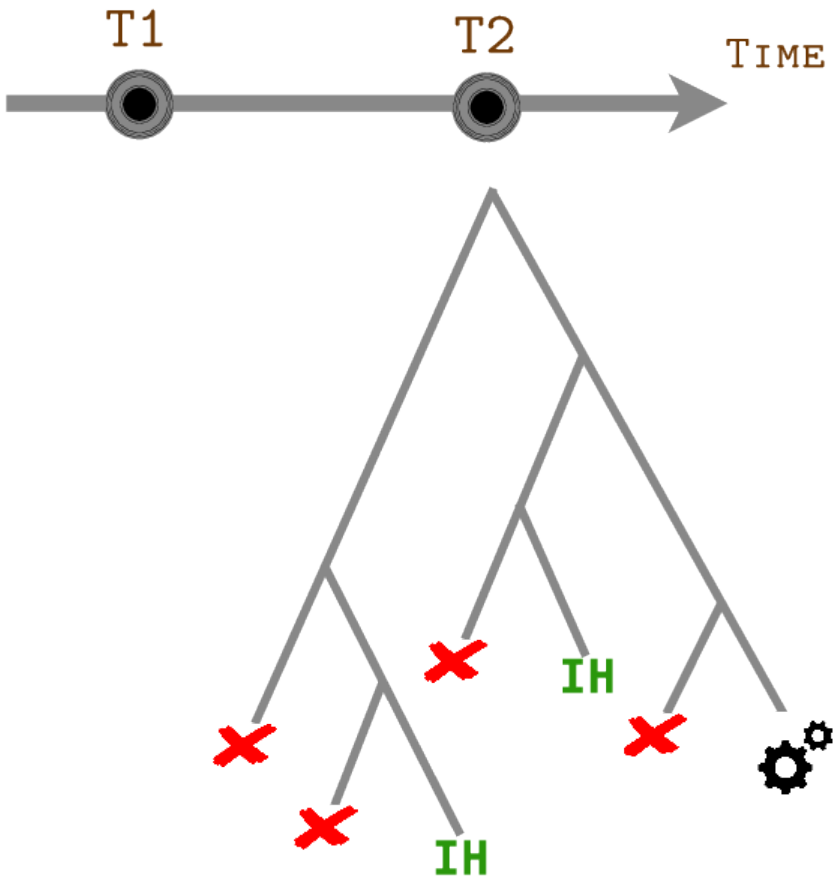


Velisarios knowledge theory





Velisarios proof automation

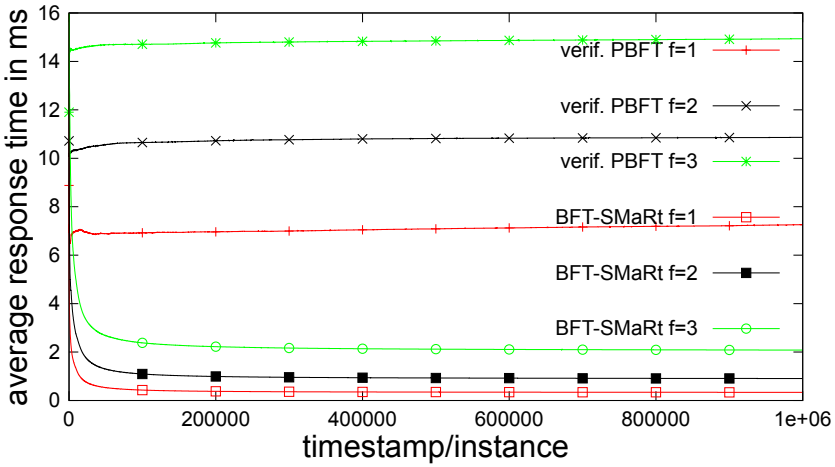


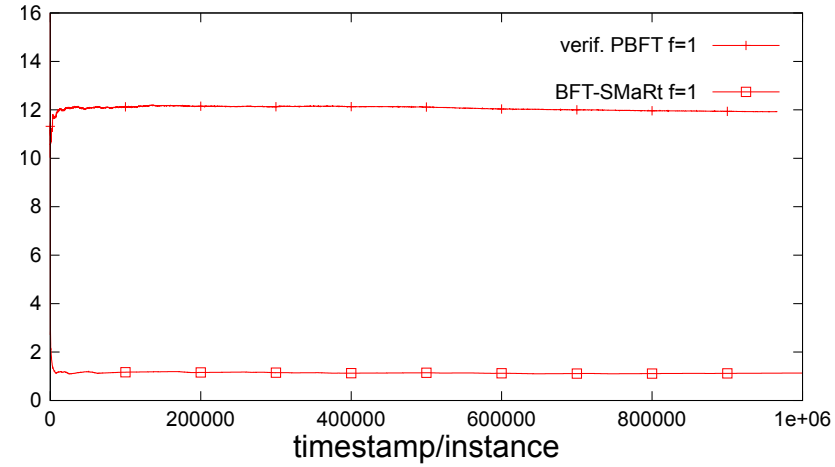
Use case: PBFT agreement

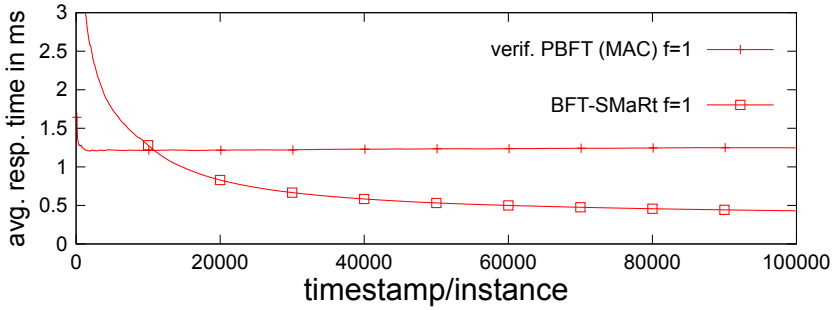
securityandtrust.lu
CritiX

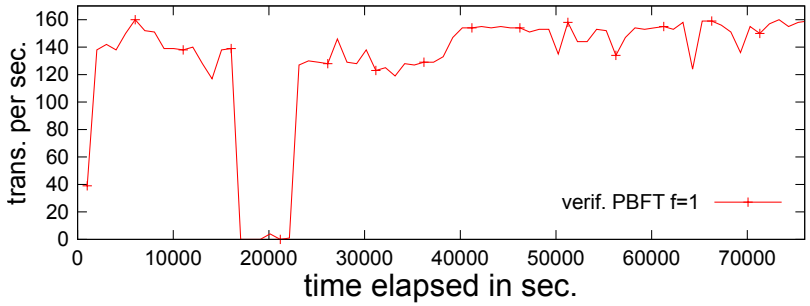
```
Lemma agreement :
  forall (eo : EventOrdering) (e1 e2 : Event) (v1 v2 : View) (ts : Timestamp)
         (c : Client) (i1 i2 : Rep) (r1 r2 : Request) (a1 a2 : list Token),
  authenticated_messages_were_sent_or_byz_sys eo PBFTsys
  → correct_keys eo
  → exists_at_most_f_faulty [e1,e2] f
  → loc e1 = PBFTreplica i1
  → loc e2 = PBFTreplica i2
  → In (send_reply v1 ts c i1 r1 a1) (output_system_on_event PBFTsys e1)
  → In (send_reply v2 ts c i2 r2 a2) (output_system_on_event PBFTsys e2)
  → r1 = r2.
```

Use case: PBFT evaluation

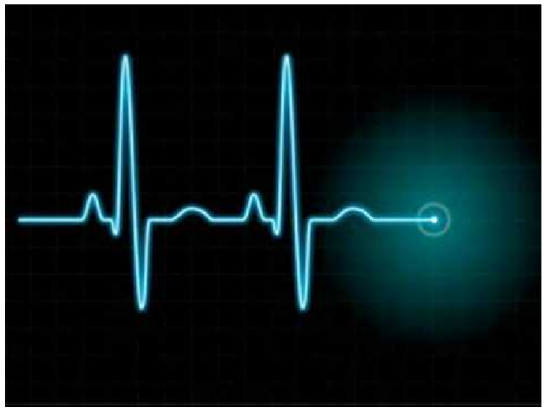






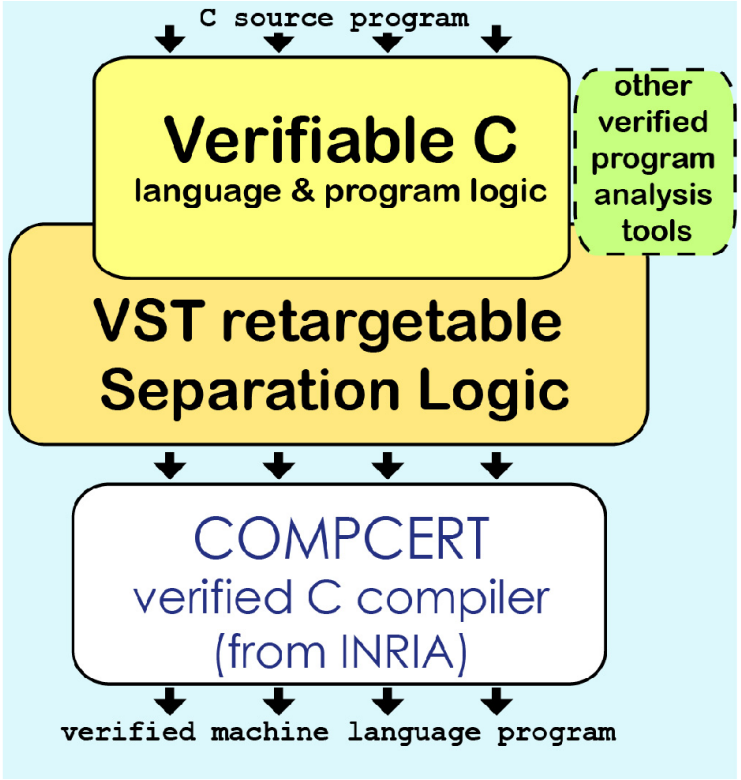


Future Work



Liveness

Timeliness



Down to C