

# Towards an Ecosystem for Verifying Implementations of BFT protocols

**PhD start:** April 2017  
**Areas:** BFT & Formal verification

**Ivana Vukotic, Vincent Rahli, Marcus Völz and Paulo Esteves-Veríssimo**

*Univ. of Luxembourg SNT  
Luxembourg*

[<name>.<surname>@uni.lu](mailto:<name>.<surname>@uni.lu)  
<http://wwwen.uni.lu/snt/research/critixv>

# Summary

- **Problem:** Distributed systems are hard to implement correct and maintain
- **Why:** Distributed systems are widely used and evolving
- **Moto:** "Trust but verify" – U.S. President Ronald Reagan
- **Consequence:** Bring stronger guaranties about correctness of existing systems, as well as help designers to build new robust systems

# Critical information infrastructure

## A horror story

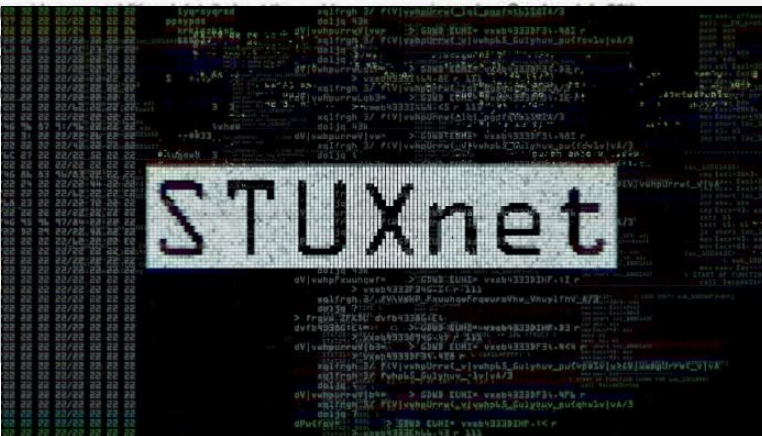
An 8-hour system-wide outage due to a single hardware fault



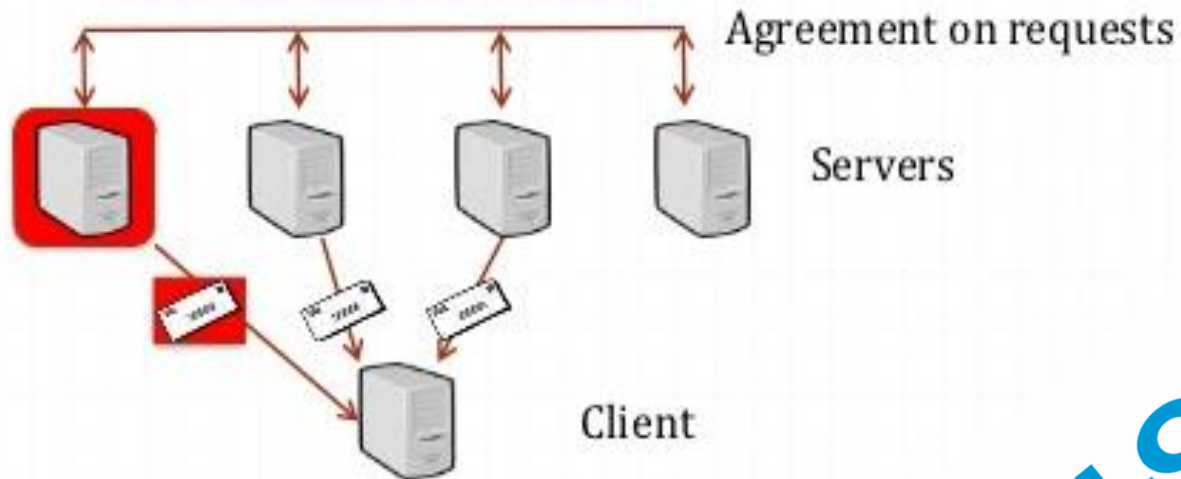
Amazon Web Services • Service Health Dashboard • Amazon S3 Availability Event: July 20, 2008

### Amazon S3 Availability Event: July 20, 2008

We wanted to  
At 8:40am PD  
rates were sig  
engaged and  
system and ac  
taking several  
health.



# BFT-SMR



**There is NO lunch for free!**

- Very complex
- No formal specification
- No implementation

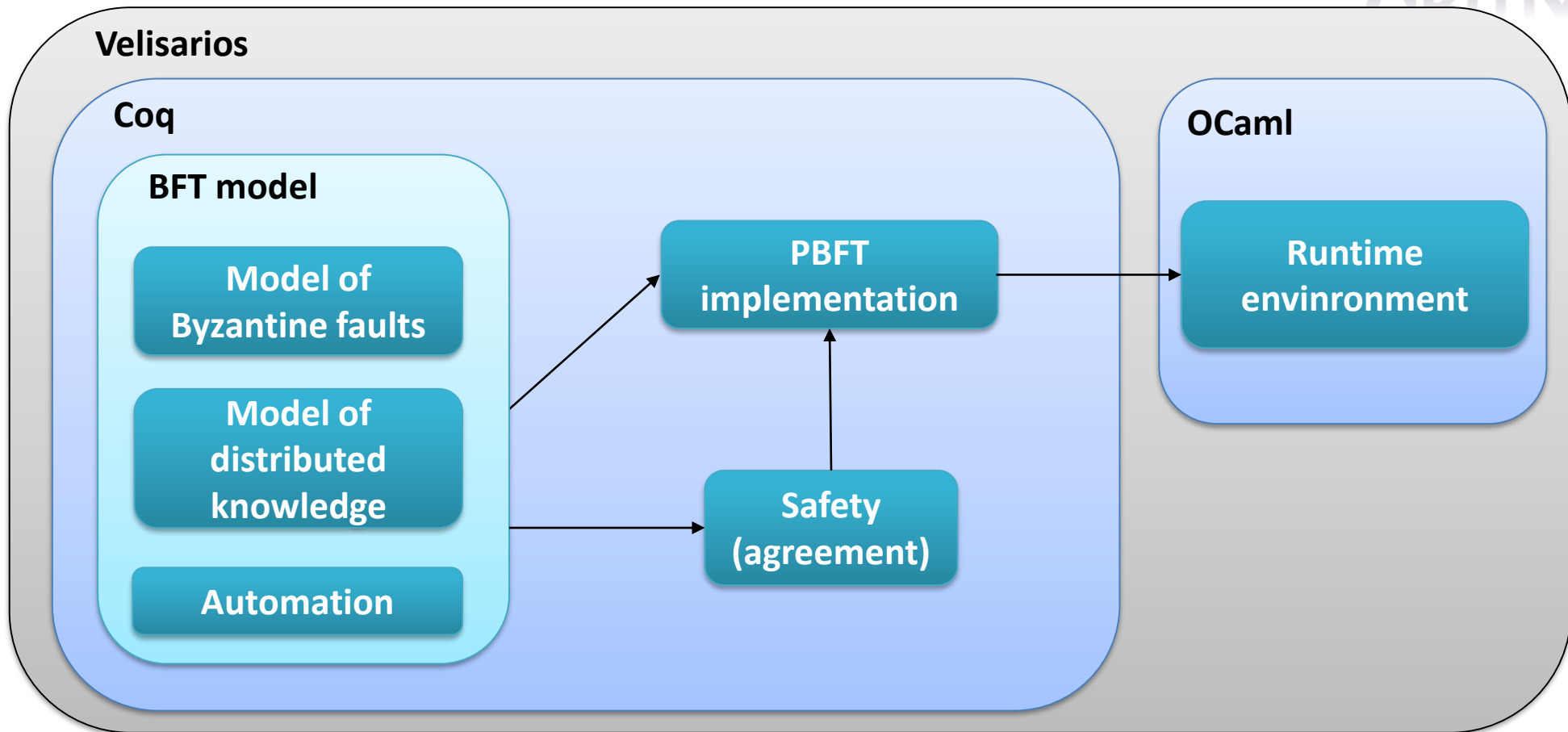


# Our goal

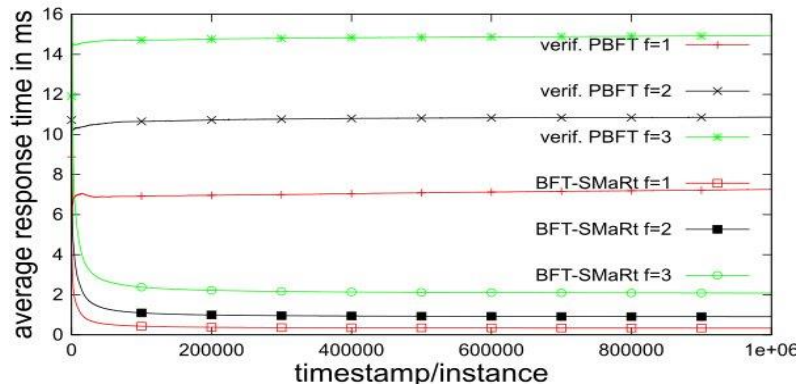
- Ecosystem of formal tools for verifying implementations of BFT protocols
- It will allow us to formally explore the breadth of possibilities for designing such protocols

# Where do we fit?

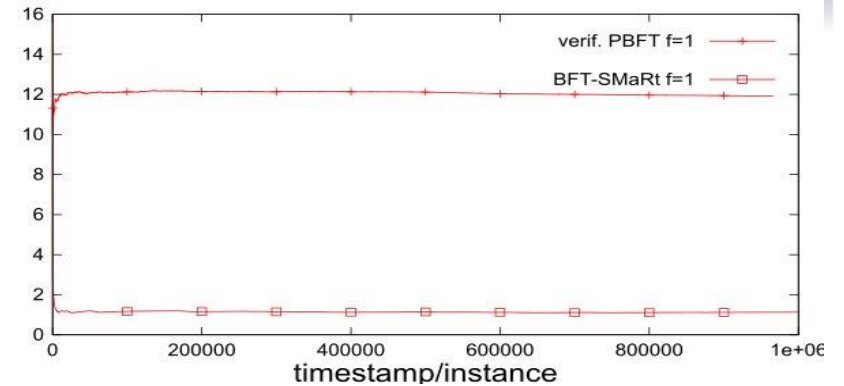
|                                     | Running code | Byzantine (synch.) | Byzantine (asynch.) |
|-------------------------------------|--------------|--------------------|---------------------|
| EventML/IronFleet/PSync/Verdi/Disel | ✓            | ✗                  | ✗                   |
| HO-model/PVS                        | ✗            | ✓                  | ✗                   |
| ByMC/IOA/TLA+                       | ✗            | ✓                  | ✓                   |
| Event-B                             | ✓✗           | ✓                  | ✗                   |
| <b>Velisarios</b>                   | ✓            | ✓                  | ✓                   |



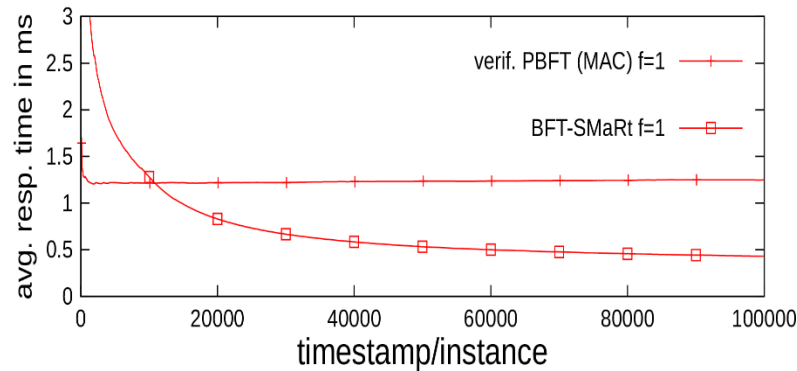
# Extraction and Evaluation



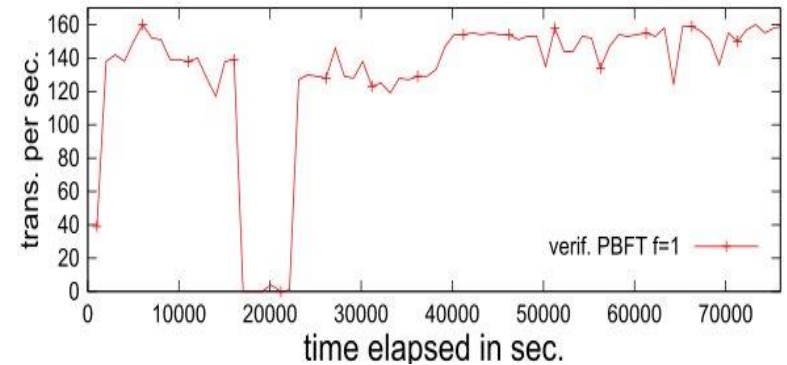
**Figure 1.** Single machine



**Figure 2.** Several machines

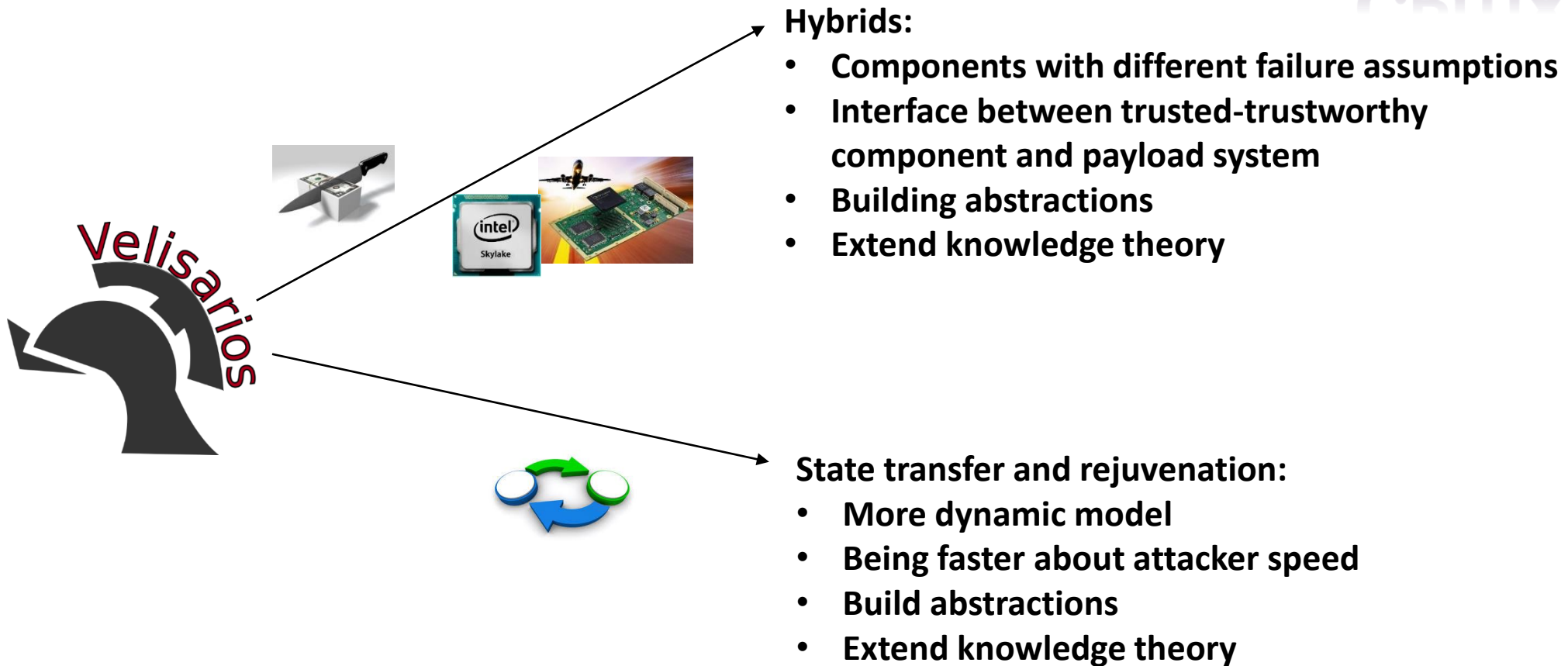


**Figure 3.** Single machine using MAC



**Figure 4.** View change response time

# Lines of Research for my PhD



# Future lines of research

## Liveness/timeliness



## Bridging the gap

