When is CAN Bus the Weakest Link? A Bound on Failures-In-Time in CAN-Based Real-Time Systems

Controller Area Network

To appear in the proceedings of the 36th IEEE Real-Time Systems Symposium (RTSS 2015)

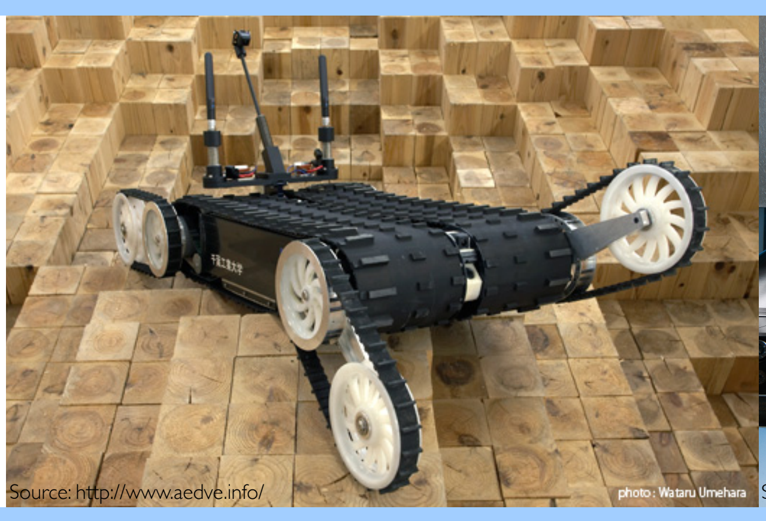
Arpan Gujarati and Björn B. Brandenburg

Max Planck Institute for Software Systems

Safety-critical real-time systems

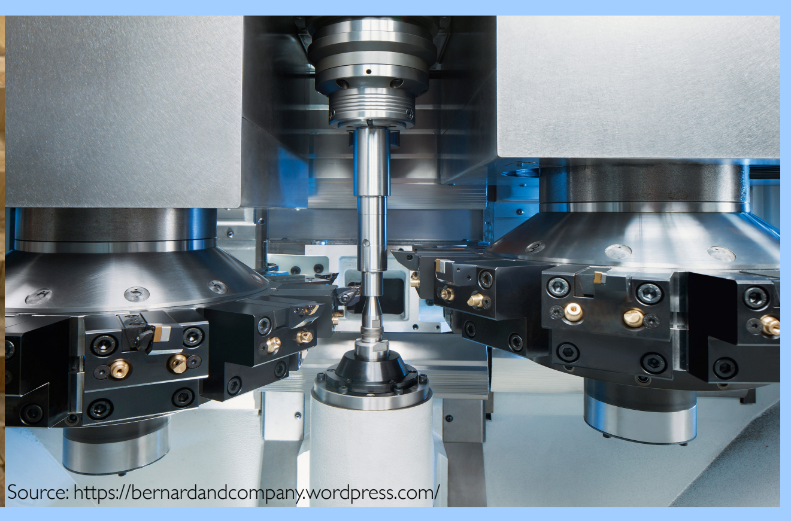
Source: http://furo.org/en/works/quince.html

Automotive systems surrounded by motors



Source: http://www.aedve.info/

Robots operating under hard radiation



Source: https://bernardandcompany.wordpress.com/

Industrial systems close to high-power machinery

Electromagnetic Interference (EMI)

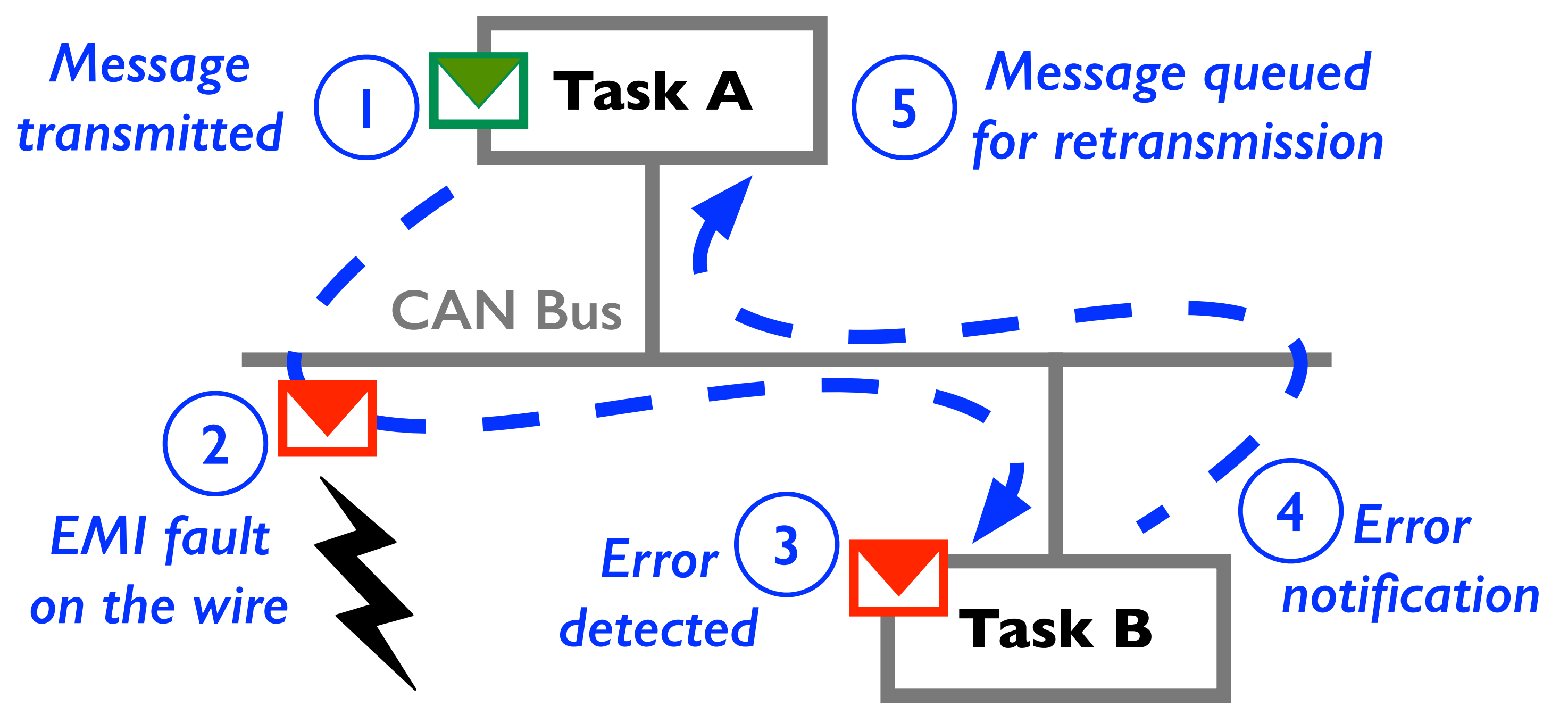
Host Faults

Hangs, crashes, incorrect outputs

Transmission Faults

Corrupted messages in networked systems

Retransmissions to tolerate transmission faults



1 *Message transmitted*

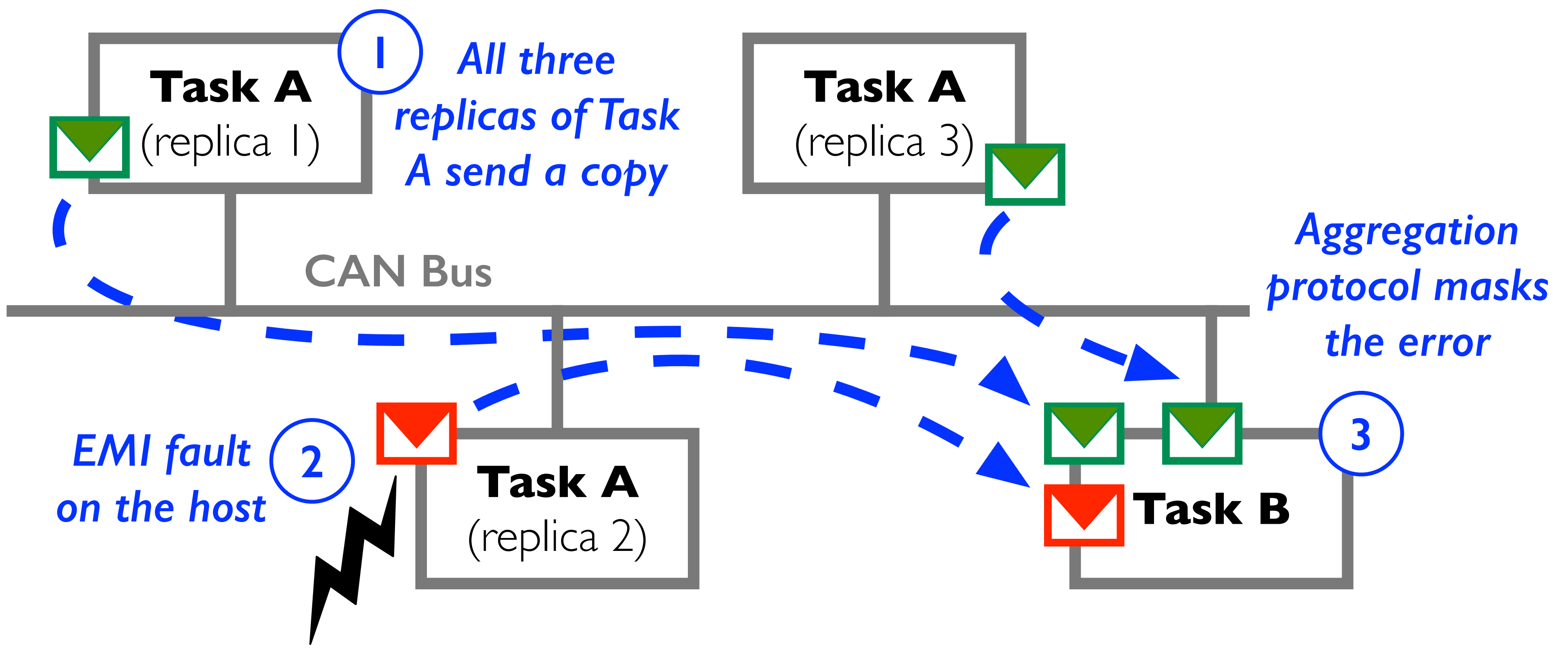
2 *EMI fault on the wire*

3 *Error detected*

4 *Error notification*

5 *Message queued for retransmission*

Active replication of tasks to tolerate host faults



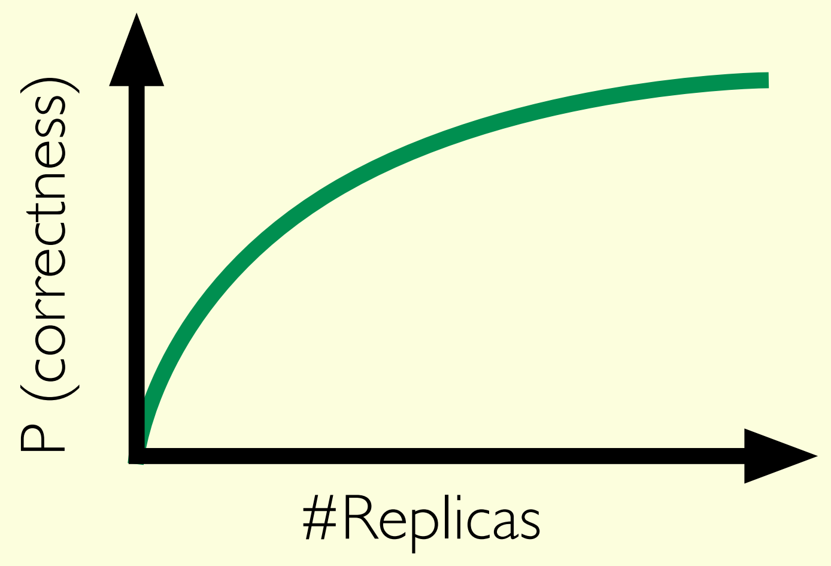
1 *All three replicas of Task A send a copy*

2 *EMI fault on the host*

3 *Aggregation protocol masks the error*

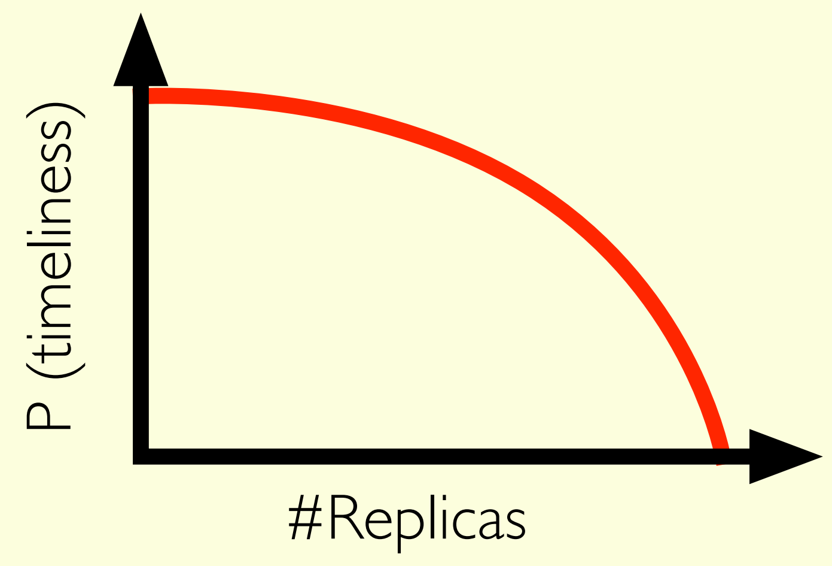
Higher Replication

- Better resiliency against host faults
- Higher probability of correctness
- But increased bus load



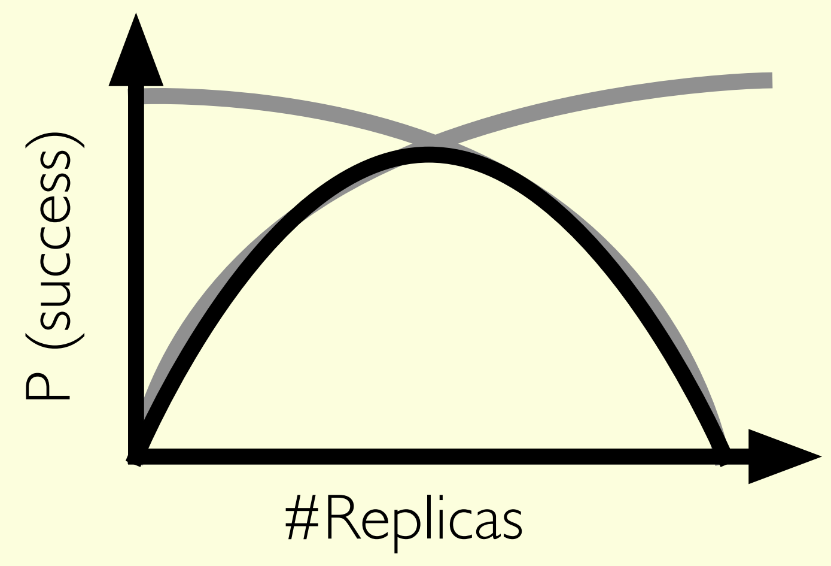
Increased bus load

- Less slack for retransmissions
- Lower probability of timely message deliveries



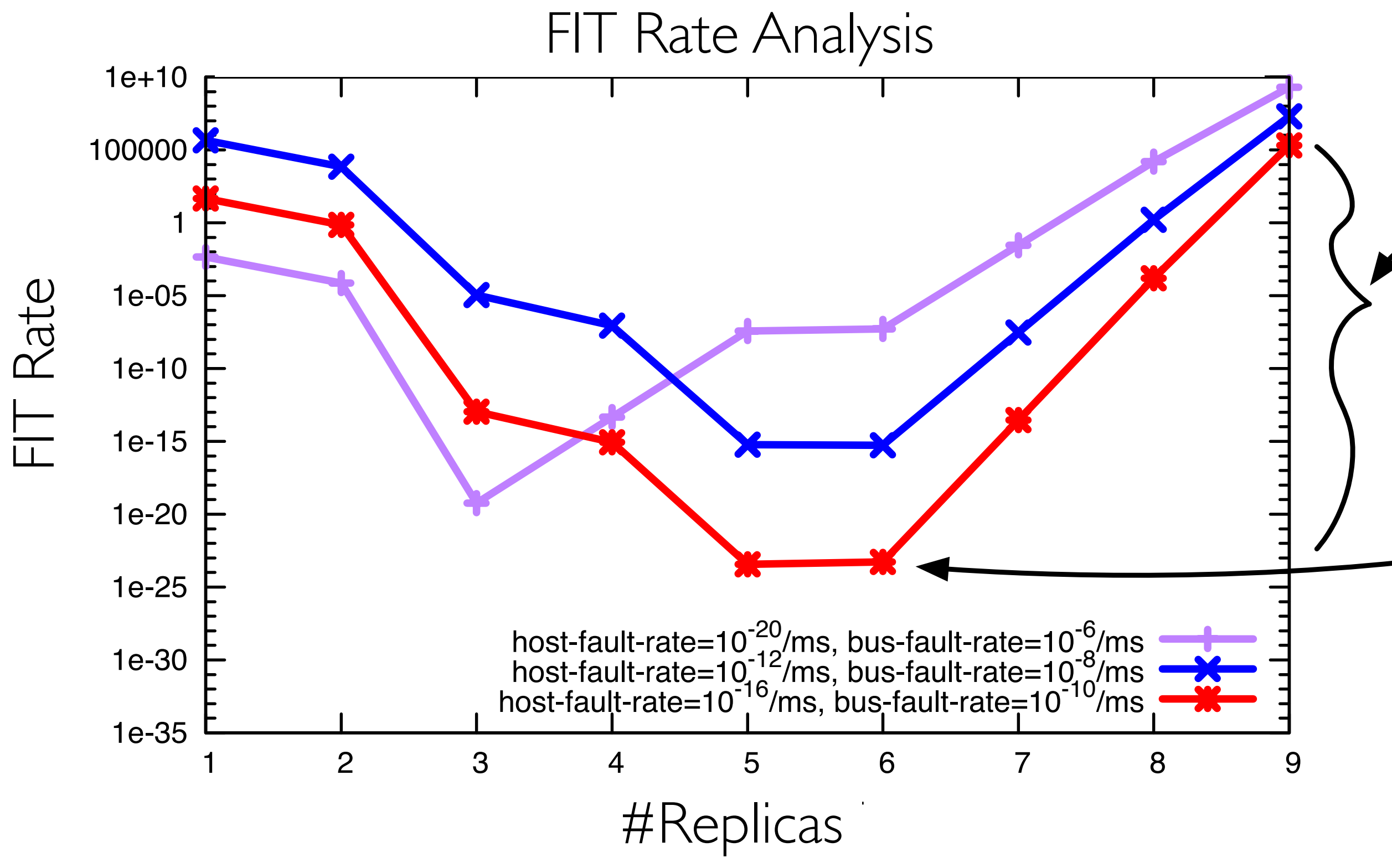
Problem

How to quantify the **inherent tradeoff** between **retransmission** and **replication**?



Probabilistic analysis to derive the Failures-In-Time (FIT) rate

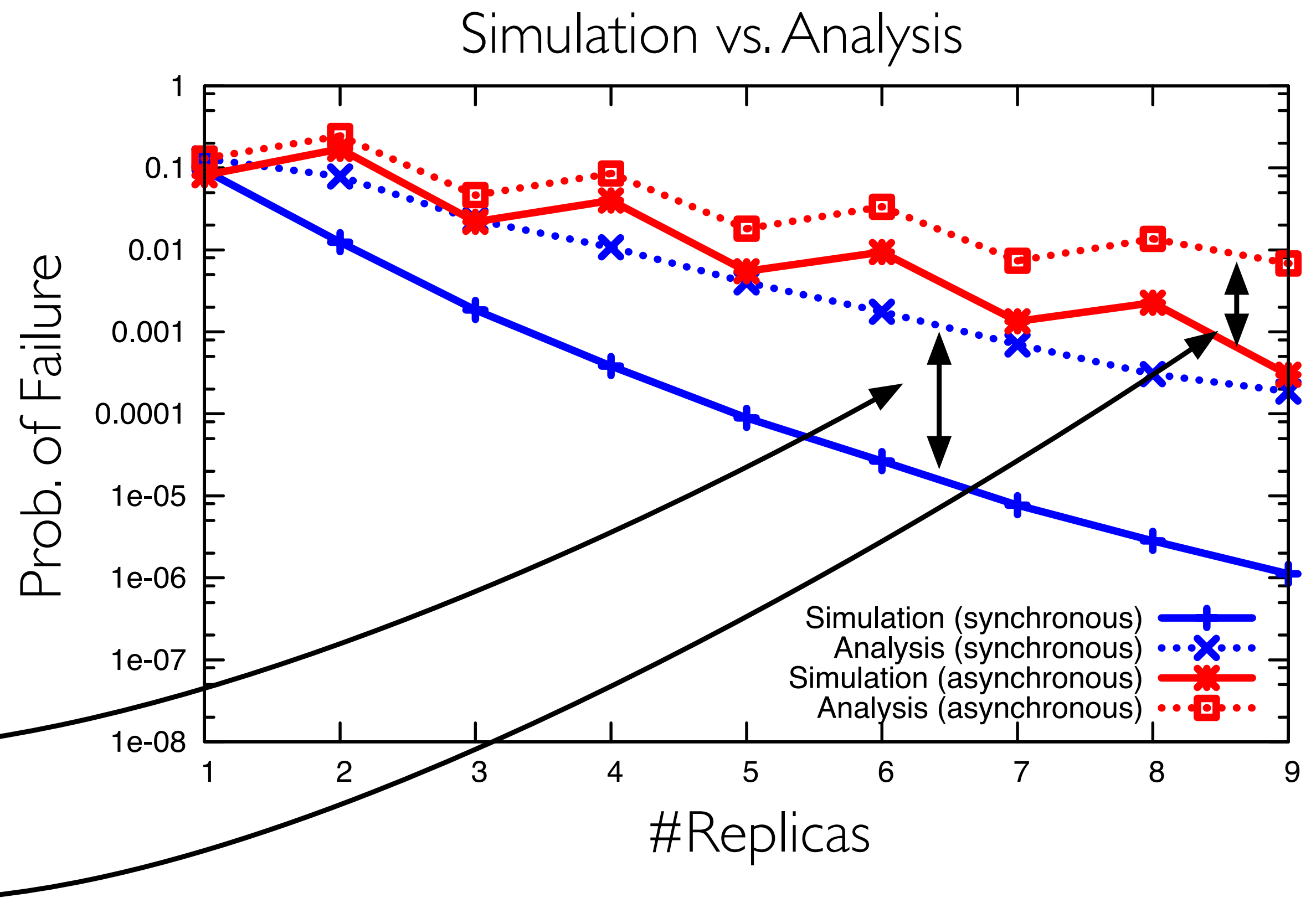
(failures in one billion operating hours, e.g., one million cars driving for one thousand hours each)



FIT rate spans more than 20 orders of magnitude

Optimal replication factor is readily apparent

Analysis is **safe** and tracks simulation results


Simulation vs. Analysis
Prob. of Failure
1e-05
1e-06
1e-07
1e-08
#Replicas
Simulation (synchronous)
Analysis (synchronous)
Simulation (asynchronous)
Analysis (asynchronous)