Probably Right, Probably on Time: An Analysis of **CAN** in the presence of **Host** and **Network** Faults

Arpan Gujarati*, Akshay Aggarwal†, Allen Clement‡, **Björn B. Brandenburg***

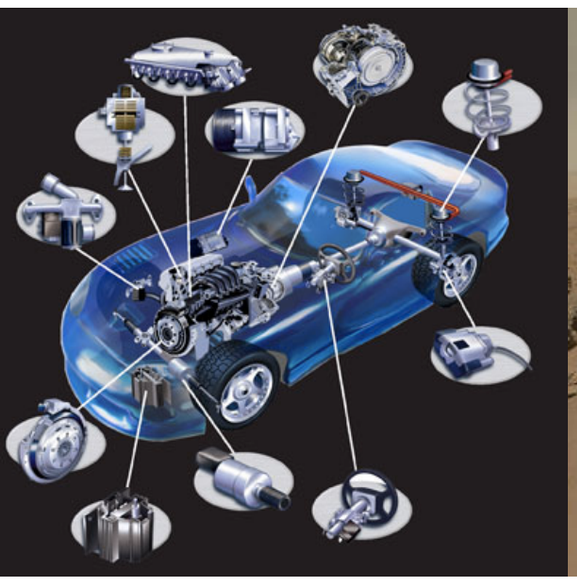
Max
Planck
Institute
for
Software Systems

**Max Planck Institute for Software Systems (MPI-SWS), Germany*

†Indian Institute for Technology (IIT) - Kanpur, India

‡Google Inc., Zurich

Safety critical real-time systems are susceptible to **electromagnetic interference (EMI)**

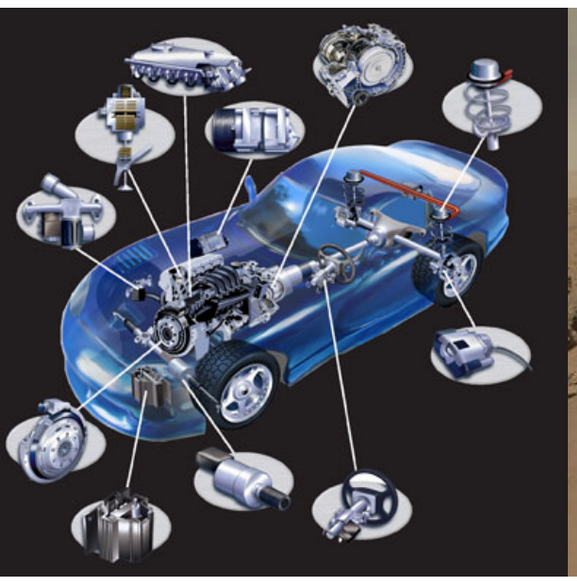


Ex: power lines

environmental radiation

high-power machinery

Safety critical real-time systems are susceptible to **electromagnetic interference (EMI)**



Ex: power lines

environmental radiation

high-power machinery

EMI can have adverse effects

- **Transmission faults**: corrupted messages in networked systems
- **Host faults**: hangs, crashes, incorrect outputs

Mechanisms to **tolerate** EMI-induced faults

Mechanisms to **tolerate** EMI-induced faults

Transmission faults

Retransmit erroneous messages
(e.g., the CAN bus protocol)

Mechanisms to **tolerate** EMI-induced faults

Transmission faults → **Retransmit erroneous messages** (e.g., the CAN bus protocol)

Host faults → **Active replication** replicate task on independent hosts

Mechanisms to **tolerate** EMI-induced faults

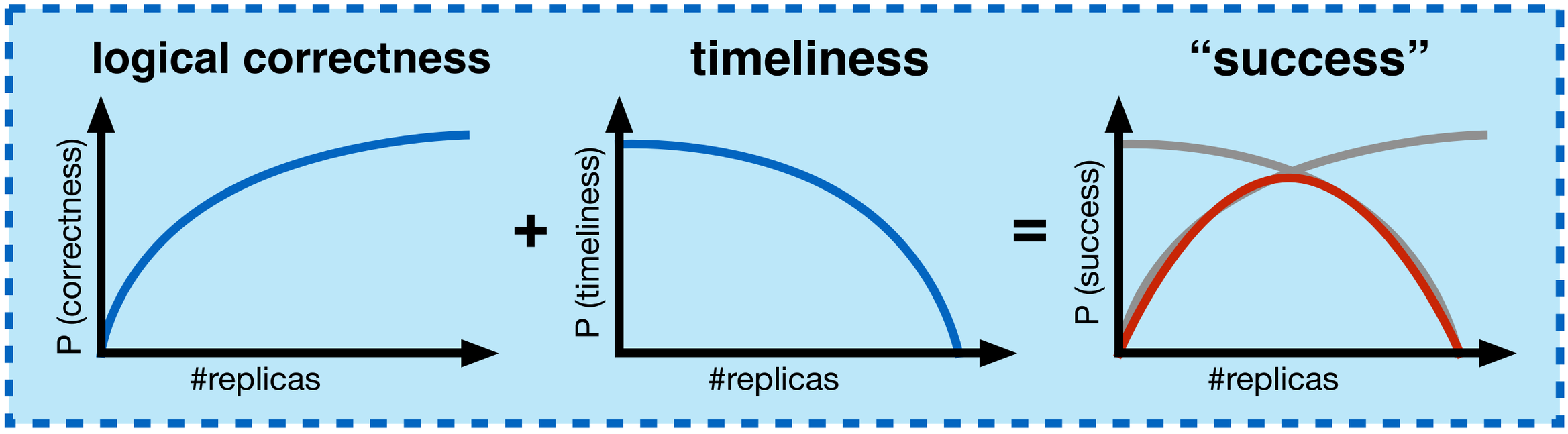
Transmission faults → **Retransmit erroneous messages** (e.g., the CAN bus protocol)

➔ *The **more slack**, **the better**!*

Host faults → **Active replication** replicate task on independent hosts

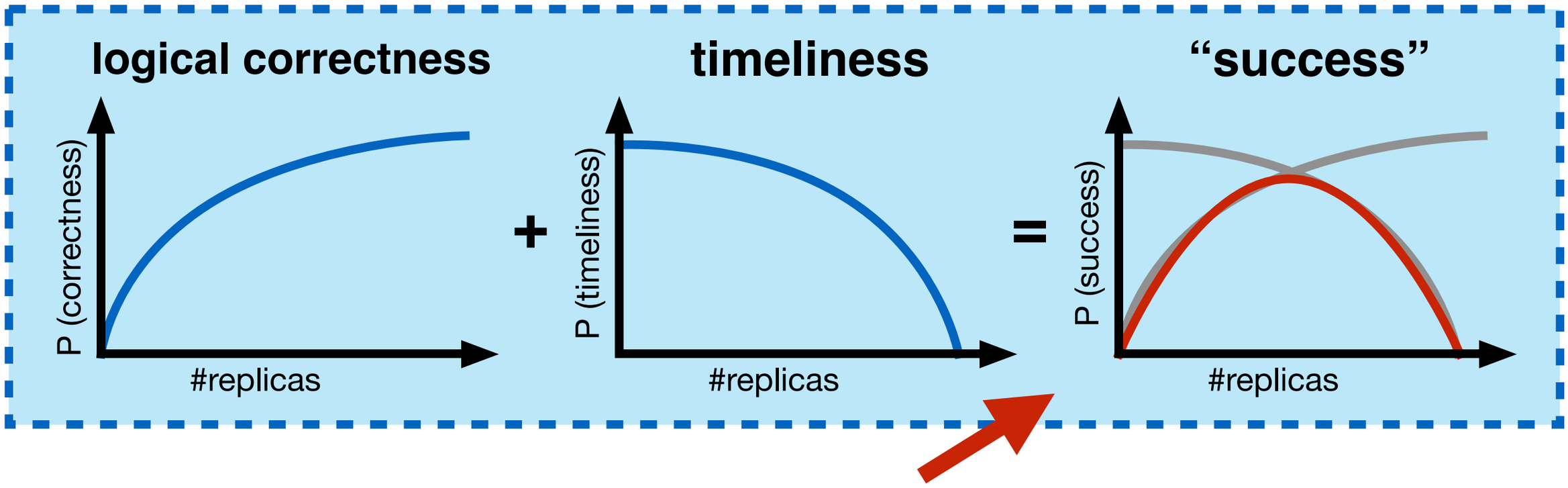
➔ ***More replicas = less slack!***

Correctness *vs.* timeliness tradeoff



More replicas = more messages = less slack!

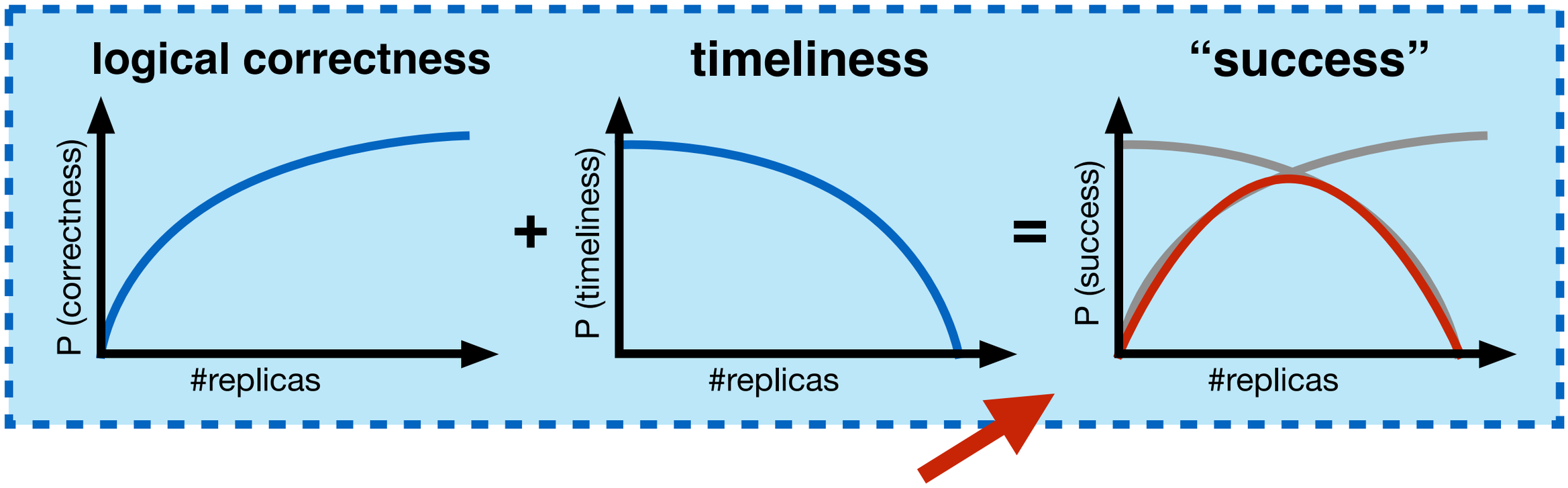
Correctness *vs.* timeliness tradeoff



Problem: What is the probability of a

“successful” message transmission?

Correctness *vs.* timeliness tradeoff



Problem: What is the probability of a

“successful” message transmission?

The message recipient infers the **correct** value of the message

The message recipient infers a value **on time**

Probabilistic analysis to **quantify** the notion of a “successful” message transmission

Probabilistic analysis to **quantify** the notion of a “successful” message transmission

Considered systems:

- **CAN-based system**
- Four different scenarios
  - ➡ **periodic / sporadic** message arrivals
  - ➡ hosts with **synchronized / asynchronous** clocks

Probabilistic analysis to **quantify** the notion of a “successful” message transmission

Considered systems:

- **CAN-based system**
- Four different scenarios
  - ➡ **periodic / sporadic** message arrivals
  - ➡ hosts with **synchronized / asynchronous** clocks

Probabilistic fault model

- **Poisson distribution** for retransmissions
- **Fixed, host-specific probabilities** for host faults
  - ➡ for omission and commission errors, respectively

Probabilistic analysis to **quantify** the notion of a “successful” message transmission

Considered systems:

- **CAN-based system**
- Four different scenarios
  - ➡ **periodic / sporadic** message arrivals
  - ➡ hosts with **synchronized / asynchronous** clocks

Probabilistic fault model

- **Poisson distribution** for retransmissions
- **Fixed, host-specific probabilities** for host faults
  - ➡ for omission and commission errors, respectively

For details, please visit our poster!