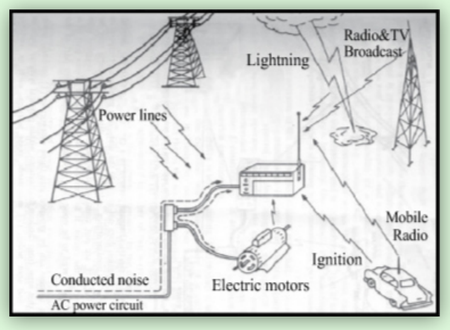
Probably Right, Probably on Time: An Analysis of **CAN** in the Presence of **Host** and **Network** Faults

Arpan Gujarati*, Akshay Aggarwal†, Allen Clement‡, and Björn B. Brandenburg*
*Max Planck Institute for Software Systems, Germany †IIT-Kanpur, India ‡Google Inc., Zurich

Safety-critical RT systems susceptible to **electromagnetic interference (EMI)**

Examples

- **Automotive systems** surrounded by electric motors
- **Industrial systems** close to high-power machinery
- **Robots** operating under hard radiation

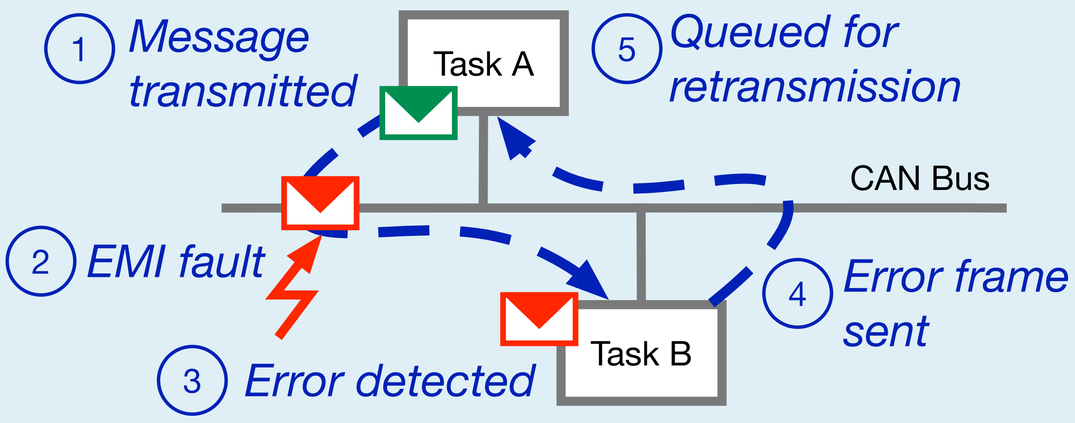


Source: http://www.bojal.com.tw/en/teach_EMI.html

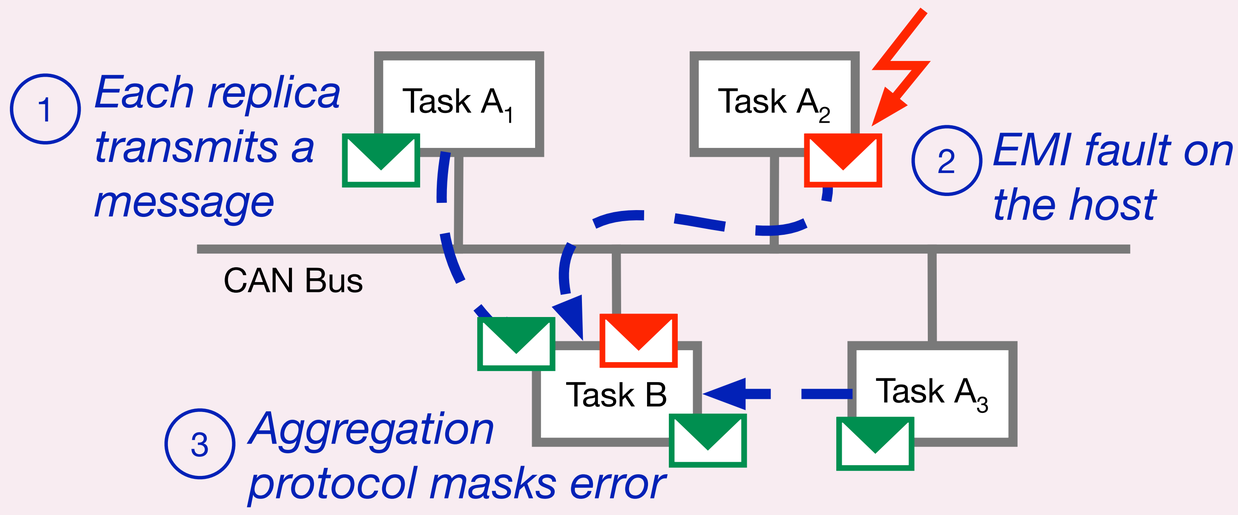
Effects of EMI

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

Retransmissions to tolerate **transmission faults**



Active replication of tasks to tolerate **host faults**

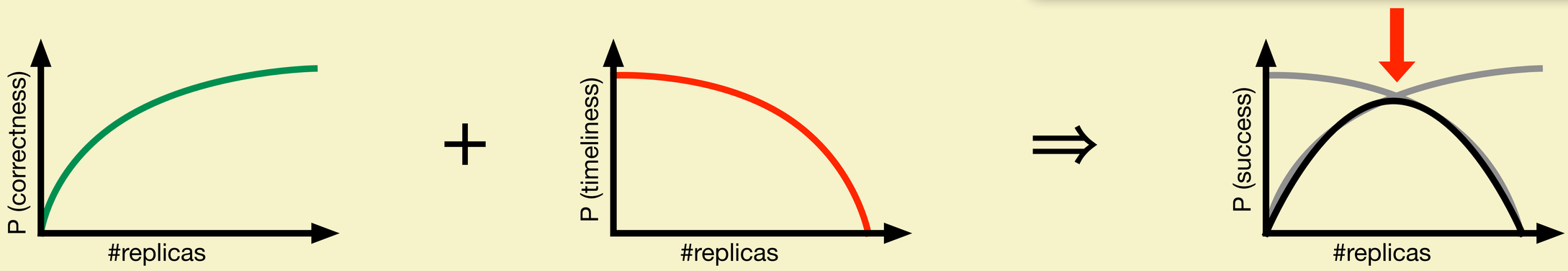


How to quantify the **inherent tradeoff** between retransmission and replication?

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

Increased bus load
⇒ Less slack for retransmissions
⇒ More deadline violations
⇒ Lower probability of timeliness

Problem
What is the **probability of a "successful" message transmission**, i.e., that task B infers the **correct** message value **on time**?



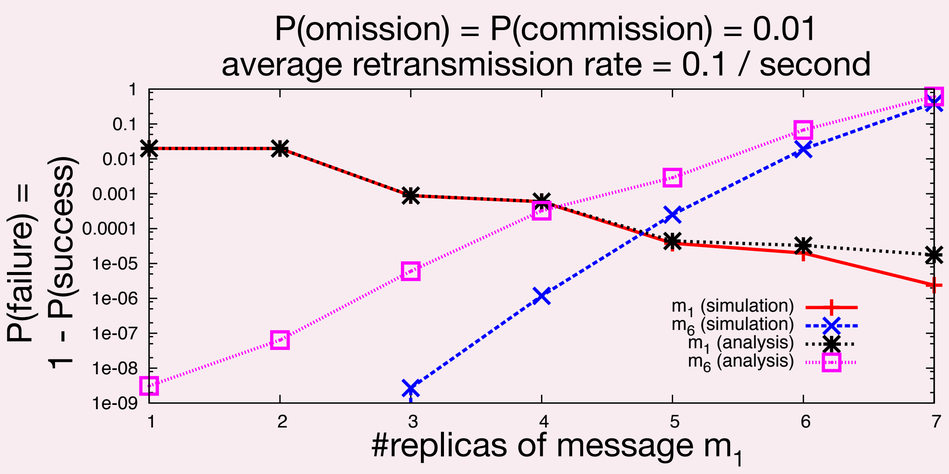
Probabilistic analysis

Probability of "success" for single round of message transmissions

Fault model

- Poisson distribution for retransmissions
- Fixed host-specific probabilities for message omissions and message commissions

Simulation vs. analysis



1. Compute probability that certain messages are omitted
2. For messages that were not omitted, compute probability of timeliness, inspired by Broster et al.'s method [1]
3. For messages that were not omitted and received on time, compute probability that a "majority" of messages are not corrupted
4. Repeat for all possible subsets of messages from this round

$$P_{su}(M_j) = \overset{4}{\sum_{O_j \subseteq M_j}} \overset{1}{P_{om}(O_j)} \cdot \sum_{k \leq |O'_j|} \overset{2}{P_{ti}(O'_j, k)} \cdot \overset{3}{P_{co}(O'_j, k)}$$

[1] I. Broster, A. Burns, and G. Rodríguez-Navas, "Timing analysis of real-time communication under electromagnetic interference," Real-Time Systems, 2005.