**Controller Area Network**

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


Arpan Gujarati and Björn B. Brandenburg

---

**Safety-critical real-time systems**

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

**Host Faults**

Hangs, crashes, incorrect outputs

**Electromagnetic Interference (EMI)**

**Transmission Faults**

Corrupted messages in networked systems

---

**Retransmissions** to tolerate transmission faults

- **Message transmitted**
- **EMI fault on the wire**
- **Error detected**
- **Message queued for retransmission**
- **Error notification**

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

- **Task A (replica 1)** sends a copy
- **Task A (replica 3)** sends a copy
- **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