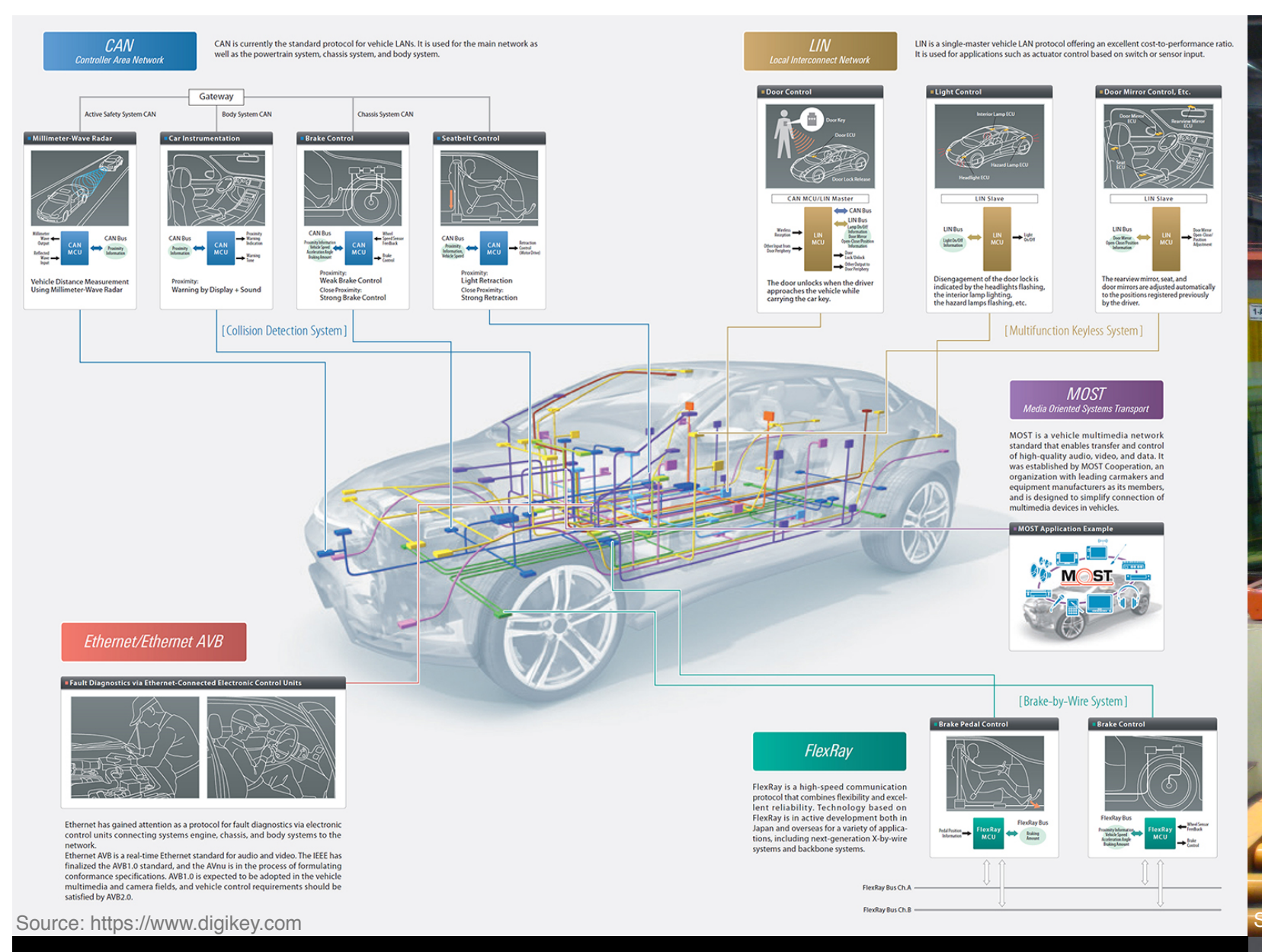
How reliable is your car under EMI?

Quantifying the resiliency of networked control systems to EMI-induced transient faults

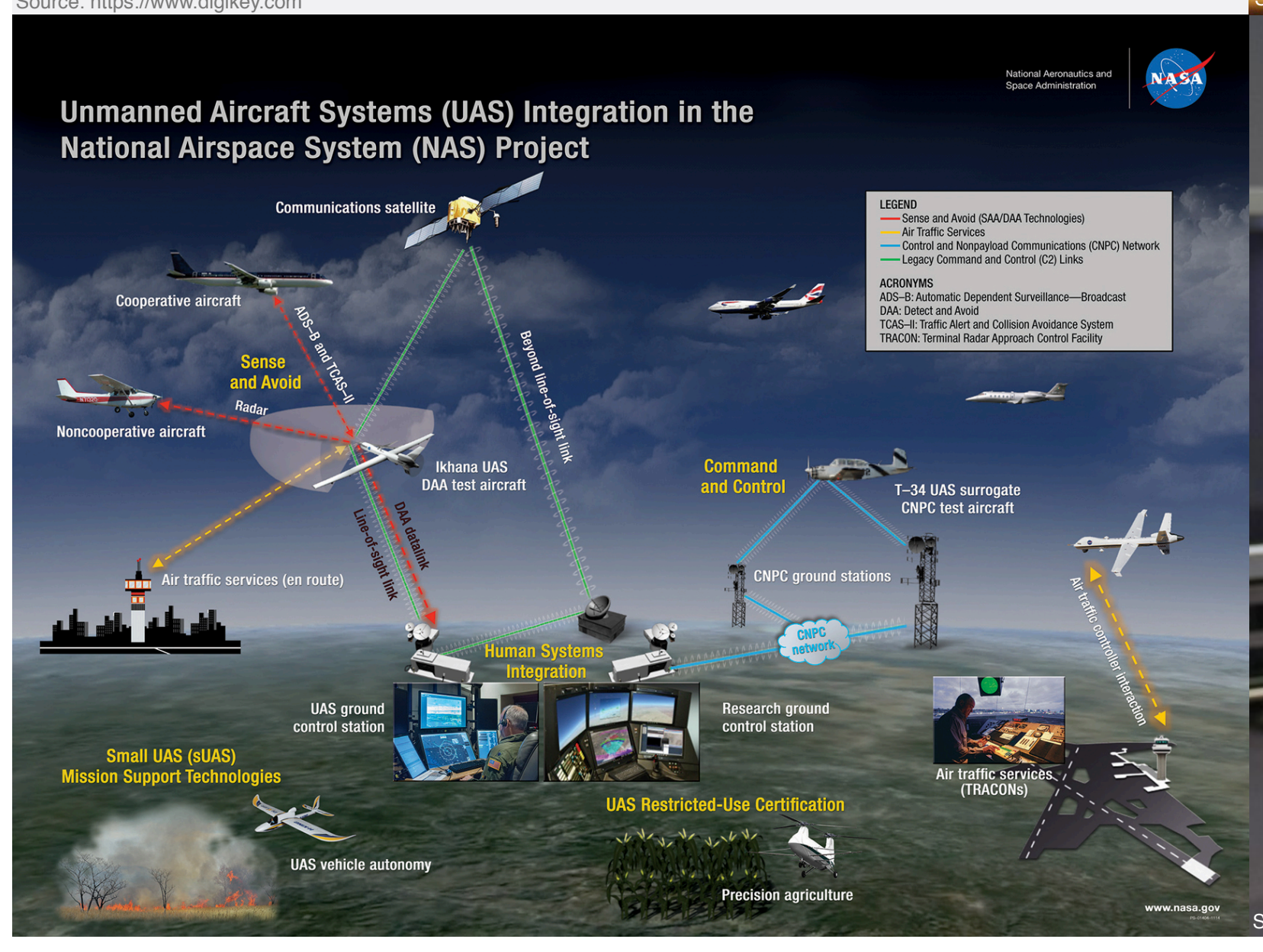
Arpan Gujarati
Mitra Nasri
Björn B. Brandenburg

MAX PLANCK INSTITUTE FOR SOFTWARE SYSTEMS



Source: https://www.digikey.com

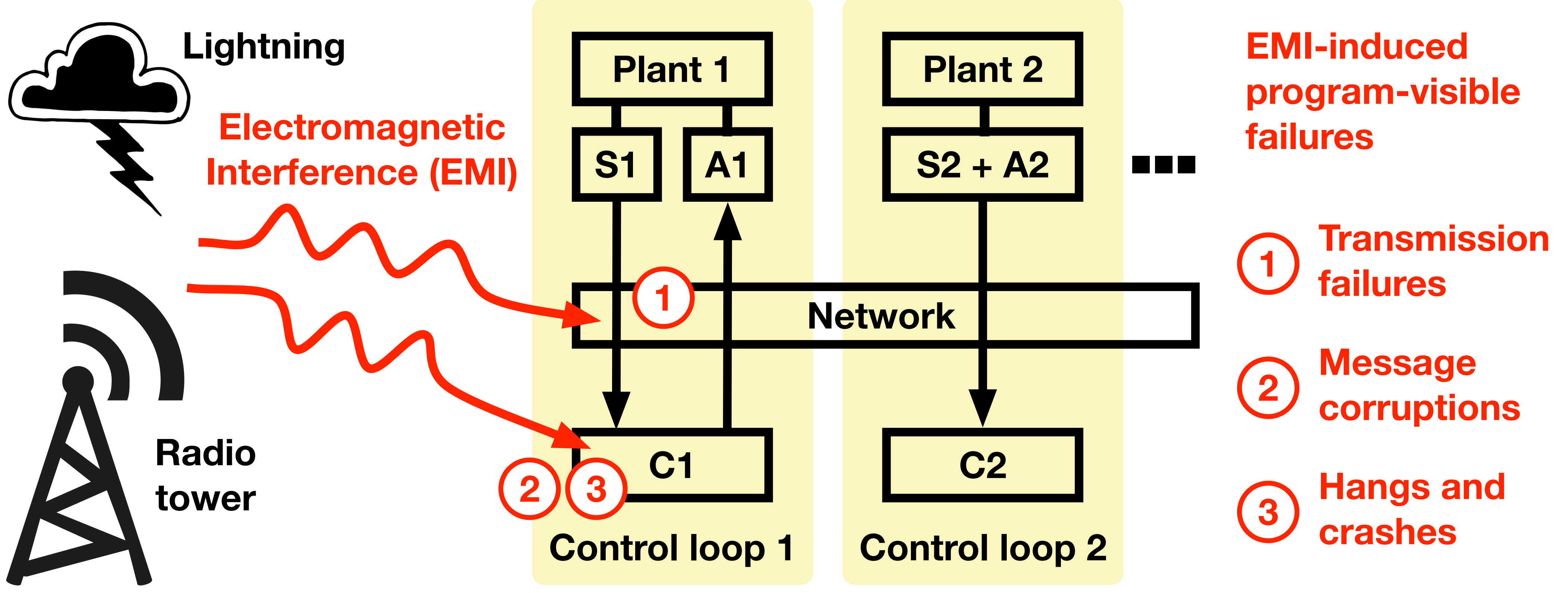
Source: https://commons.wikimedia.org/wiki/File:Float_Glass_Unloading.jpg


Unmanned Aircraft Systems (UAS) Integration in the National Airspace System (NAS) Project
NASA
Communications satellite
Cooperative aircraft
Sense and Avoid
Noncooperative aircraft
Command and Control
Human Systems Integration
UAS Restricted-Use Certification
Small UAS (sUAS) Mission Support Technologies
www.nasa.gov

Source: http://wonderfulengineering.com

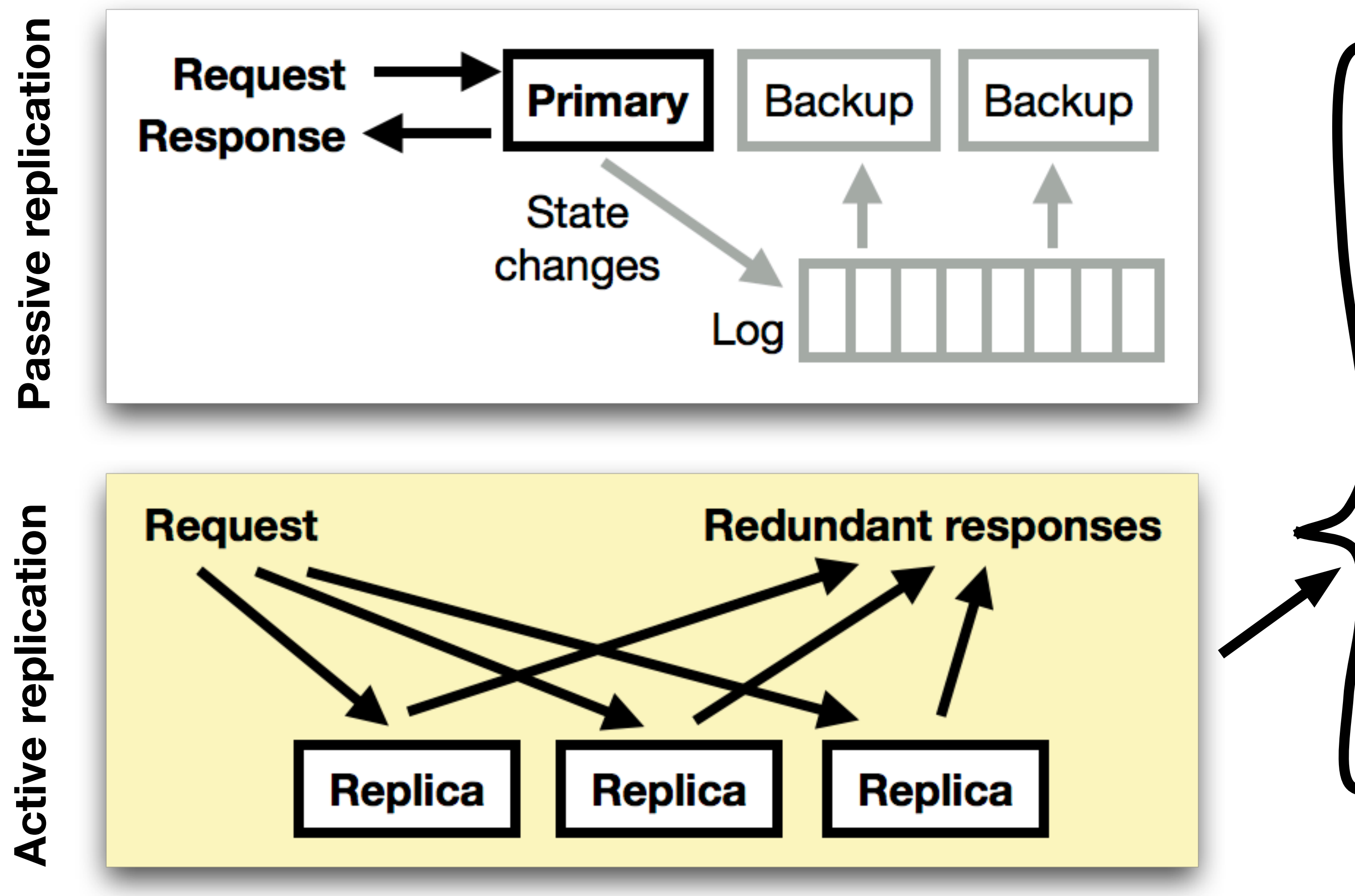
Networked Control Systems (NCS)

= multiple control loops + distributed hosts
+ shared communication network



Safety-critical NCS must be fail-operational

i.e., continue functioning despite EMI-induced failures



Active replication is often used because

- NCSs are time-sensitive
- they may contain high-frequency control loops

Problem

What is a good active replication scheme?

Objective: meet the dependability requirements

Constraints: size, weight, power, and cost

Opportunity: controller inherently robust to occasional disturbances

Solution: Quantifying NCS resiliency to EMI-induced transient faults

… to help engineers design reliable systems under resource budgets or without over-provisioning

Step 1: **P (** single control loop iteration **"fails")**

Actuation in the iteration deviates from the expected actuation in a failure-free iteration

But the control system may remain stable despite a few failed iterations!

- CAN-based NCS model
- Probabilistic failure model
- Fault tree analysis
- Simple majority voter for redundancy suppression

Step 2: **P (** control loop **"fails beyond recovery")**

The control system cannot be stabilized again, e.g., an inverted pendulum crashes on the ground

- Using Step 1
- (m,k)-firm model to characterize controller robustness i.e., at least m out of k consecutive iterations must not fail
- Failures-in-time analysis, i.e., expected failures in one billion operating hours