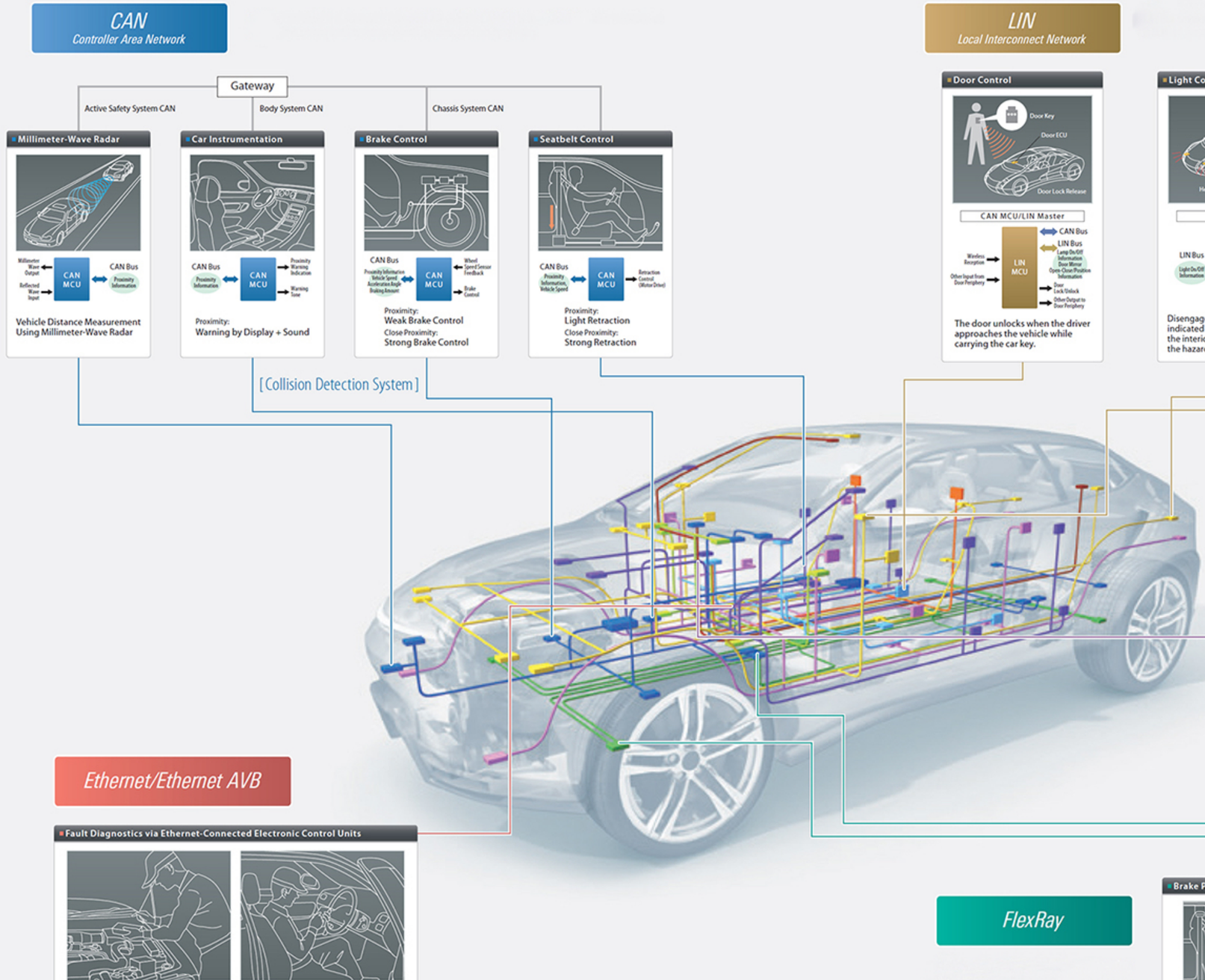
How reliable is your car under EMI?

Quantifying the Resiliency of Networked Control Systems to Transient Faults

Arpan Gujarati
Mitra Nasri
Björn B. Brandenburg

Max Planck Institute for Software Systems

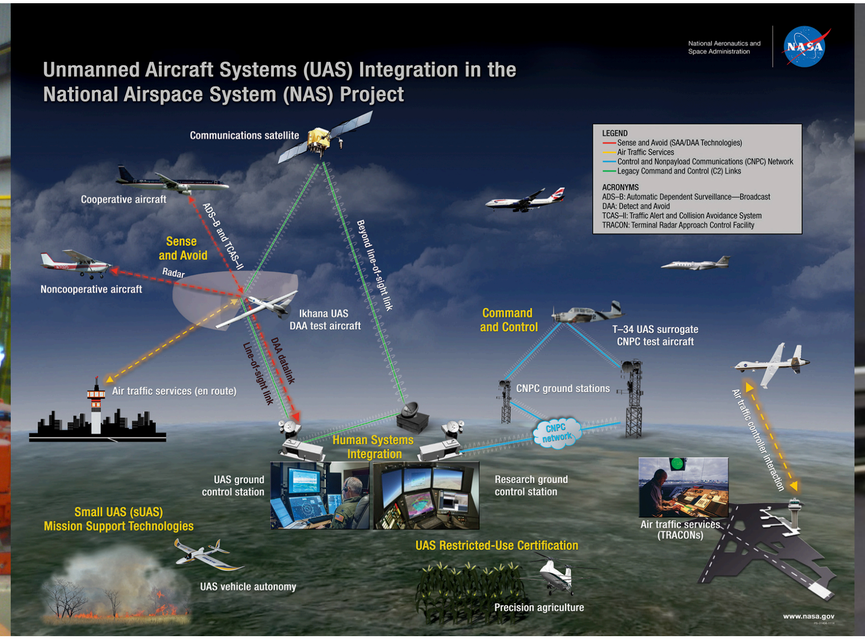


Source: https://www.digikey.com/en/articles/techzone/2014/jul/what-engineers-need-to-know-when-selecting-an-automotive-qualified-mcu-for-vehicle-applications

Networked Control Systems (NCS)

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

Factory Automation



Source: https://www.nasa.gov/sites/default/files/thumbnails/image/uas-nas-integration-lg.jpg

Unmanned Vehicle Navigation

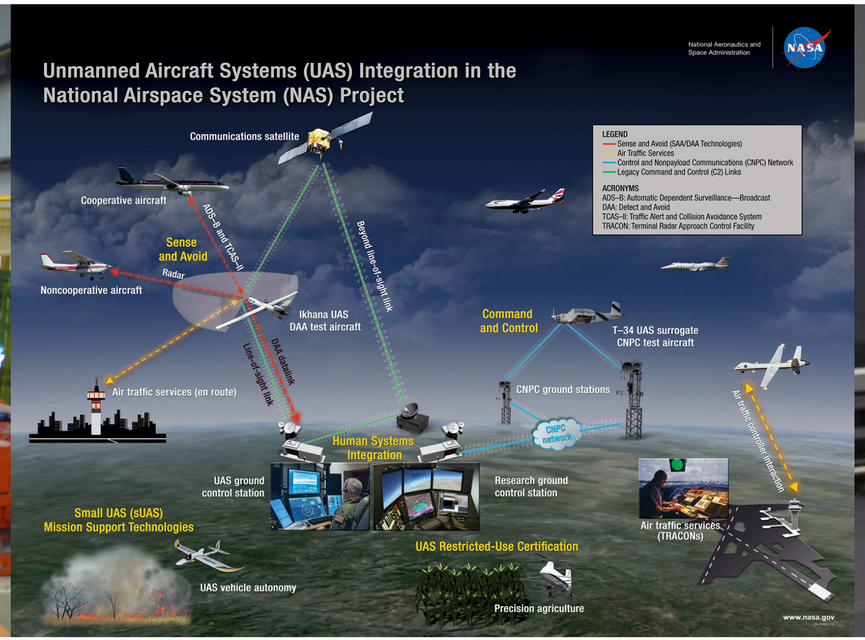
Source: http://wonderfulengineering.com/care-o-bot-is-your-personal-robotic-friend-that-will-help-you-with-everyday-tasks/

Domestic Robots

Networked Control Systems (NCS)

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

Factory Automation



Source: https://www.nasa.gov/sites/default/files/thumbnails/image/uas-nas-integration-lg.jpg

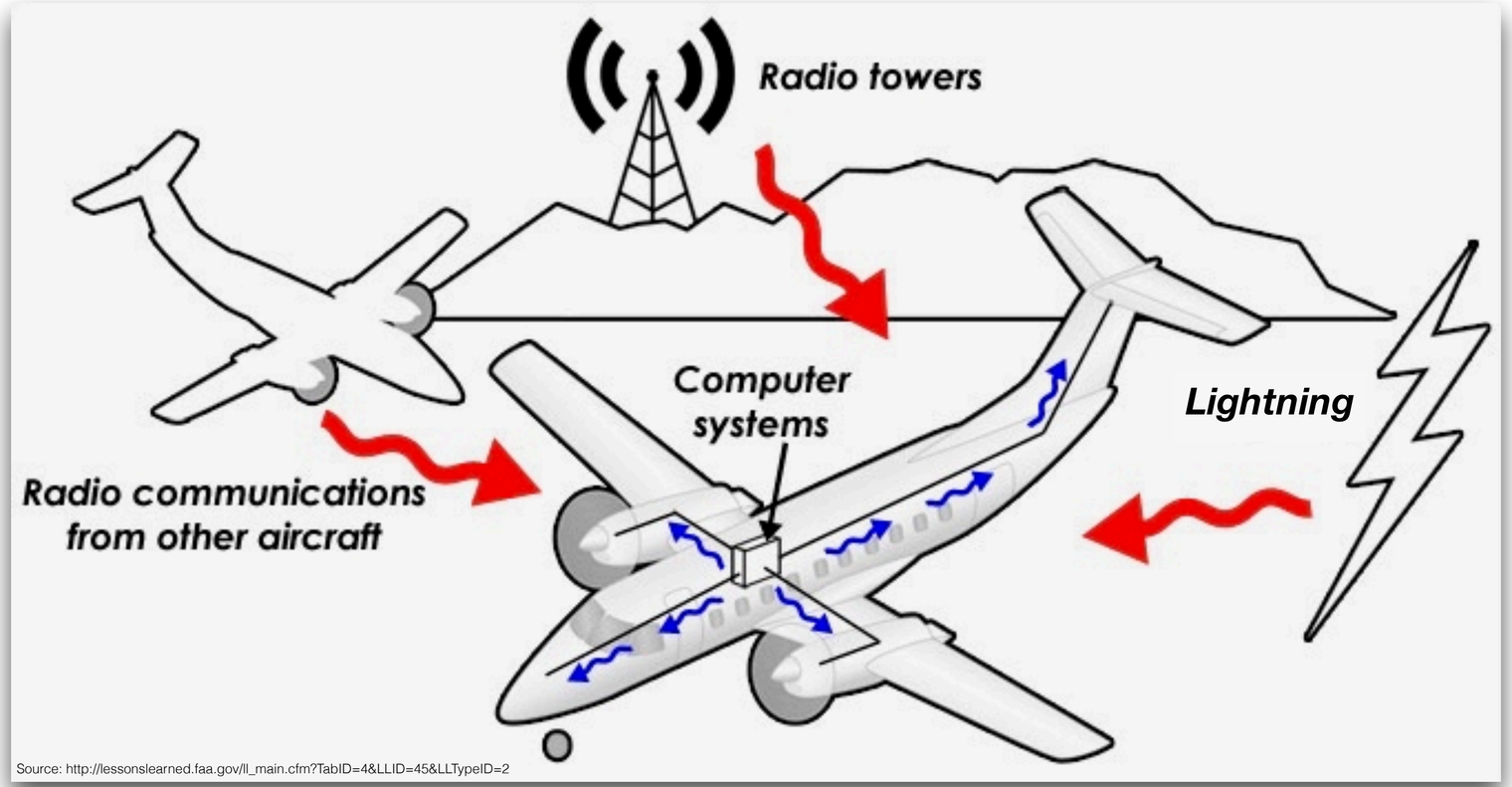
Unmanned Vehicle Navigation

Source: http://wonderfulengineering.com/care-o-bot-is-your-personal-robotic-friend-that-will-help-you-with-everyday-tasks/

Domestic Robots

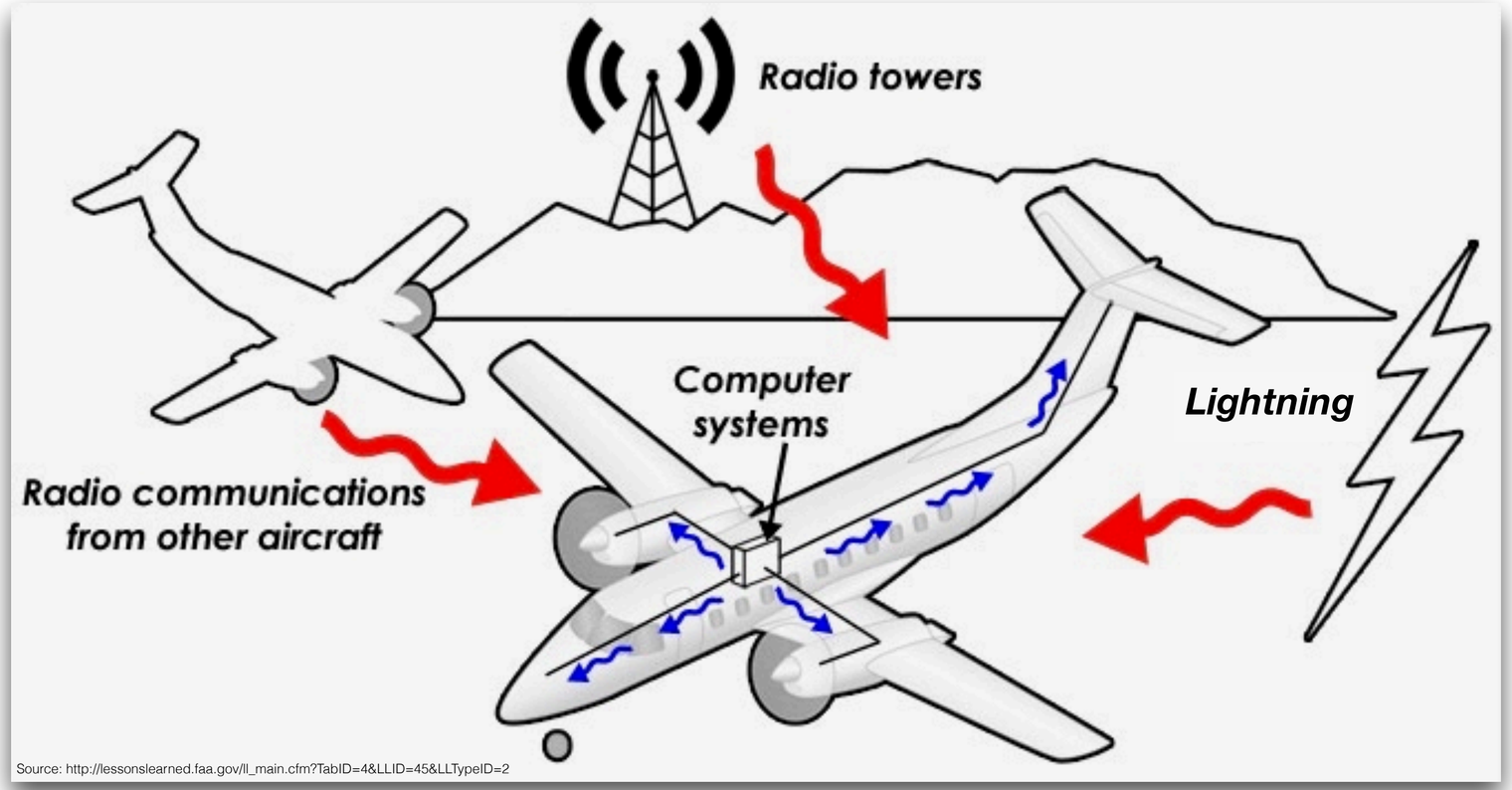
NCS = Multiple control loops + Distributed nodes
+ Shared communication network

NCSs are susceptible to **electromagnetic interference (EMI)**



Source: http://lessonslearned.faa.gov/ll_main.cfm?TabID=4&LLID=45&LLTypeID=2

NCSs are susceptible to **electromagnetic interference (EMI)**



Source: http://lessonslearned.faa.gov/ll_main.cfm?TabID=4&LLID=45&LLTypeID=2

Program-visible failures

Transmission failures

Message corruptions

Hangs and crashes

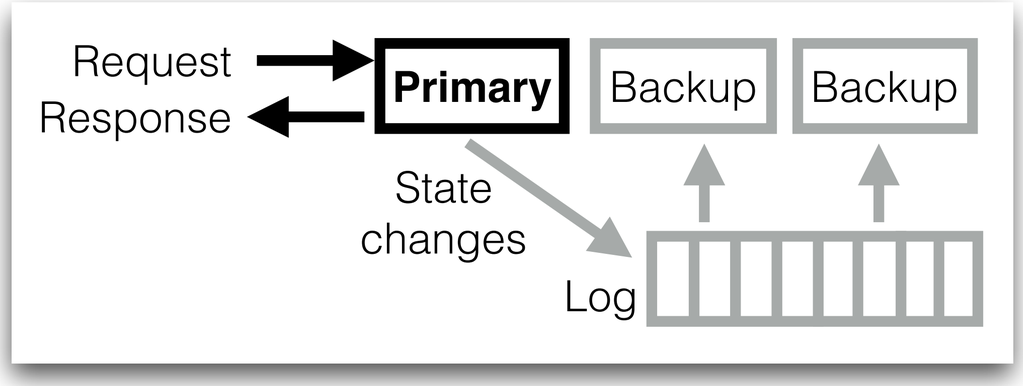
Safety-critical NCSs must be **fail-operational**

Continue functioning despite EMI-induced failures

Safety-critical NCSs must be **fail-operational**

Continue functioning despite EMI-induced failures

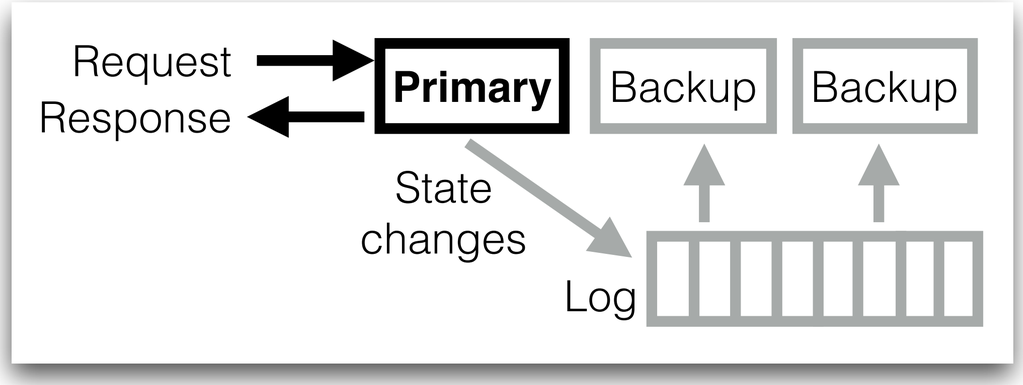
Passive replication



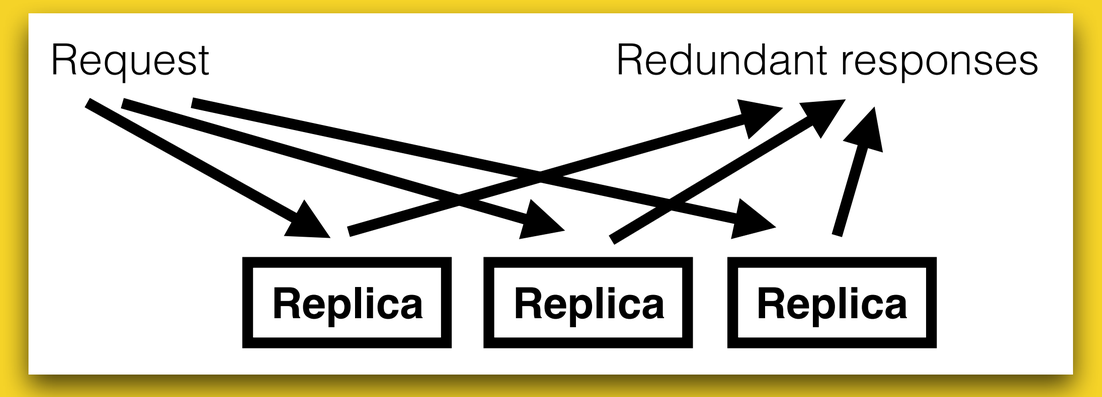
Safety-critical NCSs must be **fail-operational**

Continue functioning despite EMI-induced failures

Passive replication



Active replication



... often used for time-sensitive NCSs

What is a **good** **active replication scheme**?

- Which tasks should be replicated?
- What should be their replication factors?
- What should be the replica to node mapping?

What is a **good** **active replication scheme**?

Objective

Meet the dependability requirements

- Which tasks should be replicated?
- What should be their replication factors?
- What should be the replica to node mapping?

What is a **good** **active replication scheme**?

Objective

Meet the dependability requirements

Constraints

Size, weight, power, and cost

- ✦ Which tasks should be replicated?
- ✦ What should be their replication factors?
- ✦ What should be the replica to node mapping?

What is a **good** **active replication scheme**?

Objective

Meet the dependability requirements

Constraints

Size, weight, power, and cost

Opportunity

Control may be inherently robust to occasional disturbances

- ✦ Which tasks should be replicated?
- ✦ What should be their replication factors?
- ✦ What should be the replica to node mapping?

What is a **good** **active replication scheme**?

Objective

Meet the dependability requirements

Constraints

Size, weight, power, and cost

Opportunity

Control may be inherently robust to occasional disturbances

- ✦ Which tasks should be replicated?
- ✦ What should be their replication factors?
- ✦ What should be the replica to node mapping?

This work

Quantifying the resiliency of NCSs under EMI-induced transient faults

Features

NCSs connected using the widely used
Controller Area Network (CAN bus)

Features

NCSs connected using the widely used **Controller Area Network (CAN bus)**

(m,k)-firm model to characterize the inherent robustness of each control loop

Features

NCSs connected using the widely used **Controller Area Network (CAN bus)**

(m,k)-firm model to characterize the inherent robustness of each control loop

Fine-grained analysis at the granularity of message exchanges between nodes to reduce the analysis pessimism

Features

NCSs connected using the widely used **Controller Area Network (CAN bus)**

(m,k)-firm model to characterize the inherent robustness of each control loop

Fine-grained analysis at the granularity of message exchanges between nodes to reduce the analysis pessimism

Reliability computed as **Failures-In-Time (FITs)**, an industry-standard metric

Features

NCSs connected using the widely used **Controller Area Network (CAN bus)**

(m,k)-firm model to characterize the inherent robustness of each control loop

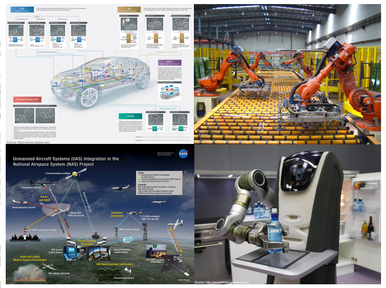
Fine-grained analysis at the granularity of message exchanges between nodes to reduce the analysis pessimism

Reliability computed as **Failures-In-Time (FITs)**, an industry-standard metric

How reliable is your car under EMI?

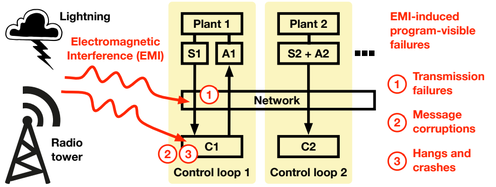
Quantifying the resiliency of networked control systems to EMI-induced transient faults

Arpan Gujarati
Mitra Nasri
Björn B. Brandenburg
MAX PLANCK INSTITUTE FOR SOFTWARE SYSTEMS



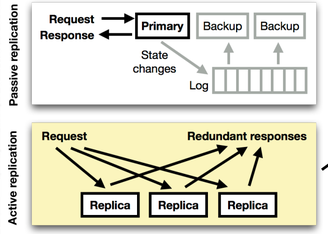
Networked Control Systems (NCS)

= 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")**

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

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!

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

- 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

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