DELAY SAFETY FOR CYBER-PHYSICAL SYSTEMS

Sept 2018

Prof. Jean-Yves Le Boudec
LCA2
Cyber-Physical Systems

Physical systems controlled by software
  factory, electrical grid, car, train, traffic flows, air plane, drone, etc.

Software is moving from simple to complex
Delay Faults

Delay fault = software controller does not perform its task within expected delay

Delay faults at critical instants can lead to accidents
Solution: replicated controllers

Smart grid controller “Commelec”
Performance Tests
Example: Masking Delay Faults in Replicated Controllers

Maaz Mashood, EPFL, PhD Thesis, August 2018

Without Axo


With Axo
Issues with Replication: Interleaving is Unsafe

Solution: lightweight agreement on input (Quarts) with delay guarantees

[Maaz Mashood and Wajeb Saab’s PhD dissertations]

Deterministic Network

Traditional cabling replaced by Network
Issue is to guarantee
end-to-end latency and avoid losses

Tool: network calculus

Challenges

1. Delay guarantees for replicated controllers
2. Certified Delay Guarantees for Deterministic Network
3. Interplay between Network and Controllers
PhD Opportunities in LCA2 (Le Boudec)

Verifiable Delay Guarantees
for Software Controllers and Deterministic networks

Required skills: software, logical thinking, discrete maths, protocols

Benefits:
1. participate in the cyber-physical revolution
2. become an expert in the growing field of internet of things