Mixed Physical and Cyber Clocks for CPS

Dionisio de Niz
SEI – Carnegie Mellon

New Clockwork for CPS Workshop
Oct 25-26 2012

© 2012 Carnegie Mellon University

Copyright 2012 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM-0000082

Role of clocks in CPS

Order events across distributed processes

Synchronize cyber and physical processes

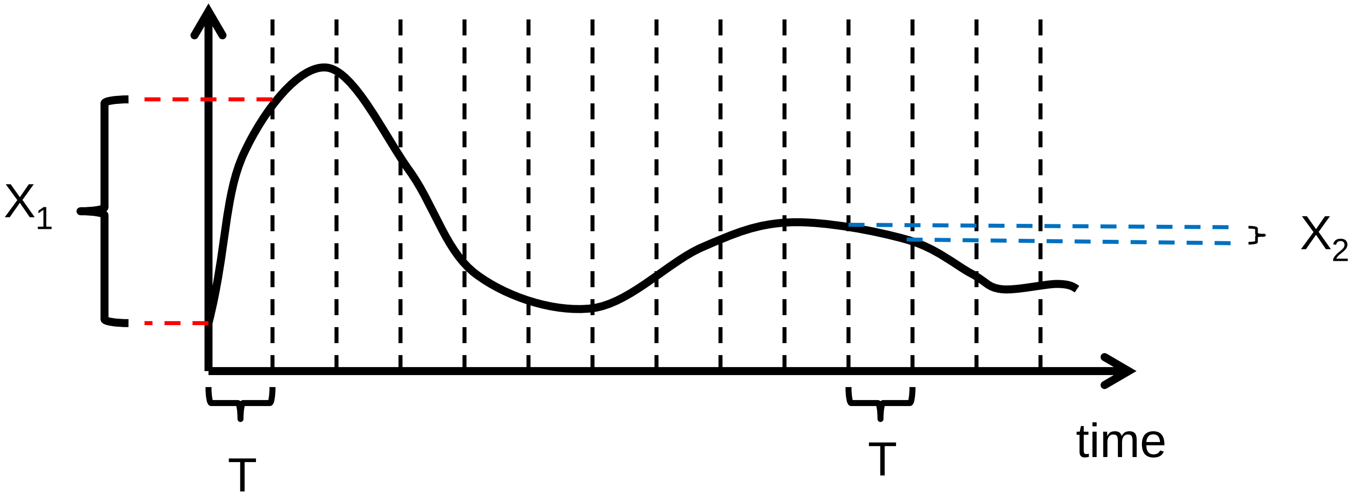
Synchronize different cyber processes

Synchronize different physical processes

© 2012 Carnegie Mellon University

Synchronize cyber processes with physical processes

Traditionally done by fixing a “sampling” period



Drawbacks:

Variation in the evolution of physical process can be large (X_1>>X_2)

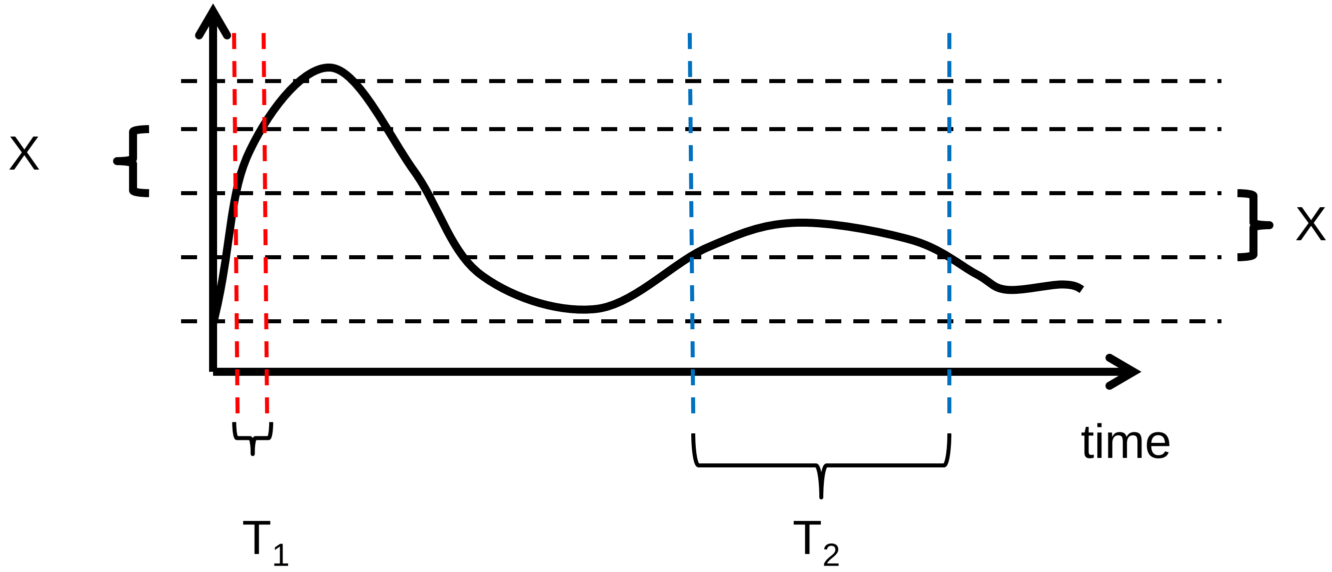
Need to force minimum period

Pessimistic resource utilization for guaranteed deadlines

© 2012 Carnegie Mellon University

Synchronize cyber processes with physical processes

Approach: Let the physical process drive the computation



Alternative approaches:
Event-based control
Self-triggered control

Improved resource utilization for guaranteed deadlines

© 2012 Carnegie Mellon University

Synchronizing different cyber processes

Using a "common" clock

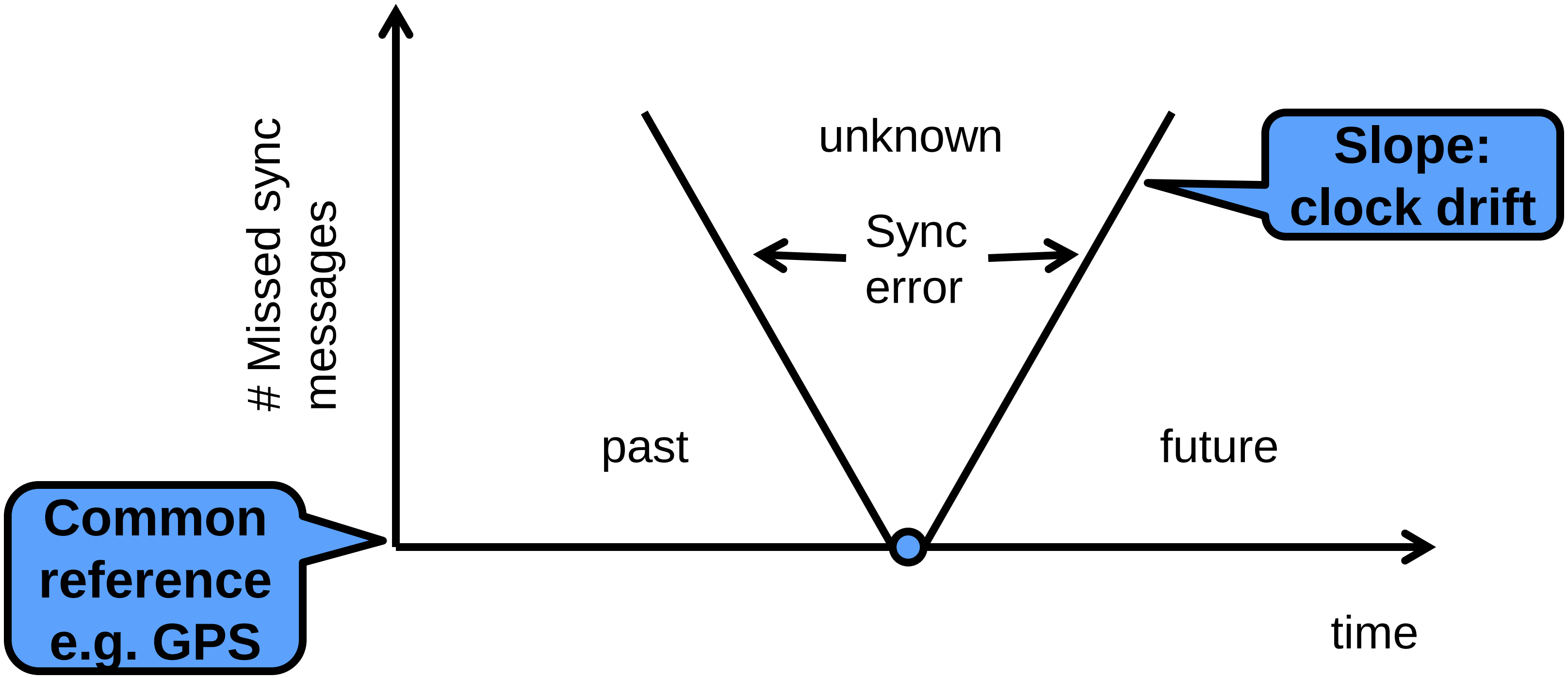
- Common reference (e.g. GPS)
- Synchronized local clocks (e.g. NTP)
- Logical clocks

Reliability needs to be taken into account

- Loss of satellite signals (GPS)
- Synchronization message loss (NTP)
- Synchronization message delays (logical clocks)

© 2012 Carnegie Mellon University

Synchronized cyber-clock accuracy



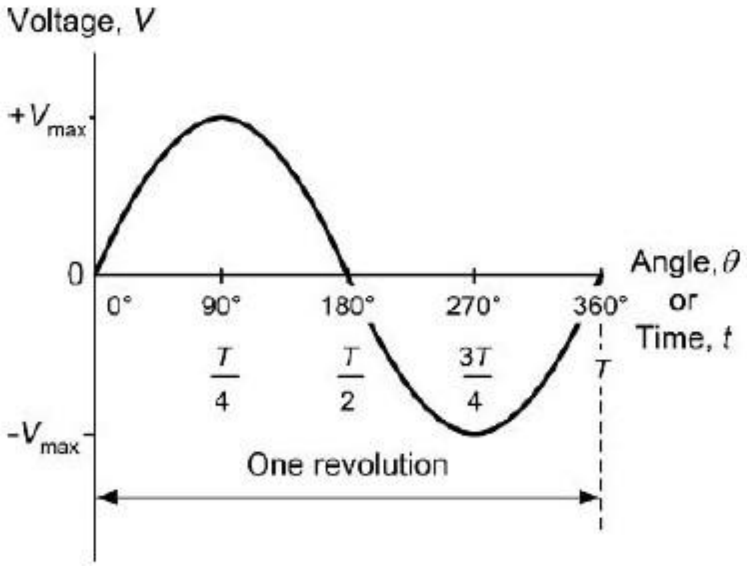
From the loss of the common reference
every time we miss a sync message the sync error increases

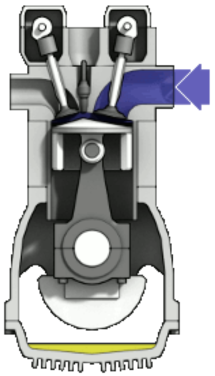
© 2012 Carnegie Mellon University

Common physical processes in CPS

In a CPS cyber processes may observe a common physical process (physical variable)

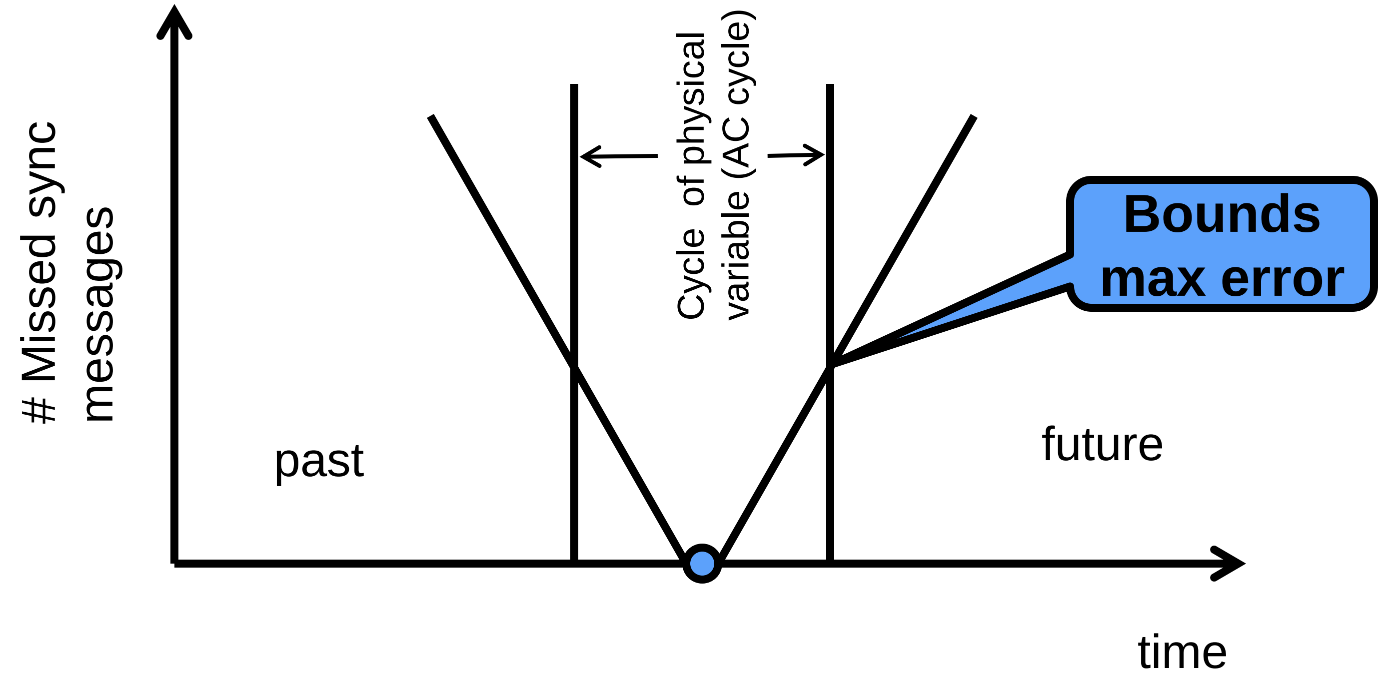
- AC cycle in the smart grid
- Crankshaft angle in an engine





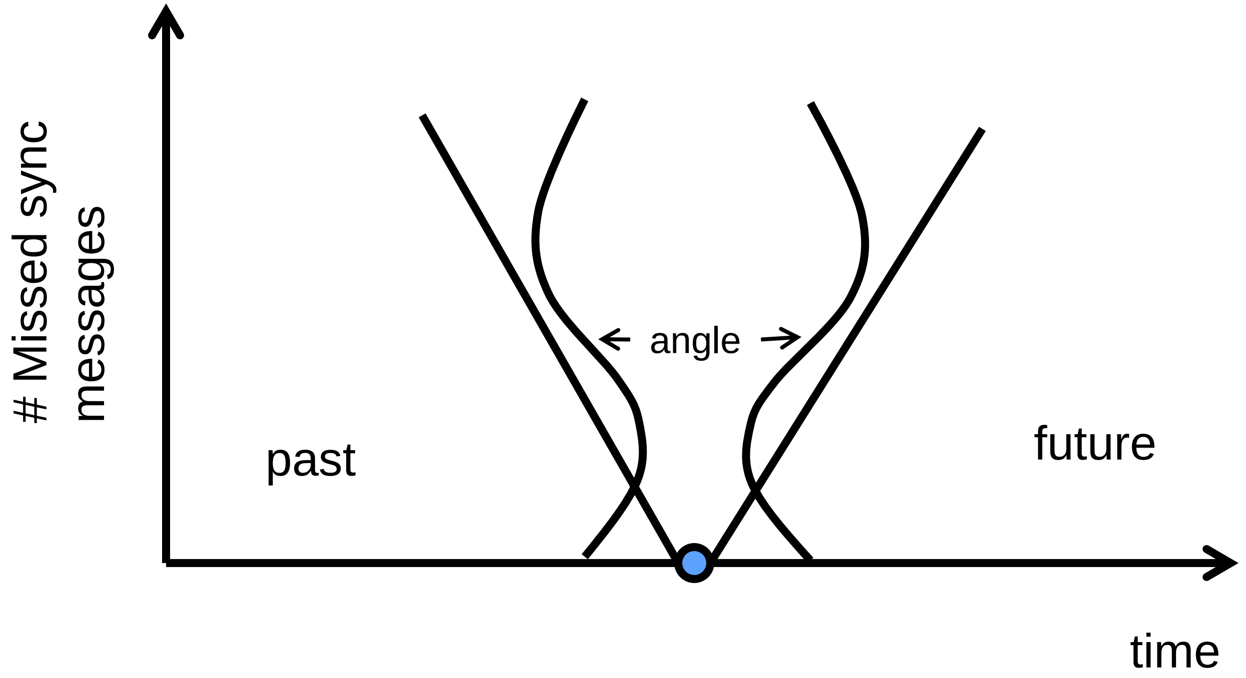
© 2012 Carnegie Mellon University

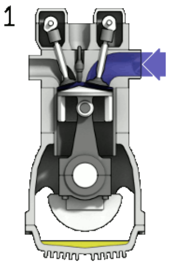
Combining sync clocks with physical variable



© 2012 Carnegie Mellon University

Physical process with variable cycles



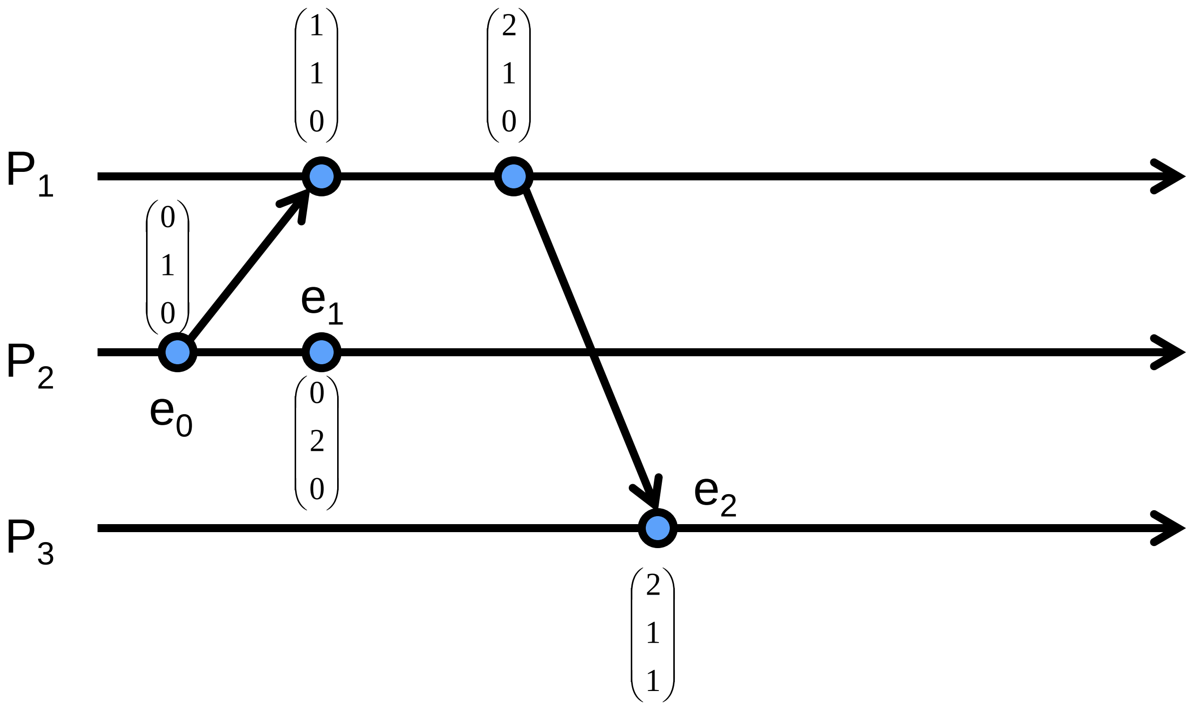


In CPS time is frequently a proxy for physical variable
Hence, cyber processes only require sync with physical variable

E.g. open/close valves sync with fuel injection

© 2012 Carnegie Mellon University

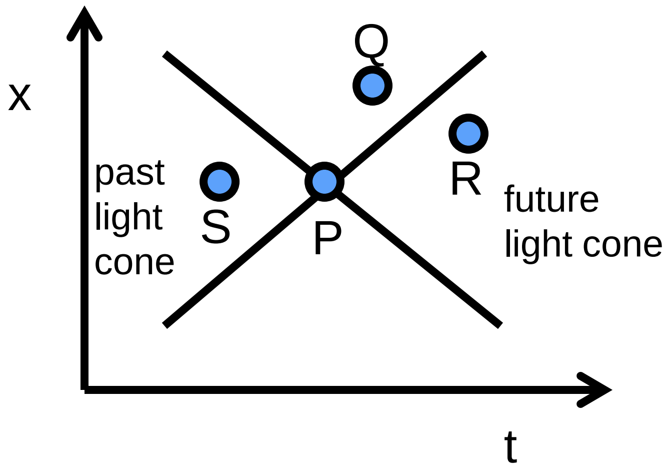
Logical (vector) clocks can also complement sync

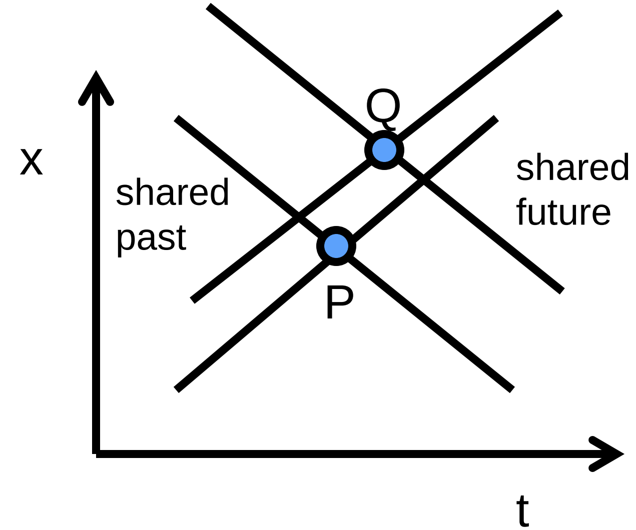


But they are also sensitive to “missed” syncs

© 2012 Carnegie Mellon University

Mattern related vector clocks to Minkowski's spacetime

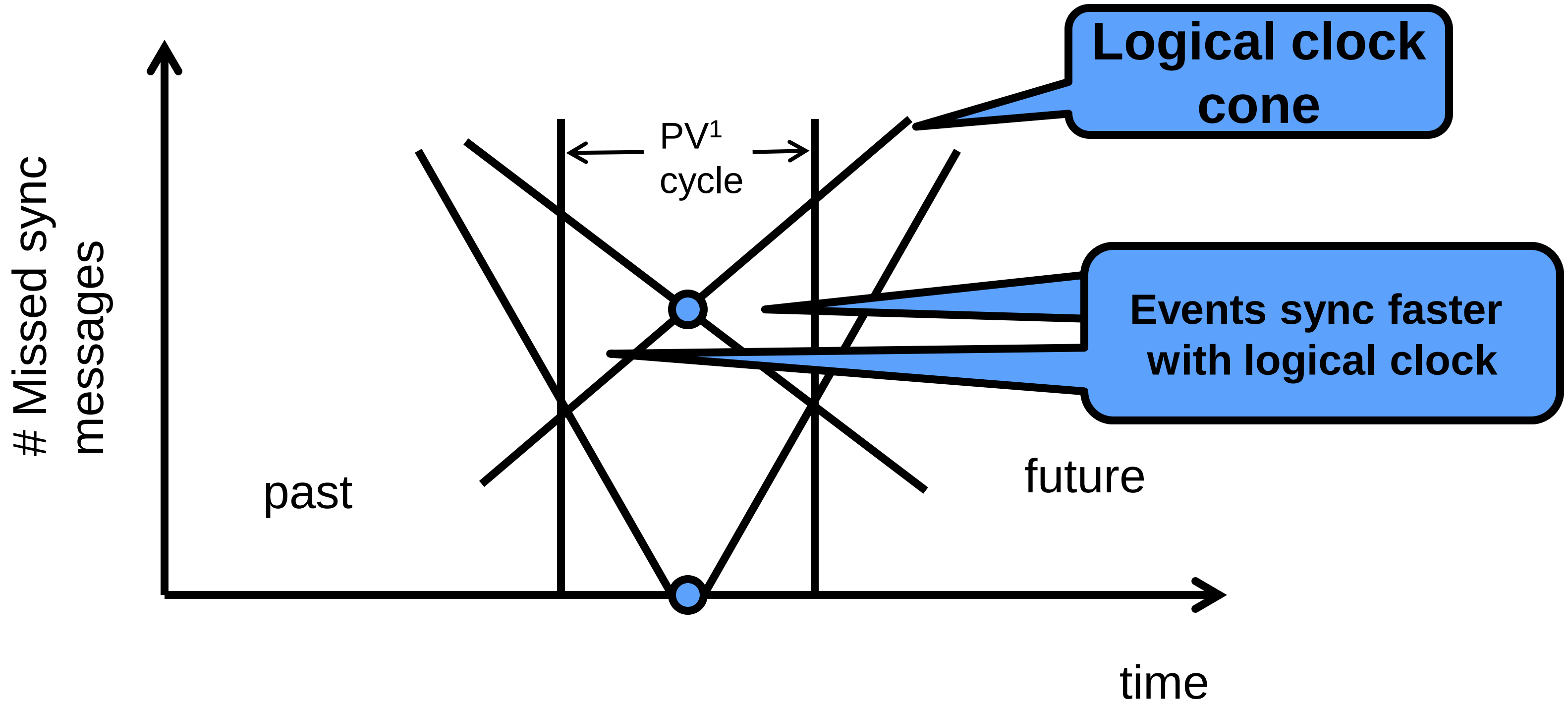




In CPS "x" can also be related to a physical variable
(and back to time)

© 2012 Carnegie Mellon University

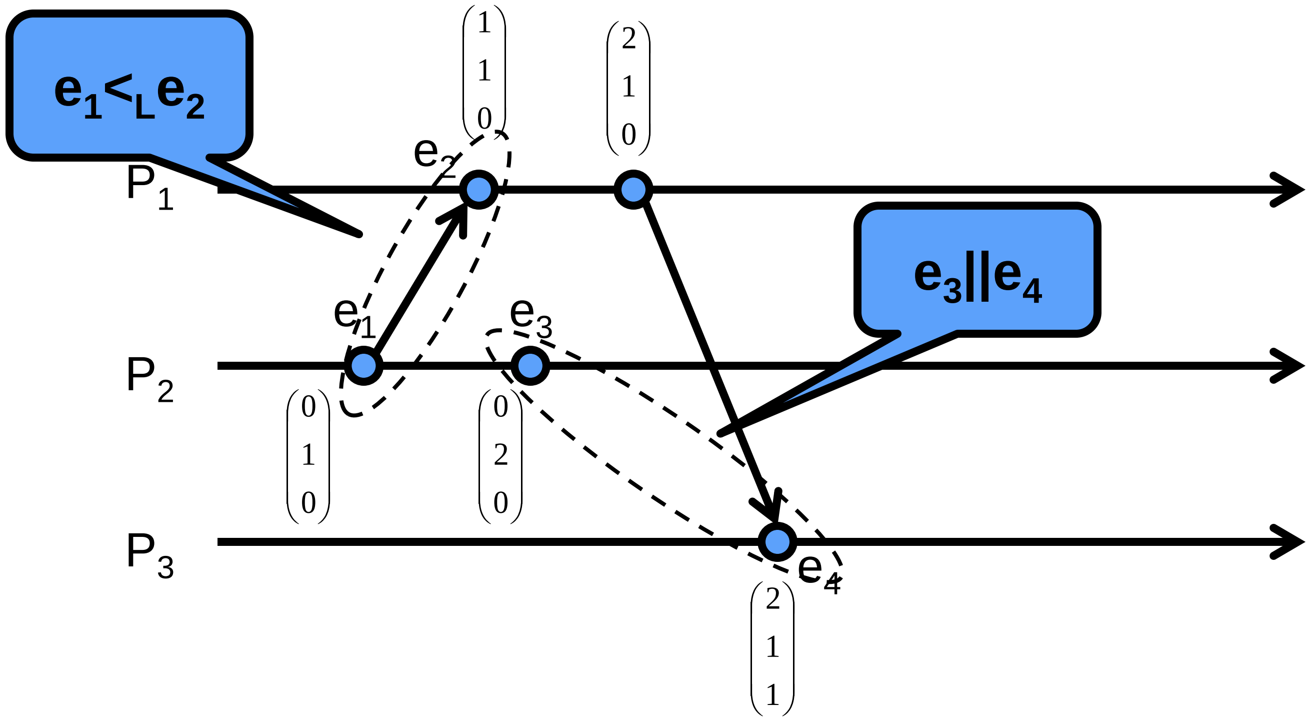
Mixed Physical and Cyber Clocks



[1]PV: physical variable

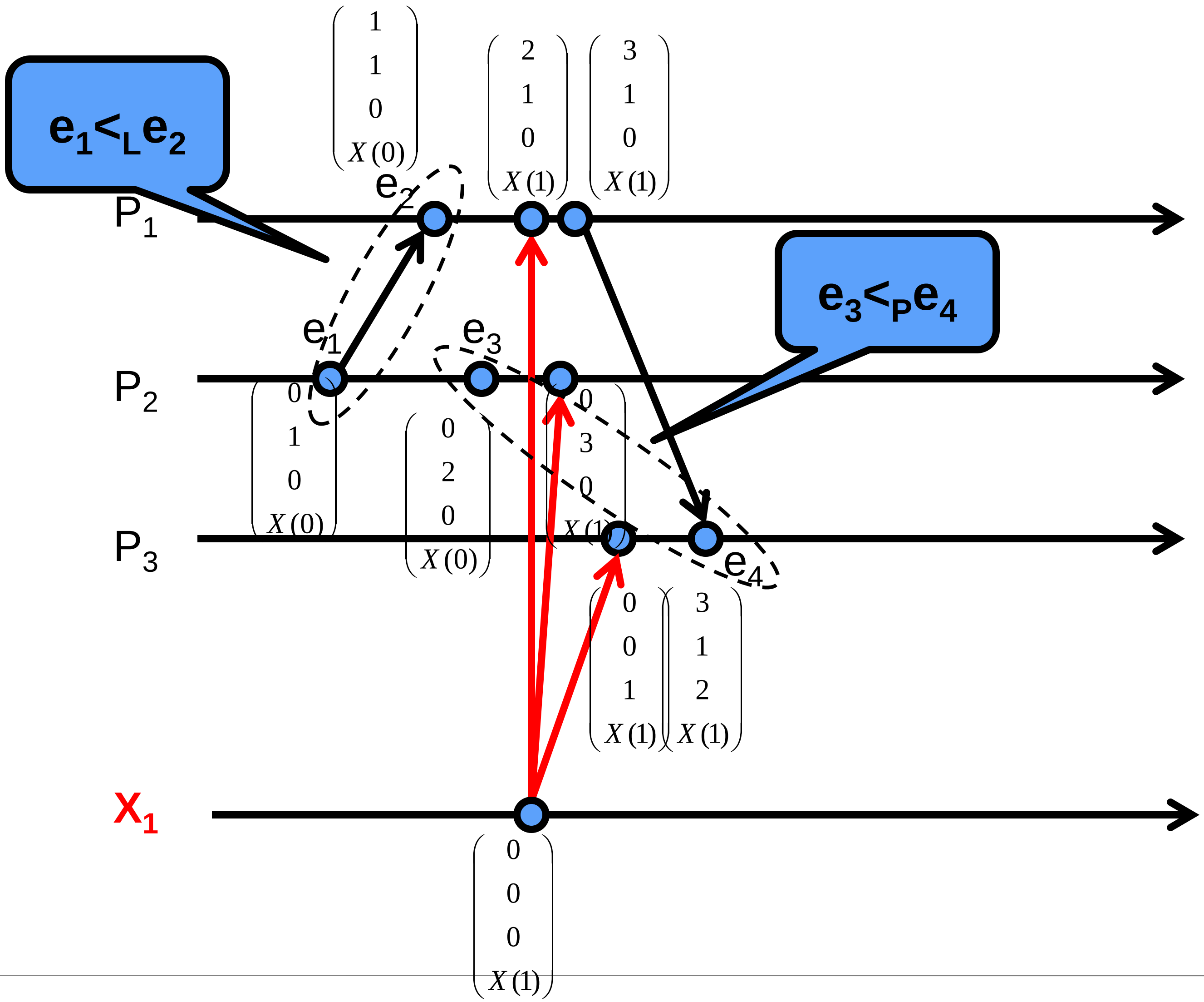
© 2012 Carnegie Mellon University

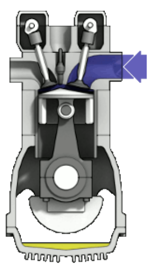
Limitations of Logical Clock



© 2012 Carnegie Mellon University

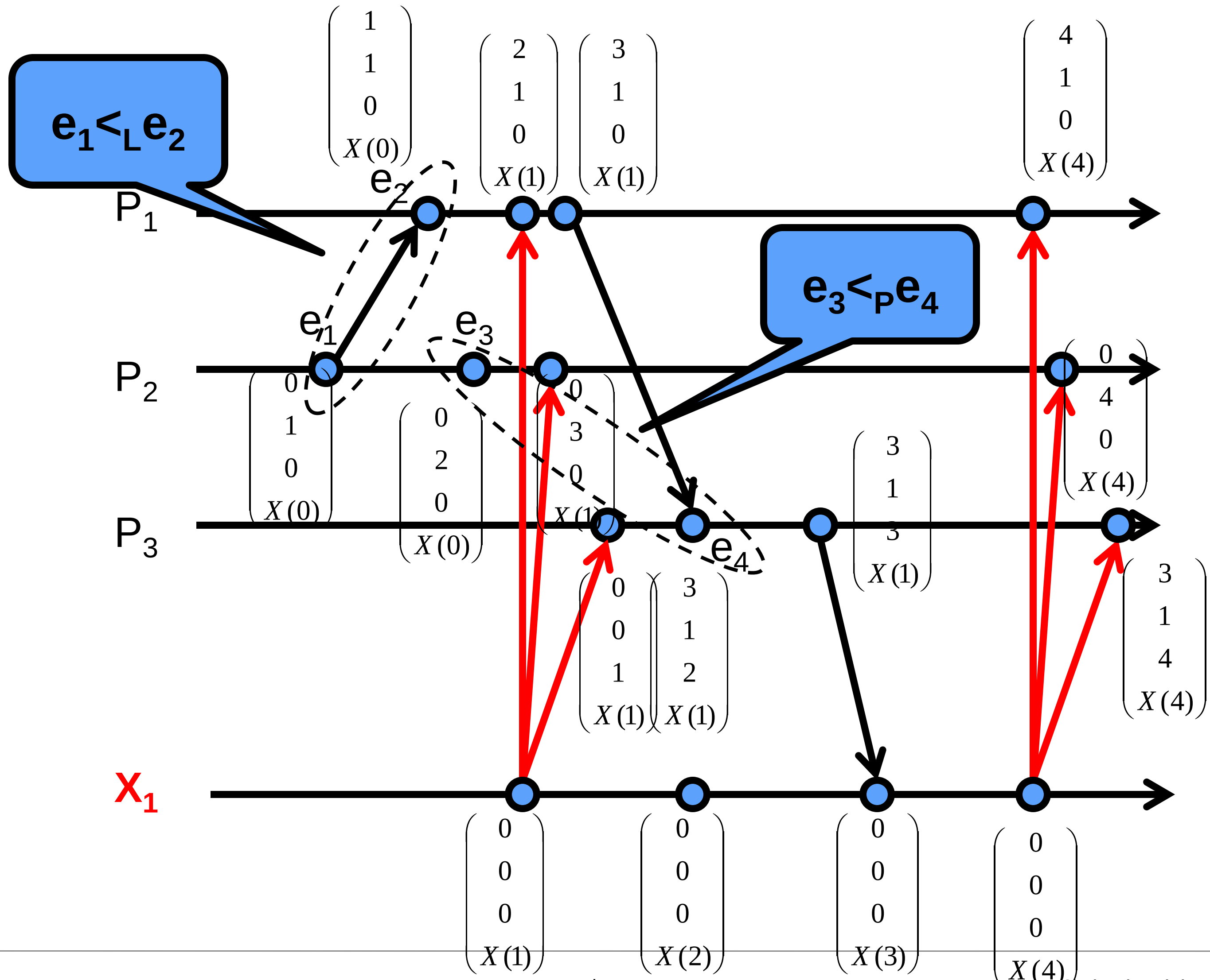
Logical + Physical Clock

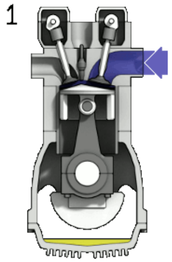


1 

© 2012 Carnegie Mellon University

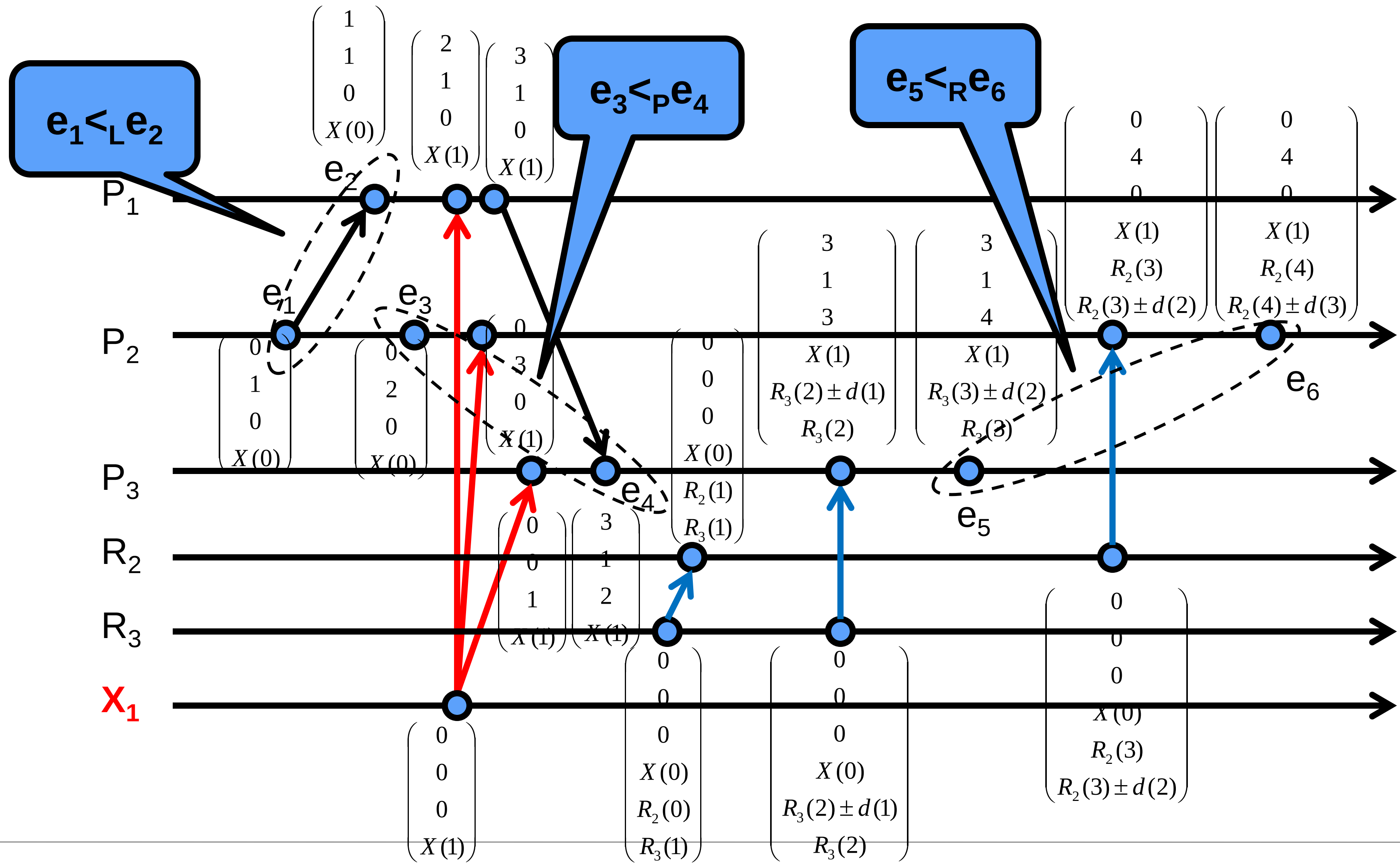
Physical processes also "receive" messages (actuation)





© 2012 Carnegie Mellon University

Logical + Physical Clock + Real-time clock



© 2012 Carnegie Mellon University

Preserving time properties[1]

1. Transitivity
   - Mixed vectors allows transitivity across domains (logical, physical, real-time)
   - But can also exhibits non-transitive concurrency
2. Irreflexibility
3. Linearity
4. Eternity
5. Density
   - Improved but variable density

[1]The Logic of Time. van Benthem.

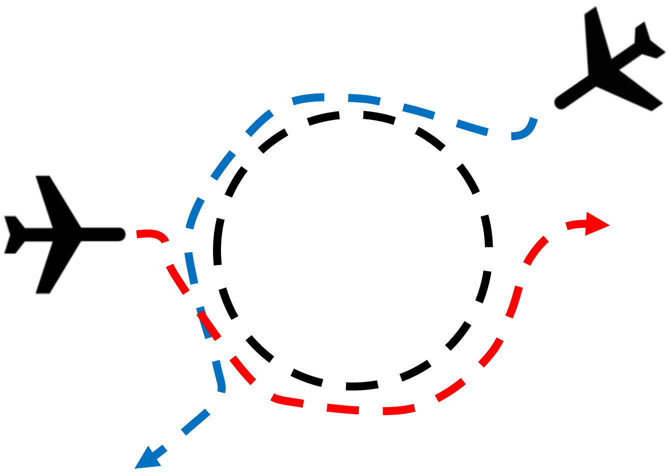
© 2012 Carnegie Mellon University

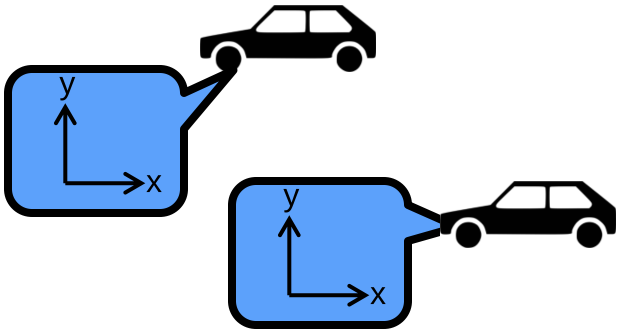
Sync (couple) different physical processes

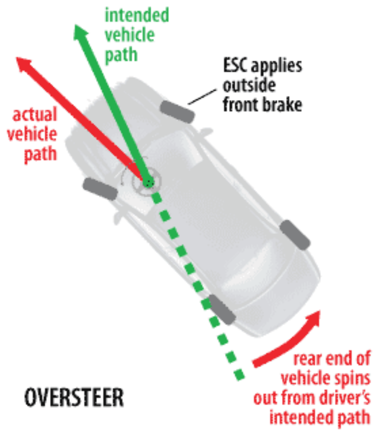
Use cyber-clocks to create a virtual process

Safety

- Airplane collision avoidance maneuvers
- Cooperative collision warning system[1]
- Electronic Stability Control





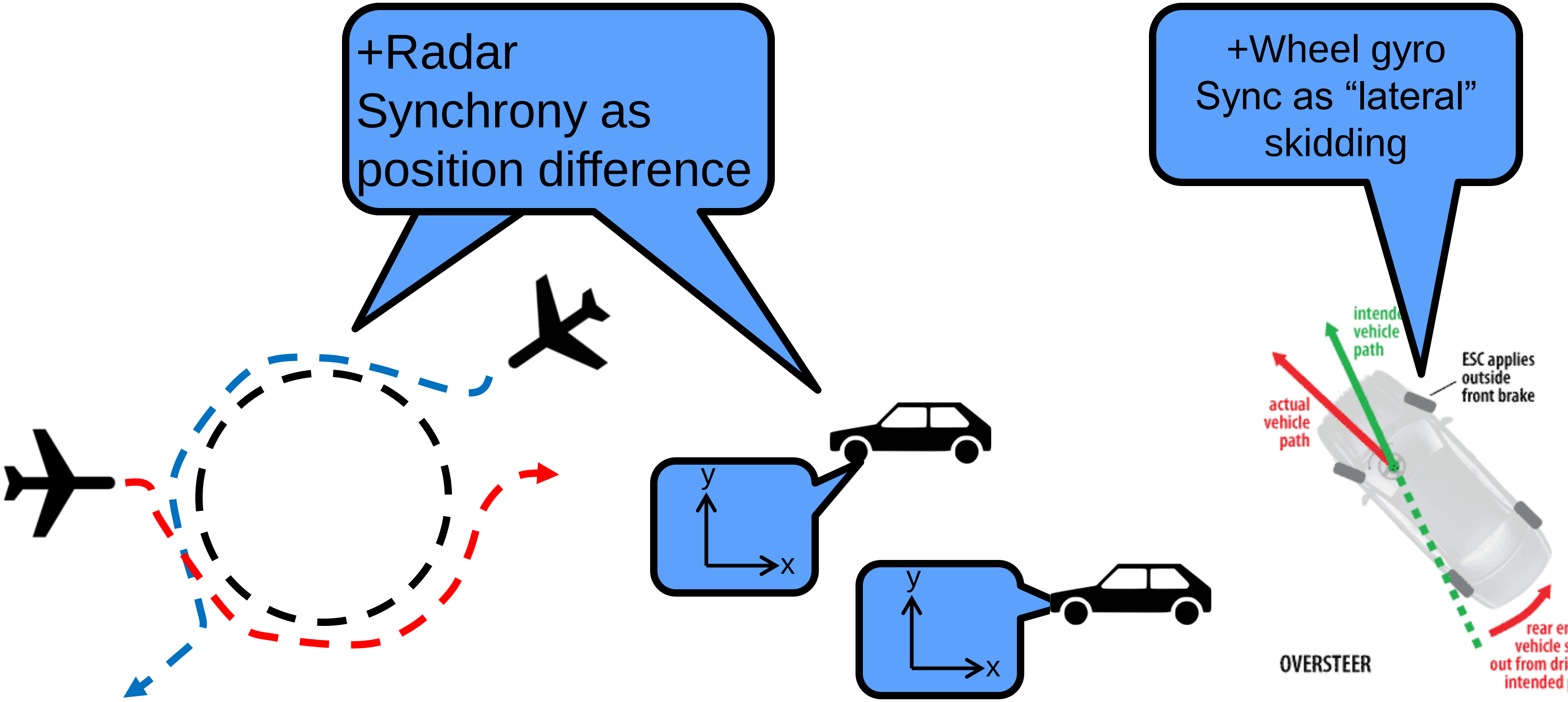


Clock failures can jeopardize coupling

[1]California PATH Research. Sengupta et al.

© 2012 Carnegie Mellon University

Robustness of Mixed Physical and Cyber Clocks



Nissan steer-by-wire:
maybe in market in 2013

© 2012 Carnegie Mellon University

Using mixed clocks: robust agreement

Co-relate cyber agreement with physical agreement

Prevent false faults

- Acknowledge cyber clock timeout but observed physical change
  - Physical model allows the detection “physical clock” advance

False agreement

- Collision avoidance:
  - Agreed roundabout trajectory
  - But no trajectory correction
    - Physical clock timeout: need physical model of expected change

© 2012 Carnegie Mellon University

Concluding Remarks

CPS allows us to revisit the concept of time

- Implementation mechanisms to improve robustness
- Application requirements

Challenges combining physical, cyber, and logical clocks

- Variable density
- Requires building consistent transitivity across domains

Improves synchronization across different types of processes

- Cyber to physical
- Physical to physical

© 2012 Carnegie Mellon University