



Processing Enhancement and Virtualization for Cyber-Physical Computations

Dionisio de Niz and Bjorn Andersson

Next Generation Operating Systems for CPS Workshop

April 15th, 2019



Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

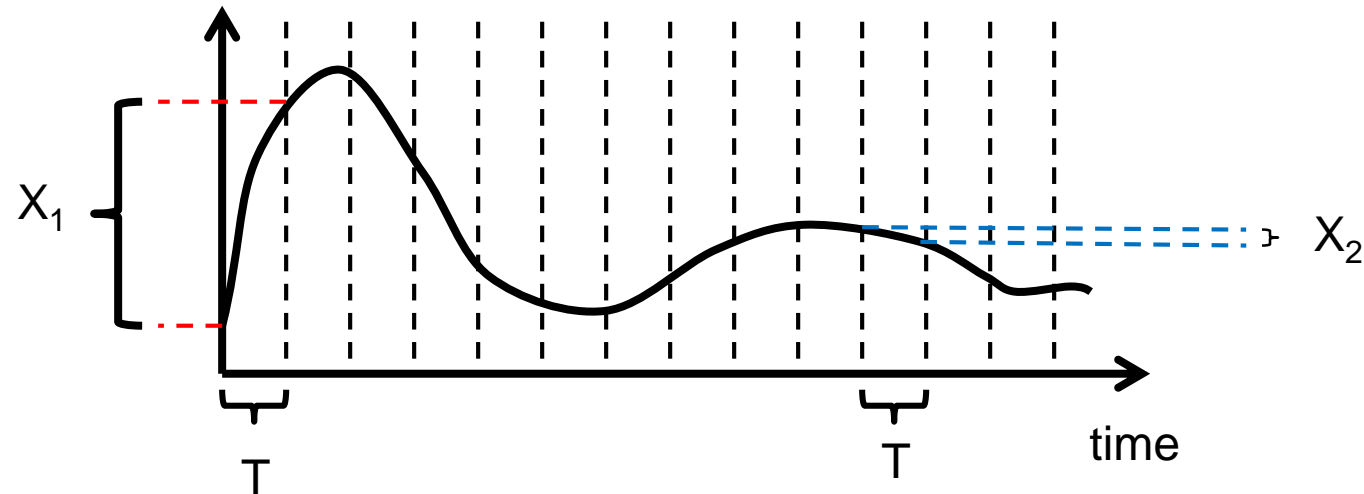
Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0388



Synchronize cyber processes with physical processes

Traditionally done by fixing a “sampling” period



Drawbacks:

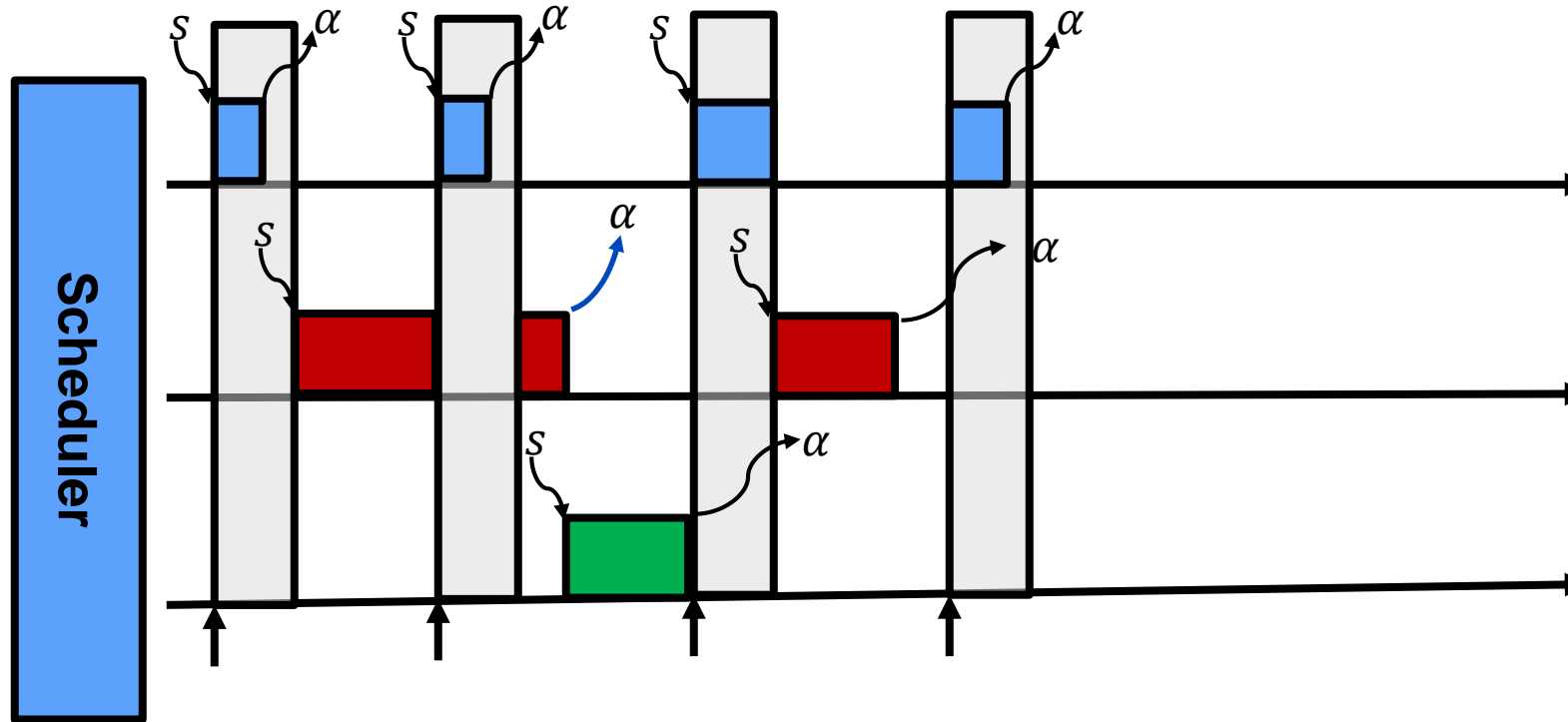
Variation in the evolution of physical process can be large ($X_1 \gg X_2$)

Need to force minimum period

Pessimistic resource utilization for guaranteed deadlines



Processing Budget

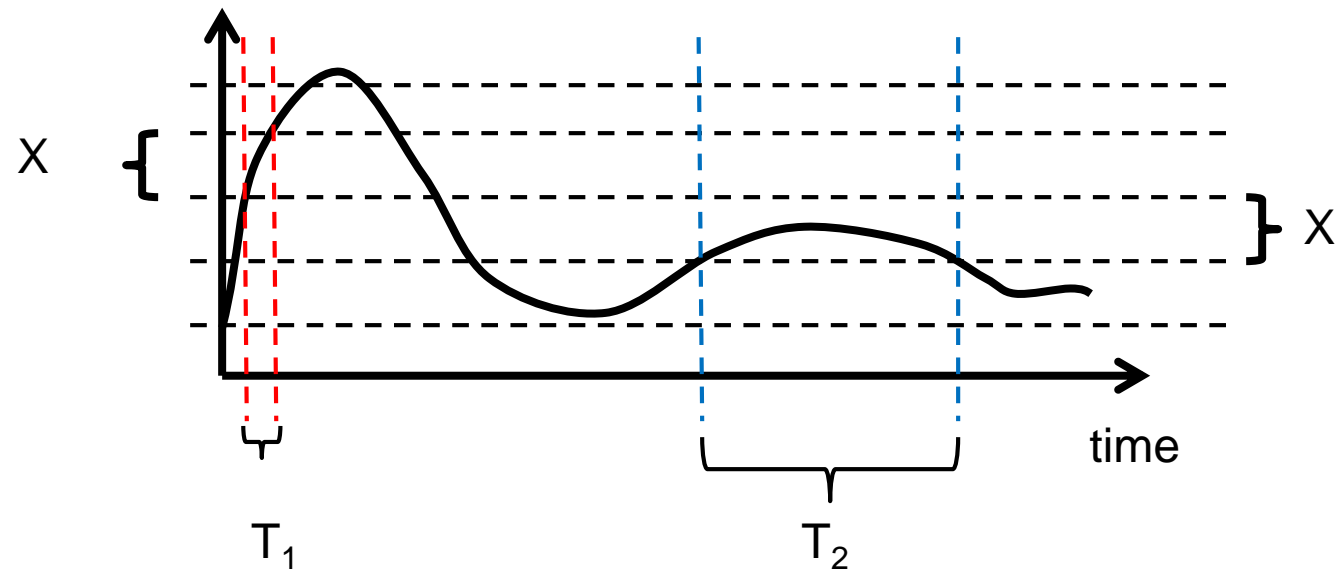


Icons credit: <http://www.doublejdesign.co.uk>



Synchronize cyber processes with physical processes

Approach: Let the physical process drive the computation

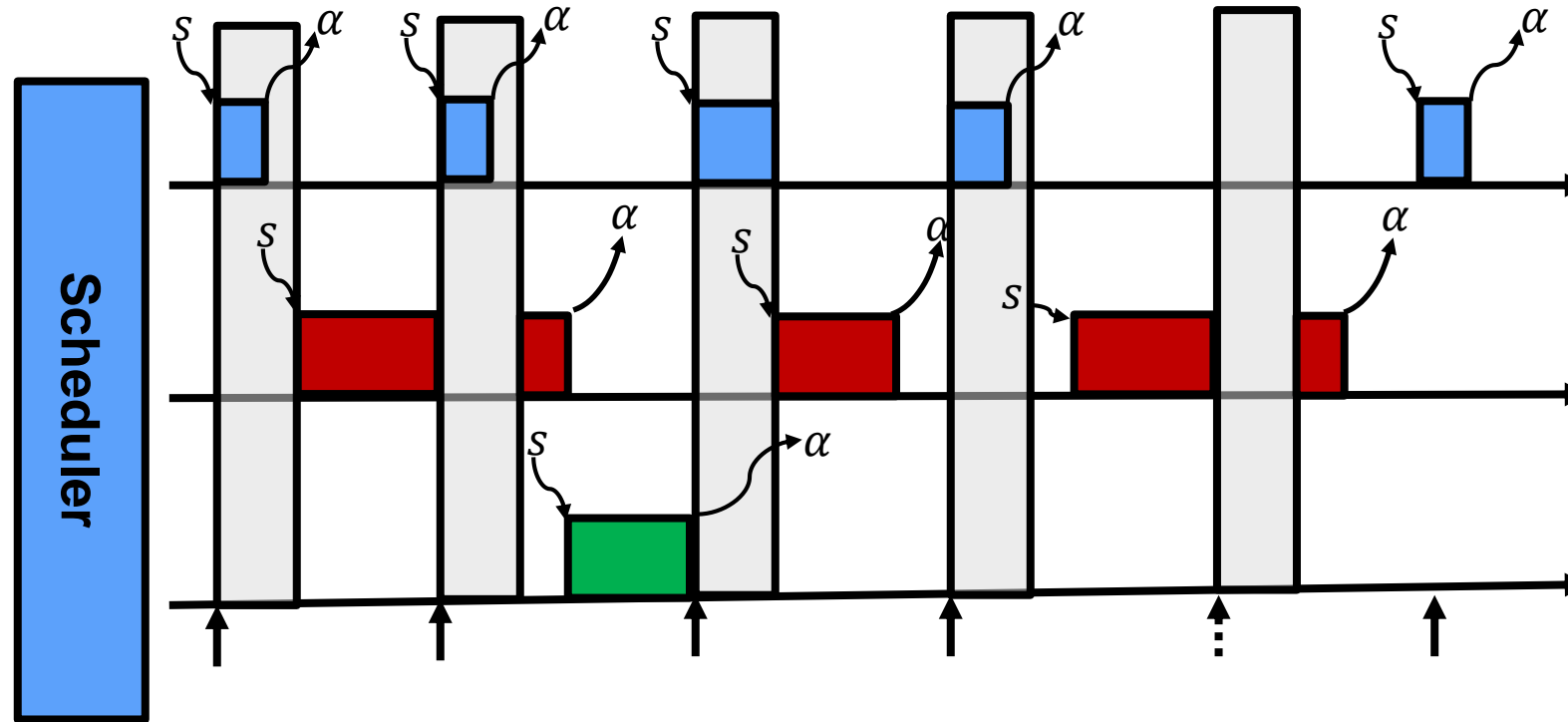


Alternative approaches:
Event-based control
Self-triggered control

Improved resource utilization for guaranteed deadlines



Processing Budget Non-Periodic Arrivals



Icons credit: <http://www.doublejdesign.co.uk>

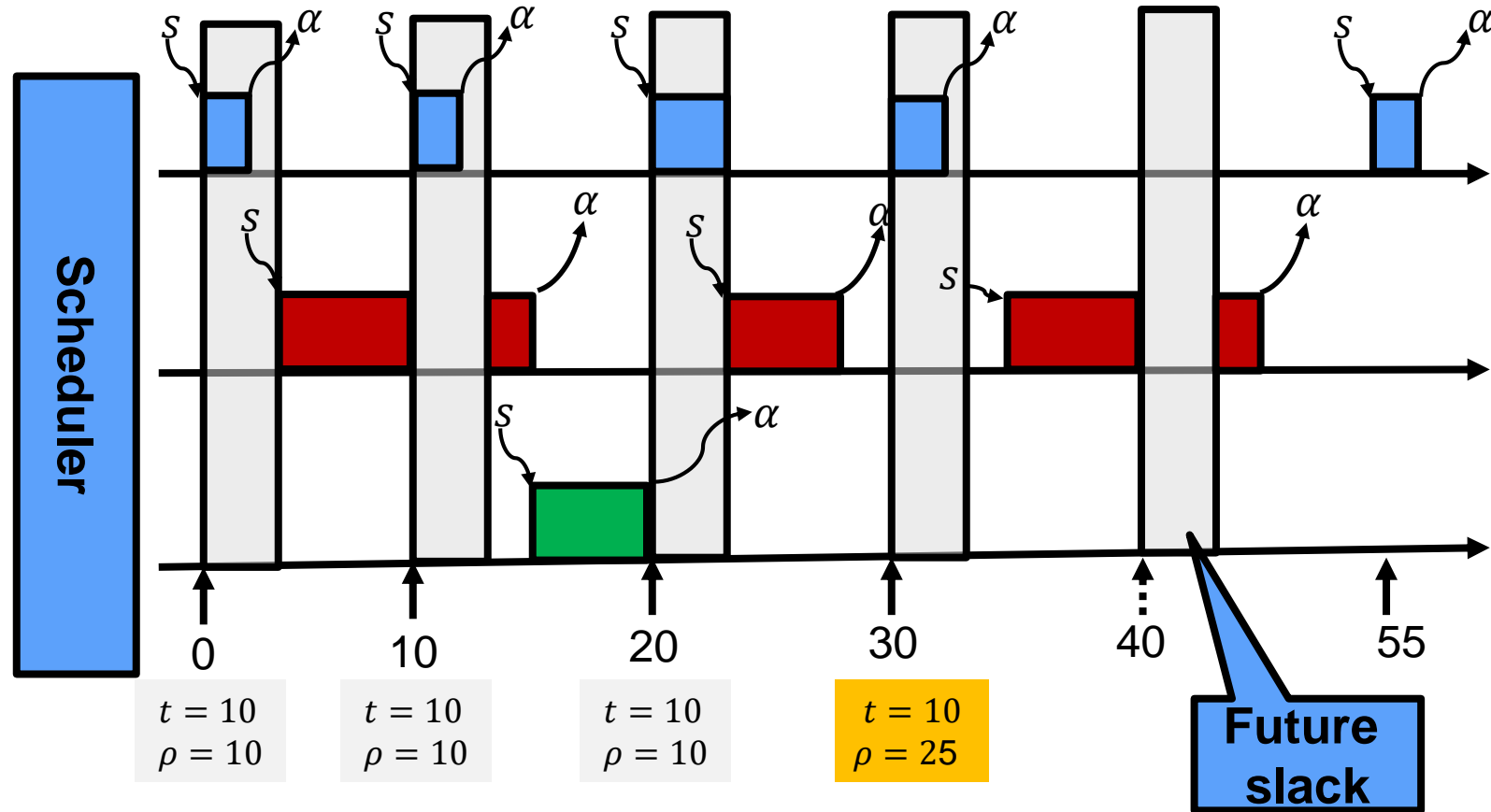


Temporal-Physical Clocks

Infinite sequence of temporal-physical ticks:

- $\psi = (t, \rho)$
 - t : traditional minimum inter-arrival time for a task (fixed at design time)
 - ρ : physical tick that defines time to the next job arrival (driven by physical evolution)
 - Can change every tick
 - $\rho \geq t$
- At design time:
 - $t = T$ is used for schedulability : $U = \sum_i \frac{C_i}{T_i} < bound$

Recover Future Slack



Icons credit: <http://www.doublejdesign.co.uk>



Synchronizing different cyber processes

Using a “common” clock

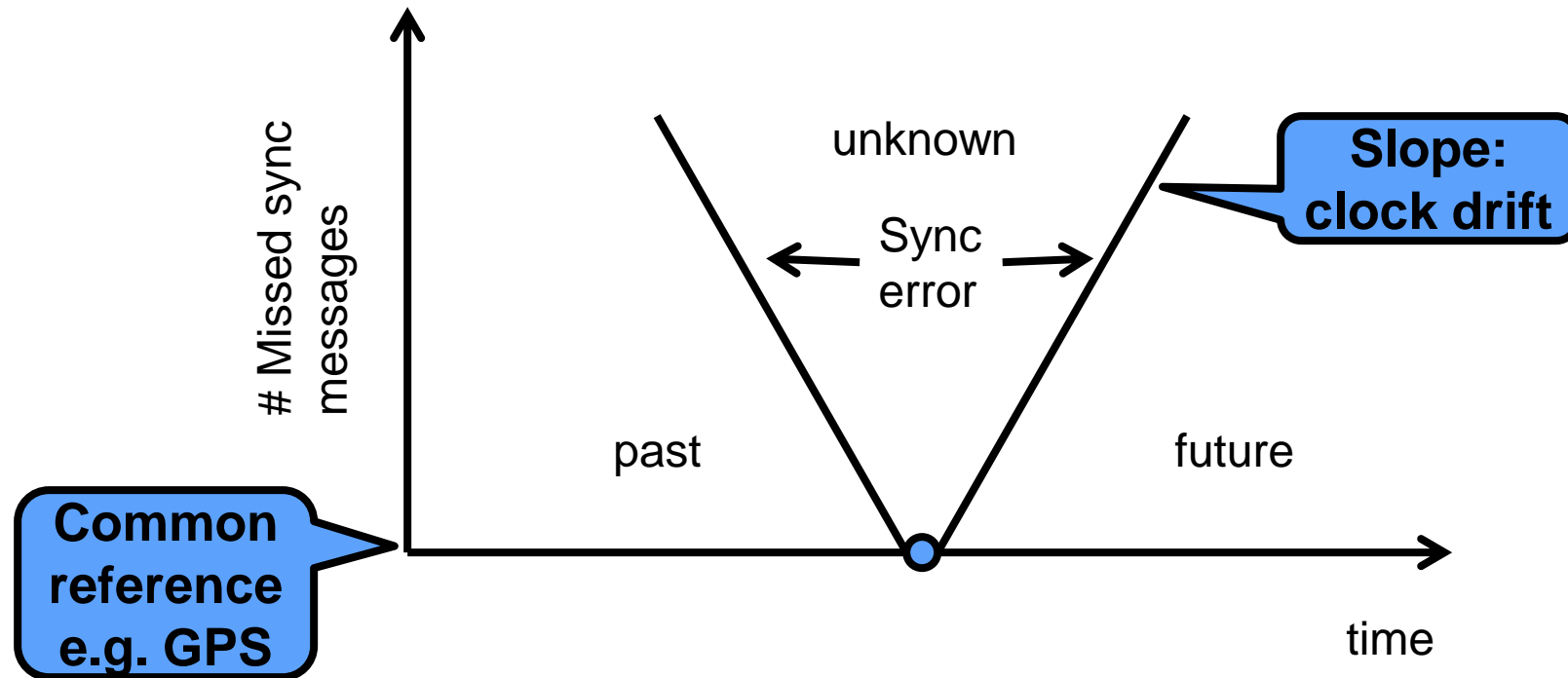
- Common reference (e.g. GPS)
- Synchronized local clocks (e.g. NTP)
- Logical clocks

Reliability needs to be taken into account

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



Synchronized cyber-clock accuracy



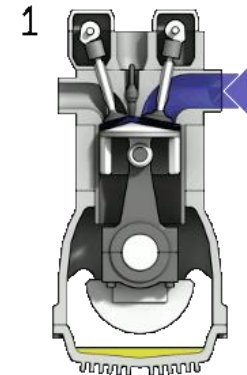
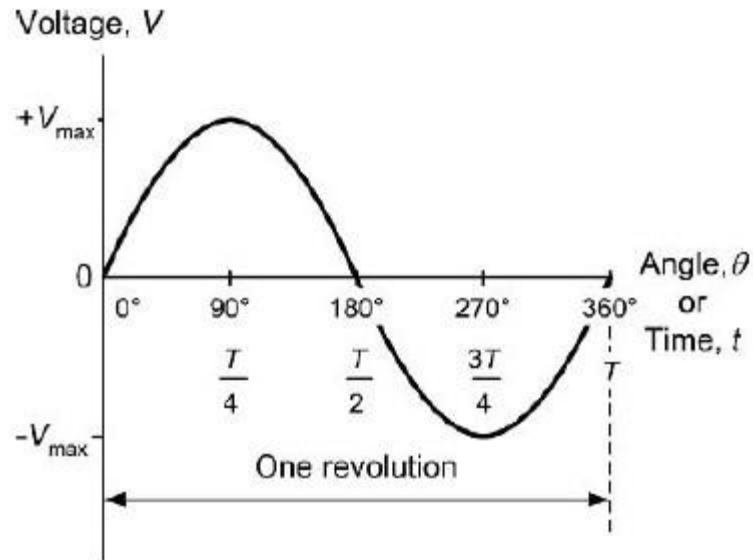
From the loss of the common reference every time we miss a sync message the sync error increases



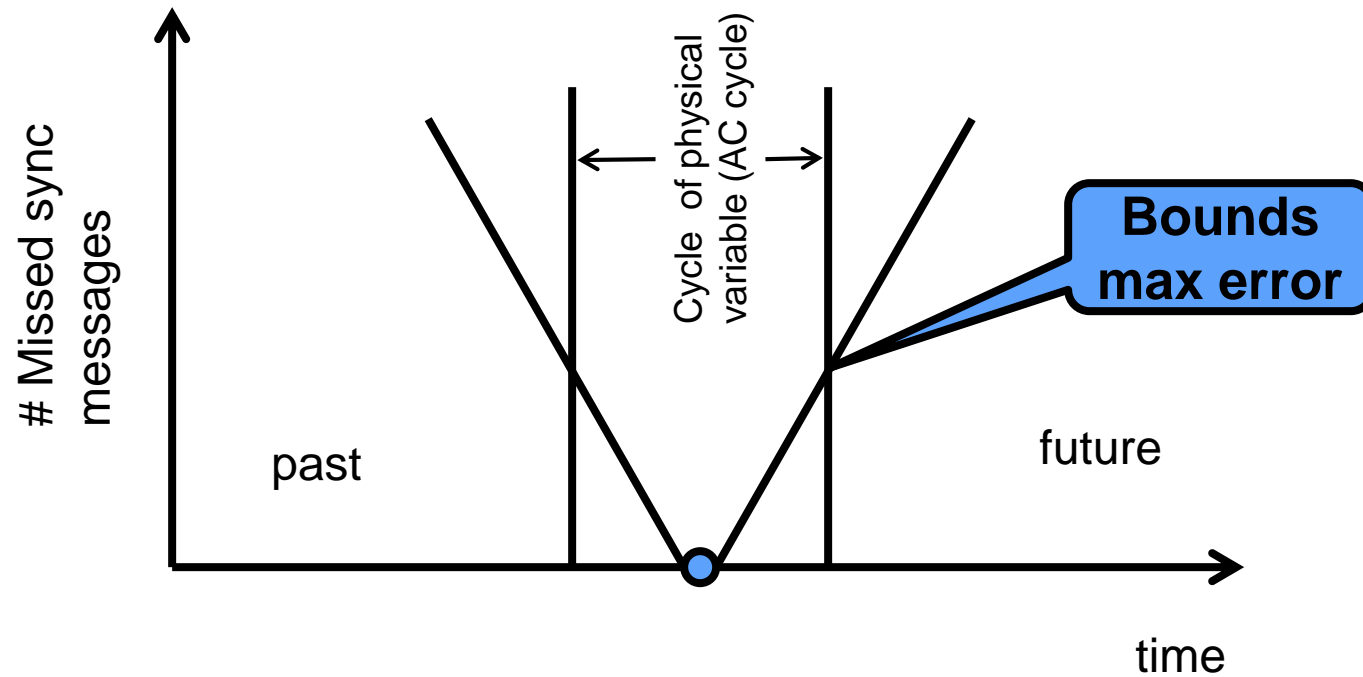
Common physical processes in CPS

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

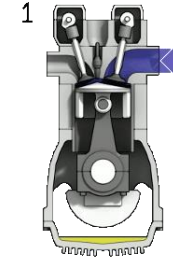
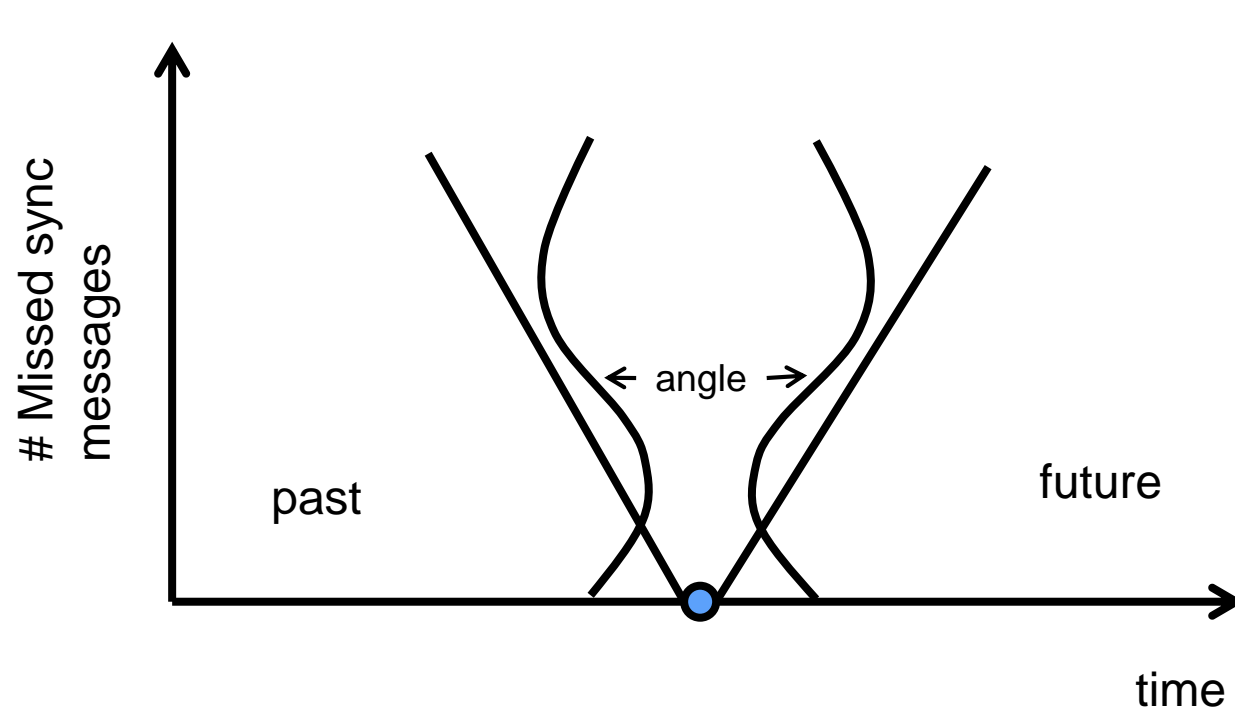
- AC cycle in the smart grid
- Crankshaft angle in an engine



Combining sync clocks with physical variable



Physical process with variable cycles

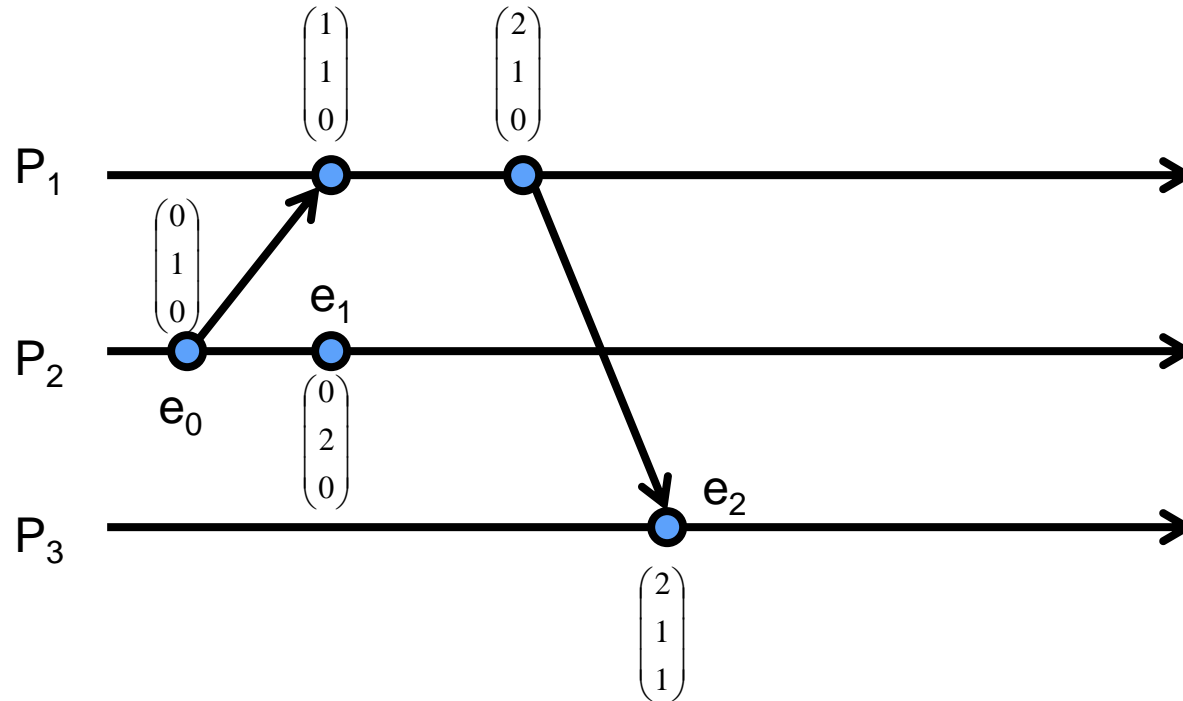


In CPS time is frequently a proxy for physical variable
Hence, cyber processes only require sync with physical variable

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



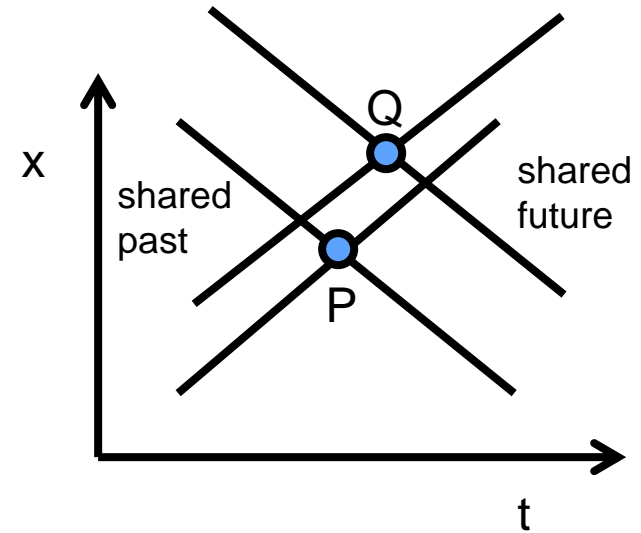
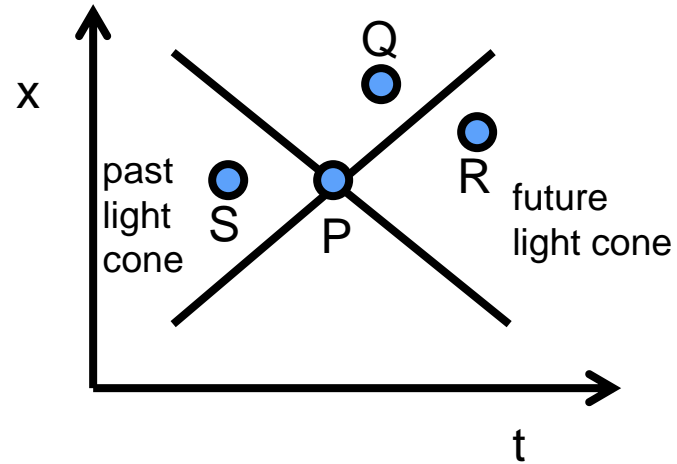
Logical (vector) clocks can also complement sync



But they are also sensitive to “missed” syncs



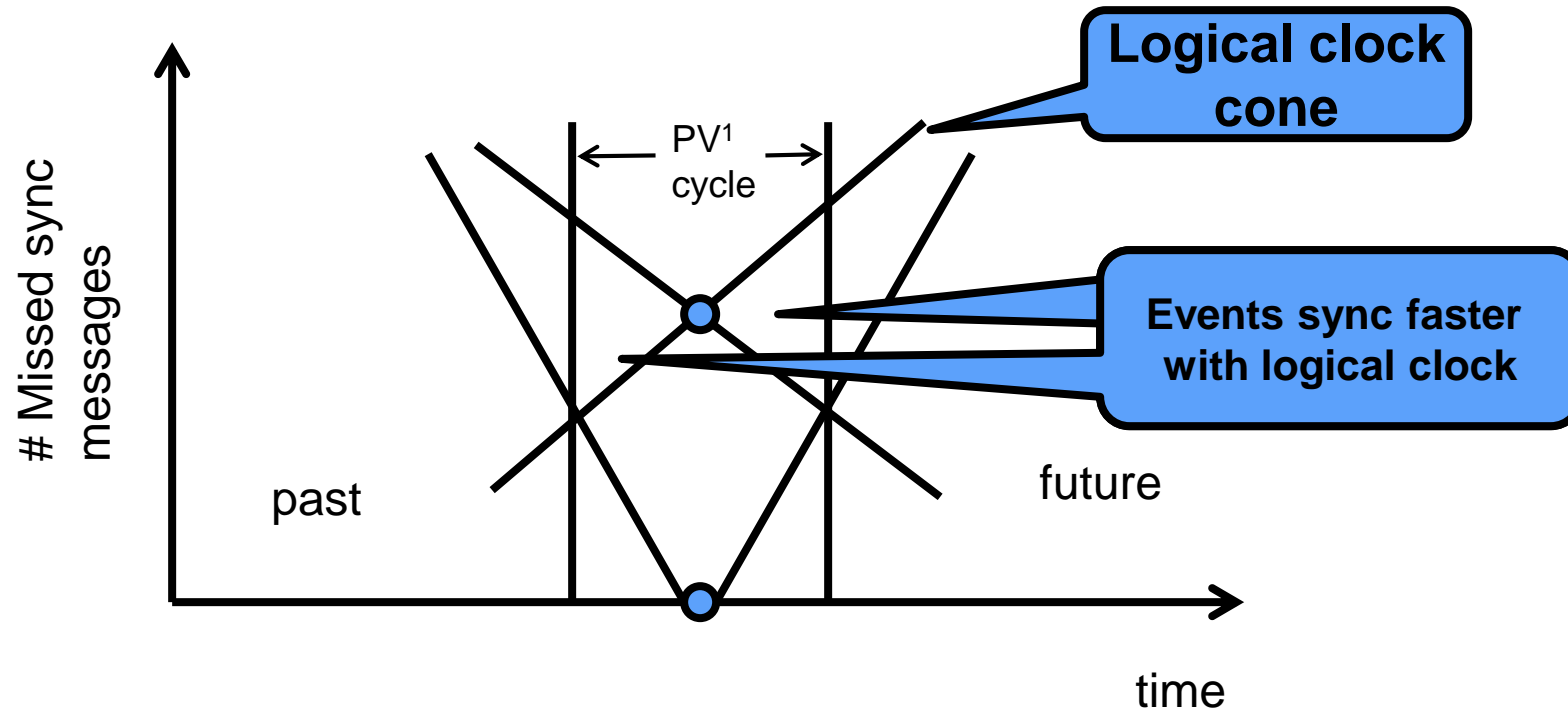
Mattern related vector clocks to Minkowski's spacetime



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



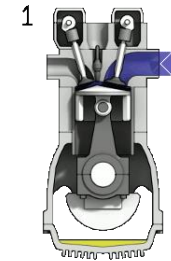
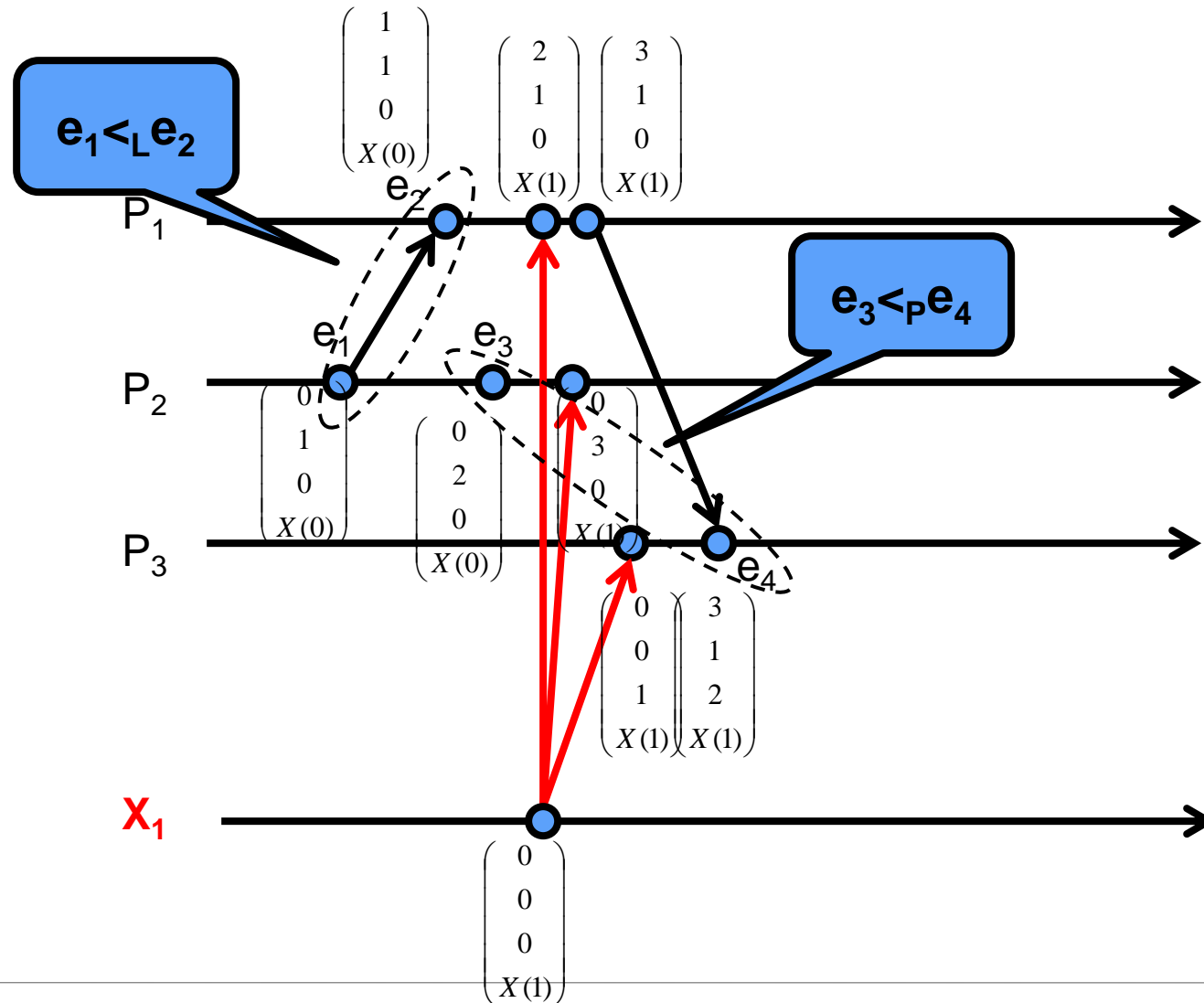
Mixed Physical and Cyber Clocks



¹PV: physical variable



Logical + Physical Clock



Distributed Physical-Temporal Clocks

Add maximum instantaneous speed of change of physical variable x .

- \hat{x}

Distributed Physical-Temporal Tick:

- $\delta\psi = (t, \rho, \hat{x})$

Bounding maximum physical disagreement

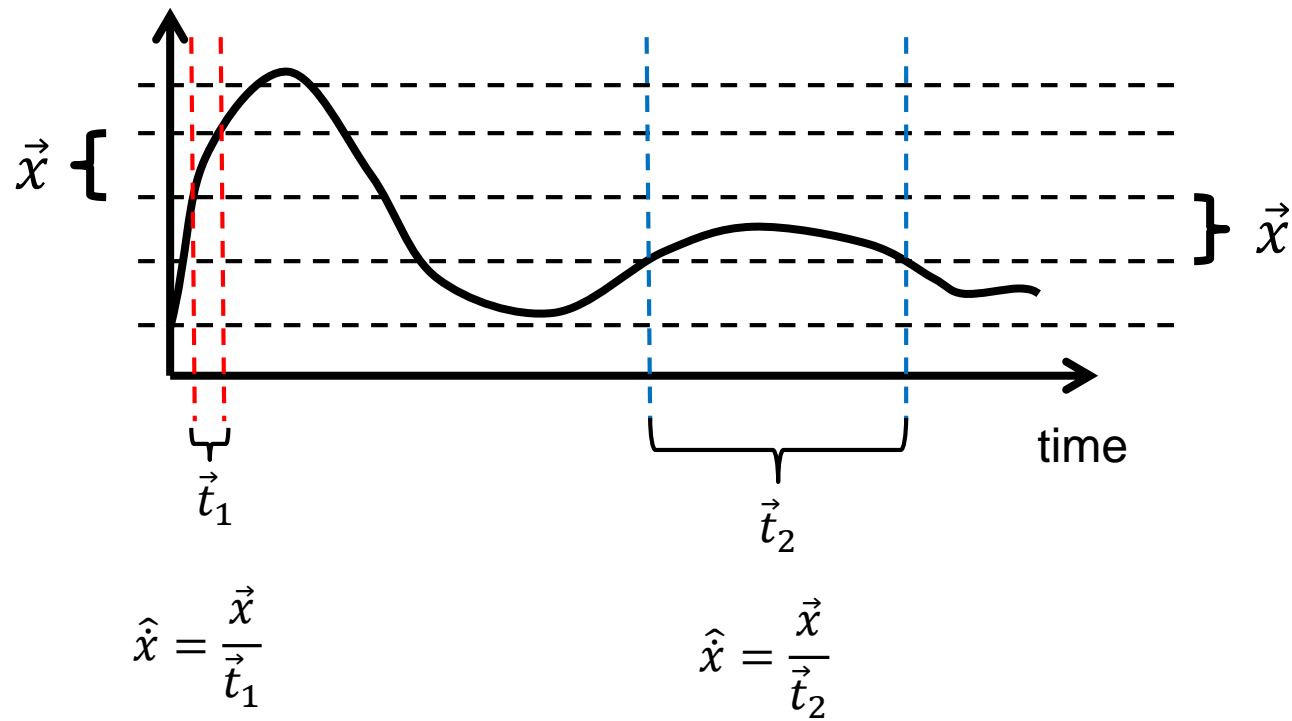
- Given maximum disagreement bound: \vec{x}
- Calculate maximum out of sync interval:

$$- \vec{t} = \frac{\vec{x}}{\hat{x}}$$

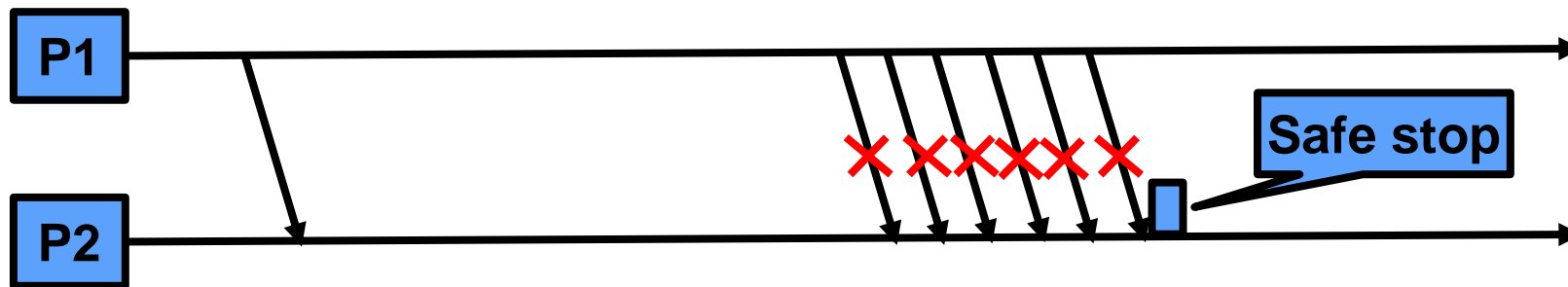
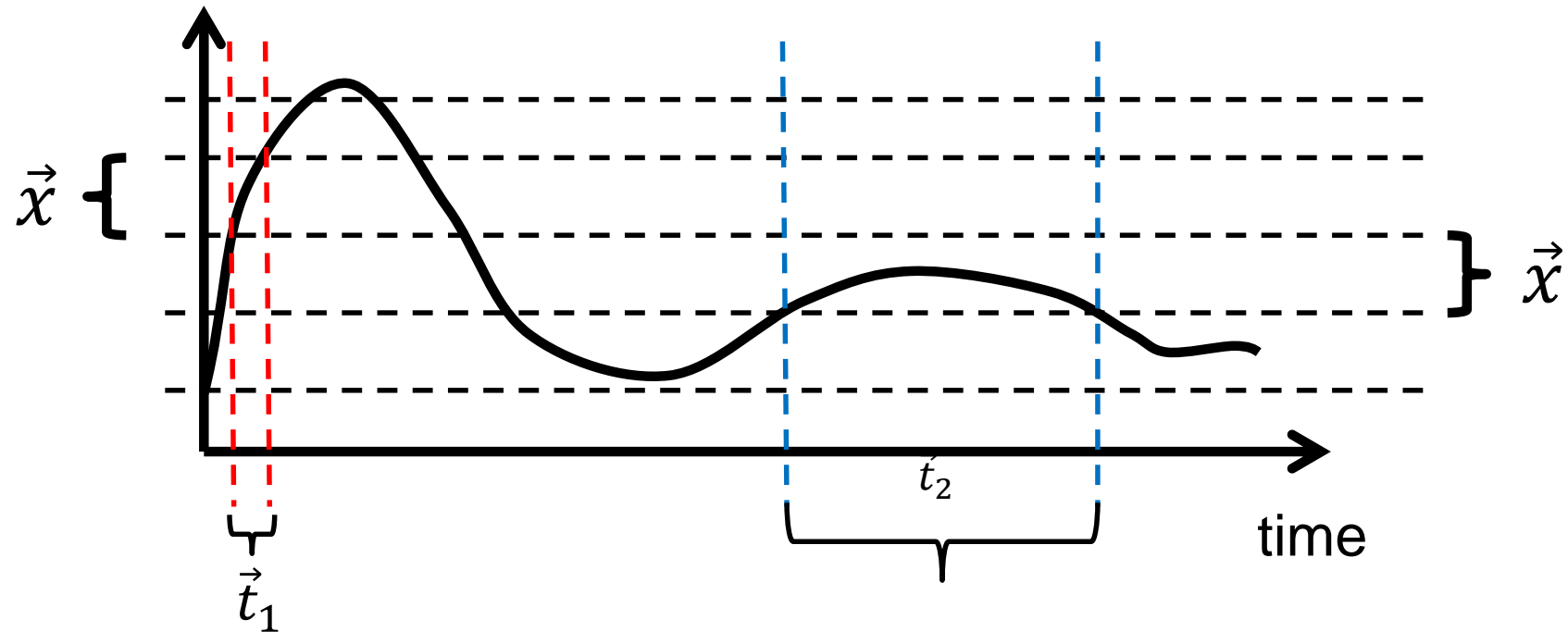
Use \vec{t} to adaptively timeout and take corrective actions



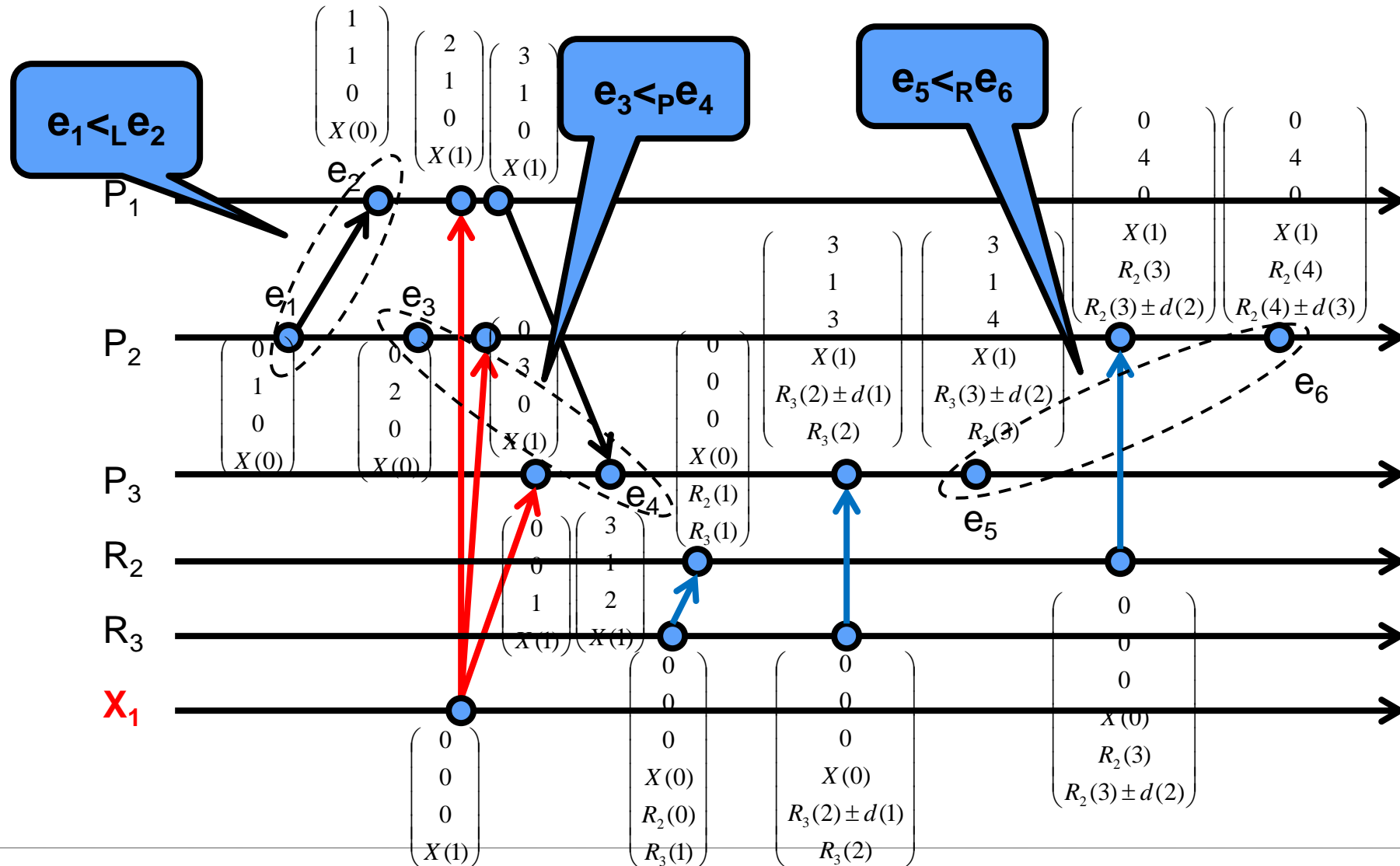
Physical Tick



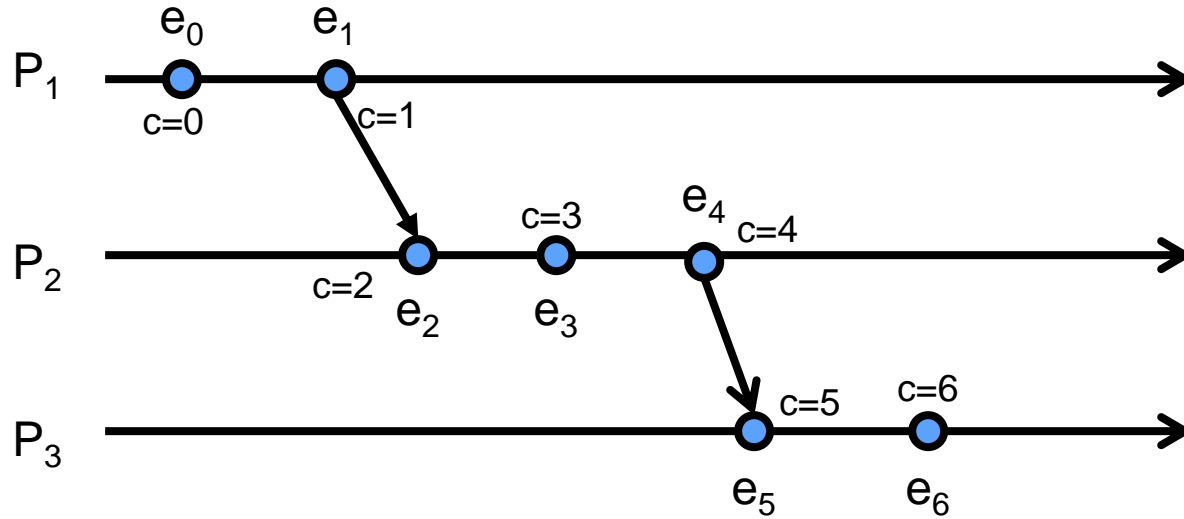
Dynamic Timeout and Safe Stop



Logical + Physical Clock + Real-time clock



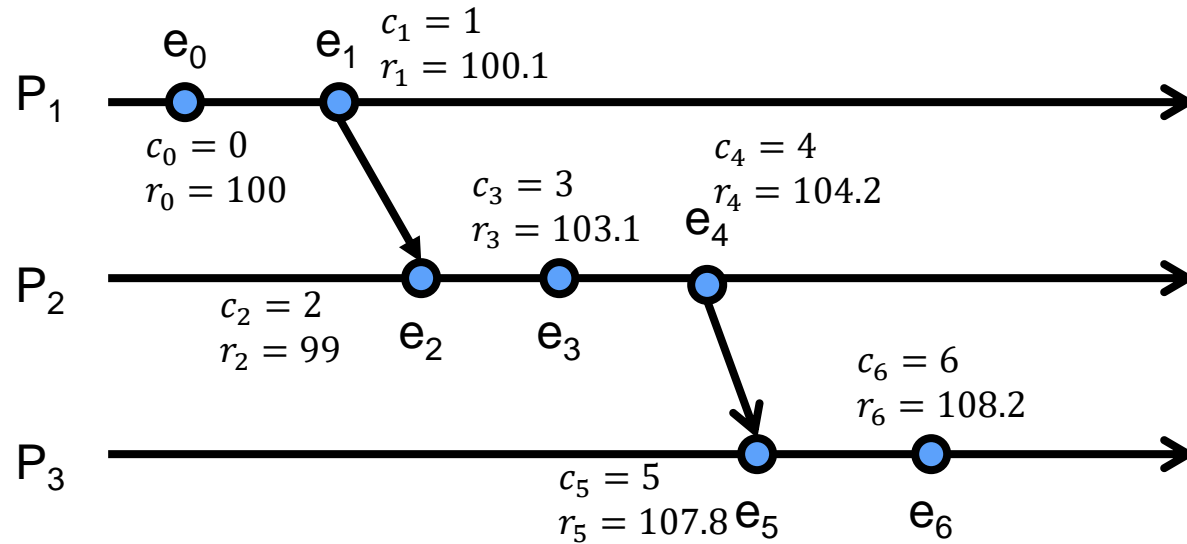
Traditional Virtual Clocks



e_i occurred before e_j if clock at e_i smaller than at e_j

BUT: No physical time relationship

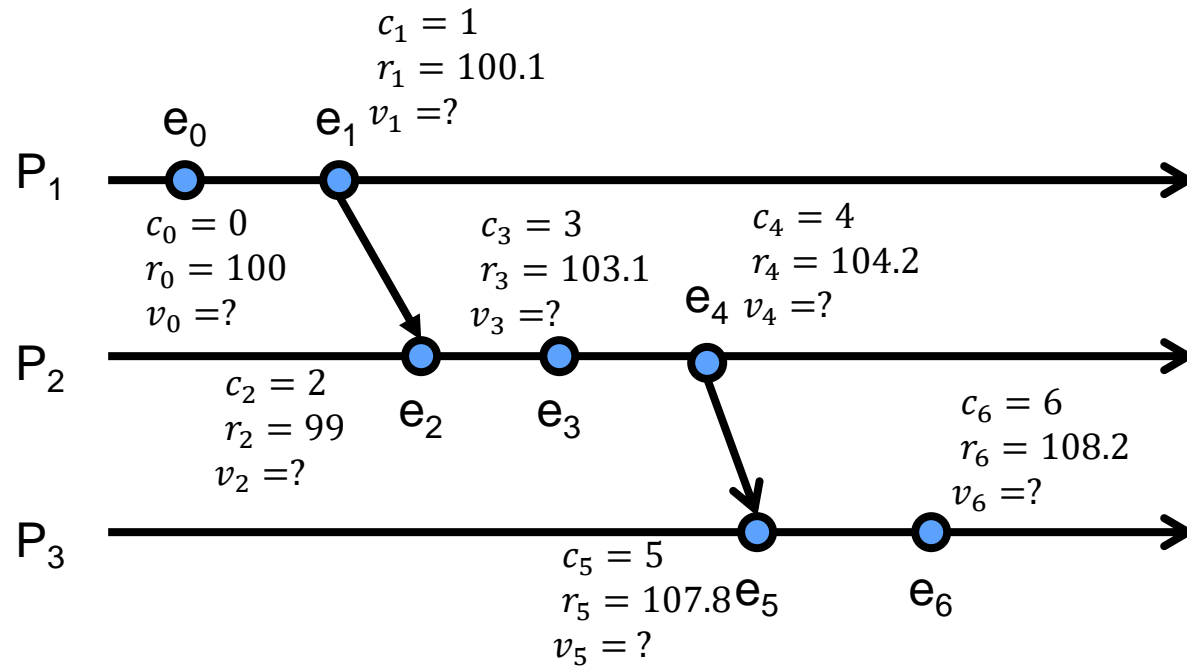
Incorporating Physical Time



e_i occurred before e_j if clock at e_i smaller than at e_j



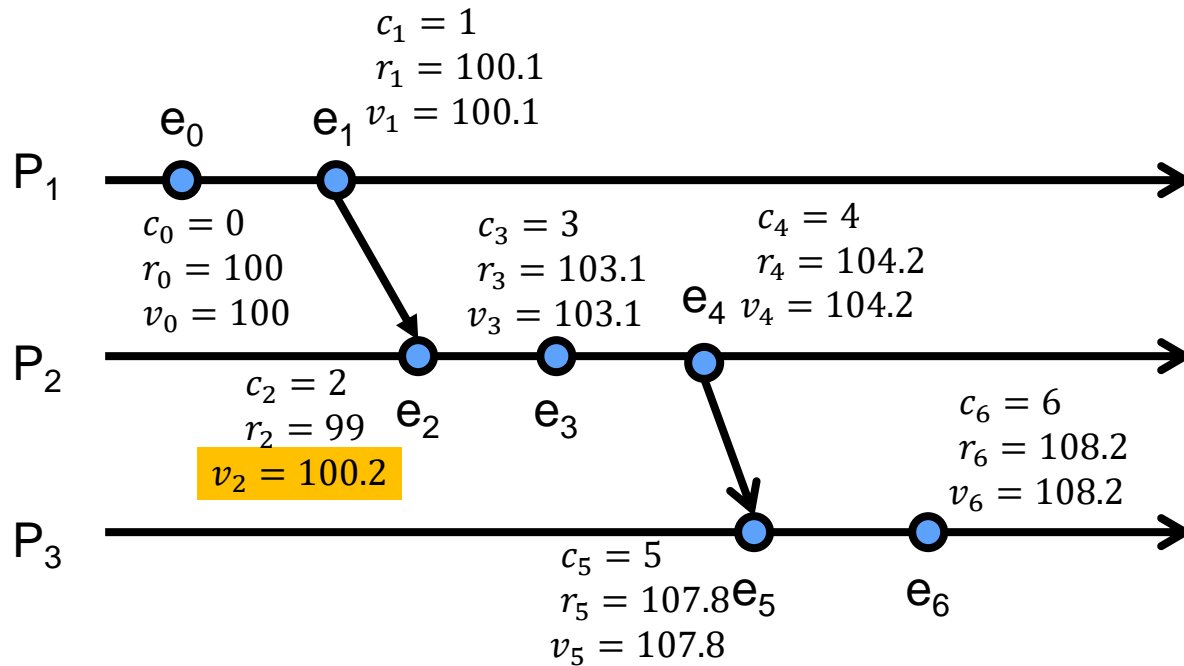
Incorporating Physical Time



e_i occurred before e_j if clock at e_i smaller than at e_j



Incorporating Physical Time



Minimize:

$$\max_i |v_i - r_i|$$

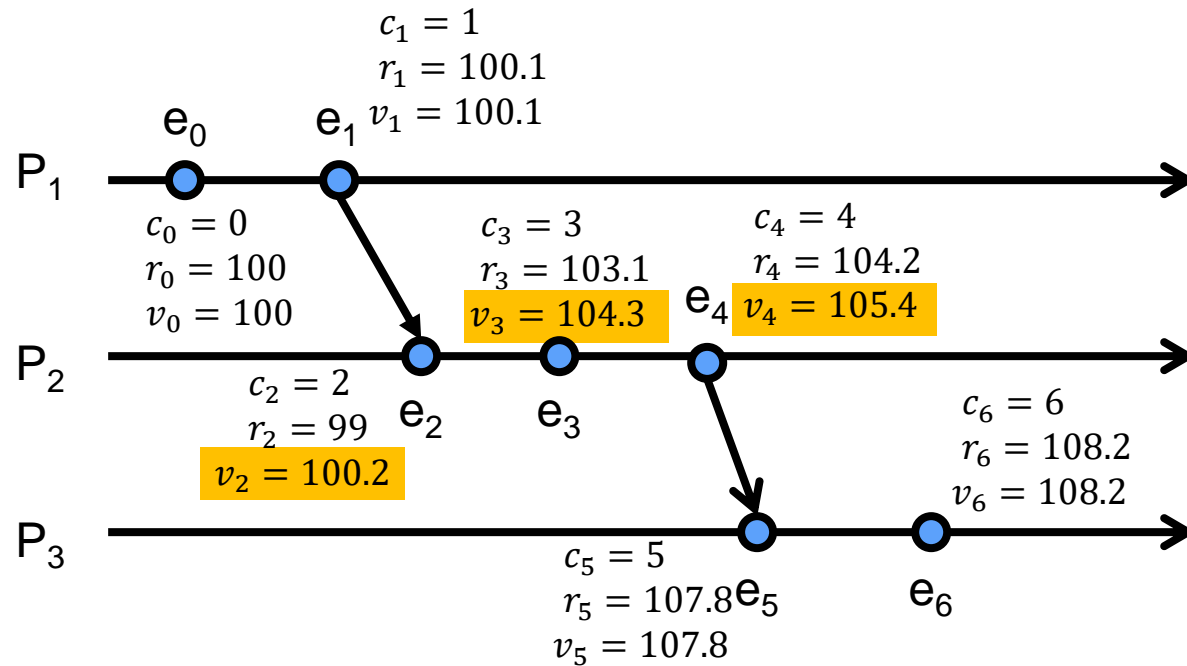
Subject to:

respecting event ordering

e_i occurred before e_j if clock at e_i smaller than at e_j



Incorporating Physical Time



Minimize:

$$\max_{p \in \{1..m\}} \max_{e_i, e_j \in p} |(v_i - v_j) - (r_i - r_j)|$$

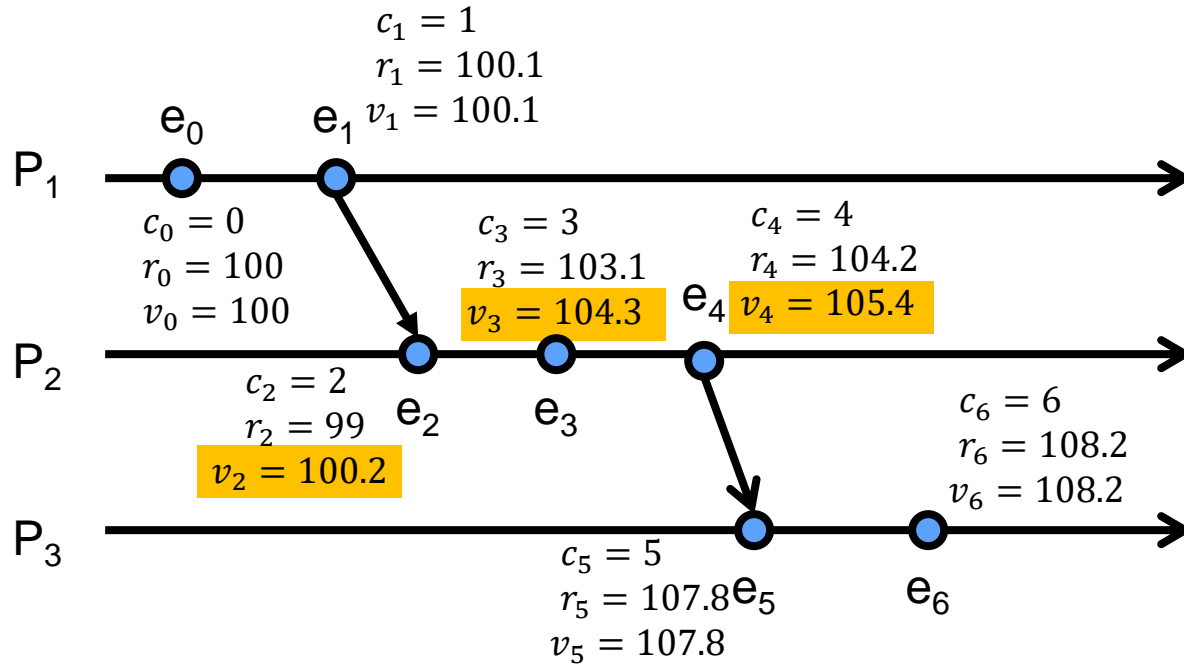
Subject to:

respecting event ordering

e_i occurred before e_j if clock at e_i smaller than at e_j



Incorporating Physical Time



Minimize:

$$\max_{p \in \{1..m\}} \max_{e_i, e_j \in p} |(v_i - v_j) - (r_i - r_j)|$$

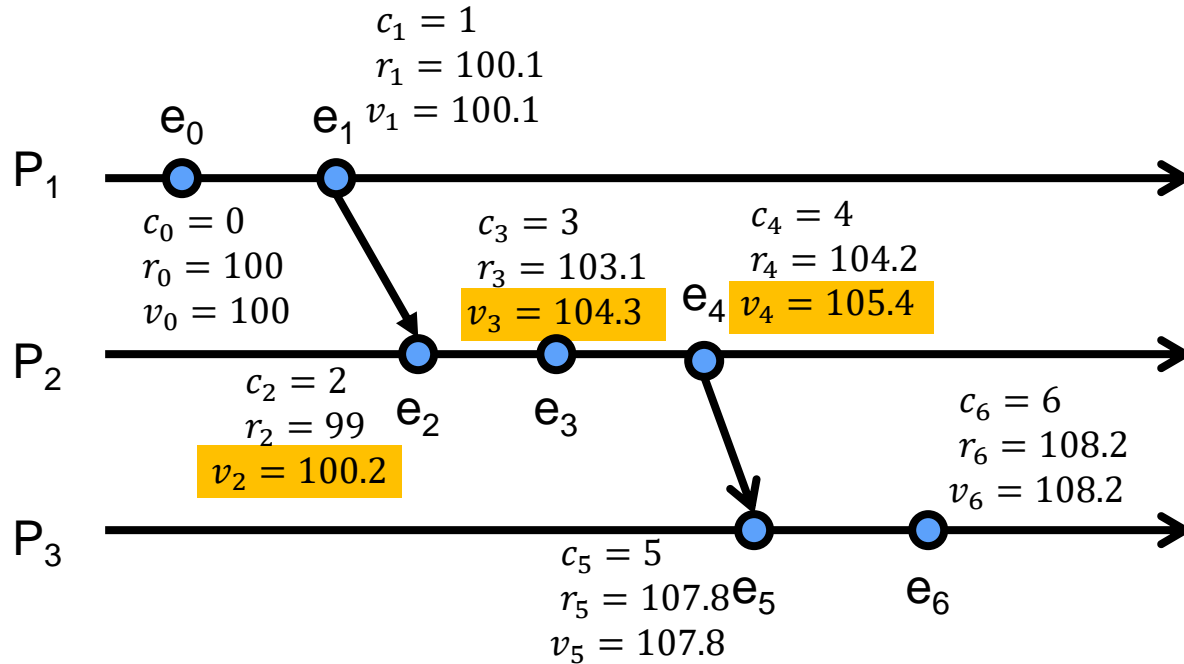
Subject to:

respecting event ordering

e_i occurred before e_j if clock at e_i smaller than at e_j



Incorporating Physical Time



e_i occurred before e_j if clock at e_i smaller than at e_j

Minimize:

$$\max_{p \in \{1..m\}} \max_{e_i, e_j \in p} \left| \frac{(v_i - v_j) - (r_i - r_j)}{(r_i - r_j)} \right|$$

Subject to:

respecting event ordering



Concluding Remarks

Resource Optimization

- Exploiting new non-periodic control algorithms to minimize resource consumption

Distributed Agreement Optimization

- Exploit knowledge of physical state to minimize synchronization

Deriving Physical Timestamps from Agreement

- Assigning timestamps to events such that timestamps can be used to find event order and the timestamps mimic physical time.

