BUILDING CYBER-PHYSICAL SYSTEMS WHERE PRECISE TEMPORAL SEMANTICS ARE "CORRECT BY CONSTRUCTION"

John C. Eidson

WSTS-2015

www.calnexsol.com

Overview

Calnex

- NIST Public Working Group on CPS and TAACCS items of interest
- “Correct by construction” temporal semantics
- Reminder of an existence proof
- What will it take?

NIST and TAACCS

NIST Public Working Group on CPS

- Initial meetings June 30, 2014, August 11-13, 2014
- Initial report from each of the five subgroups – Reference Architecture, Use Cases, Cybersecurity, Data, and **Timing** . Completed December 2014
- CPS Technology Roadmap identifying opportunities for a coordinated effort on key technical challenges (due March 2015)

NIST PWG Timing Subcommittee

Leaders:

- Government: Marc Weiss, NIST
- Academia: Hugh Melvin, National University of Ireland, Galway
- Industry: Sundeep Chandhoke, National Instruments

Participants from Europe and US with backgrounds in T&M, industrial automation, clock technology, smart grid

Quote from the NIST PWG Report section on timing

" 'Time correctness by design` includes this concept of: designers including accurate timing in designs, independent of hardware . Designers need to be able to specify timing in a CPS as an abstraction, much as most modern systems are designed as abstractions, without reference to specific hardware. This is necessary to allow a design to persist through upgrades in the hardware and software. There is a lot of work to be done to realize time correctness by design in full. In its ideal realization, a designer could include timing as an abstraction in a GUI design system. Upon choosing the target hardware, the system determines if that hardware can support the timing, and if so, generates the code and implementations to support the design."

“Correct by construction” temporal semantics: the fine print

- Designs must not violate causality
  - Not all timing designs can be executed (no laughing until tickled)
  - Not all timing designs can be executed on a given set of hardware and network resources
- All realizable designs will have limits on input/output rates (Kopetz’ closed world assumption) and achievable timing intervals
- All computation and network transmission times must have an upper bound

IF the fine print conditions are met!

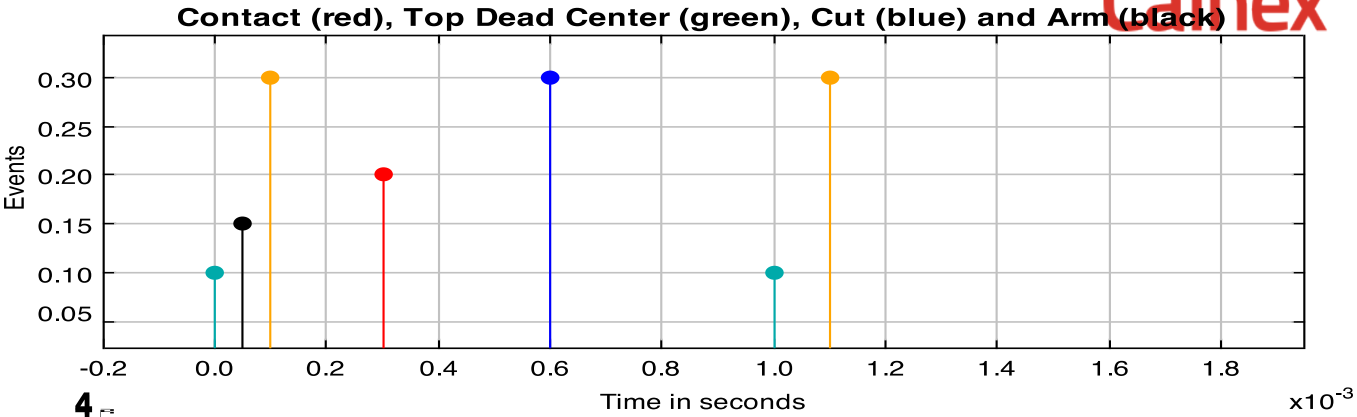
Calnex

Then it is possible to create a design environment where:

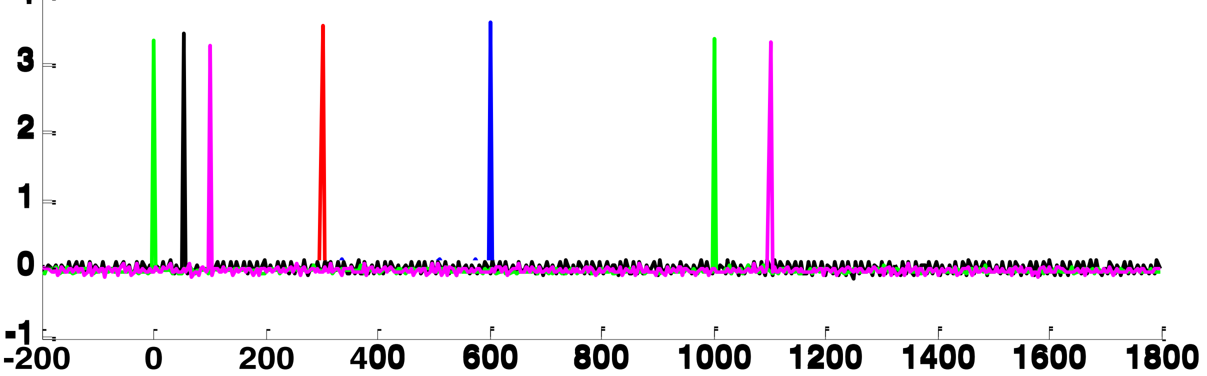
- The designer can explicitly specify timing in the context of the design
- Timing designs will compile and execute with correct timing on any capable set of hardware and network resources
- Upgrades (or downgrades) of hardware and network resources that continue to meet the fine print conditions will not affect the correctness of the timing

EXISTENCE PROOF: Renesas vs. XMOS: I/O timing (from ISPCS 2013 report on work at UC Berkeley)

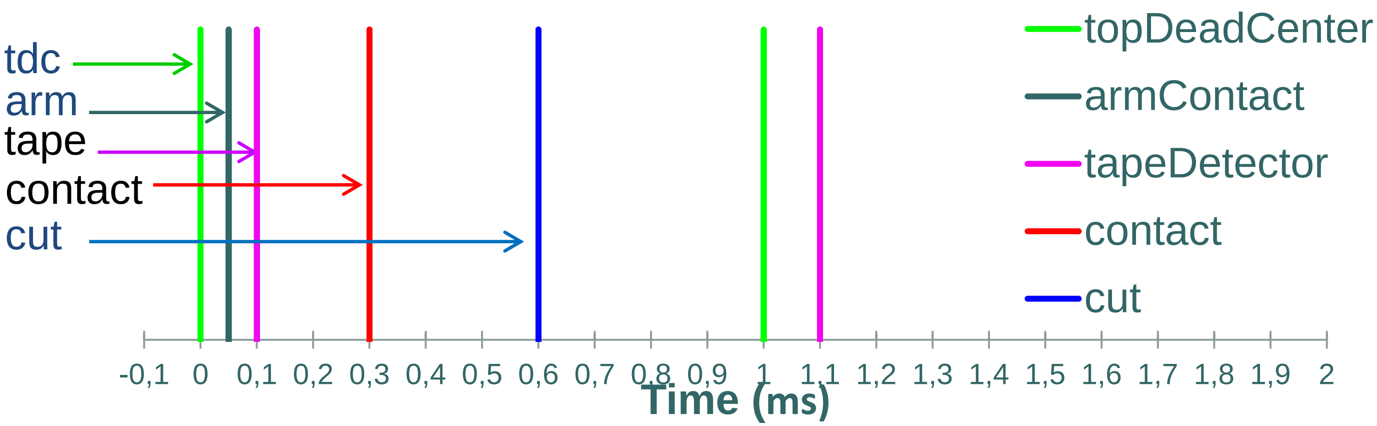
Simulation



Renesas

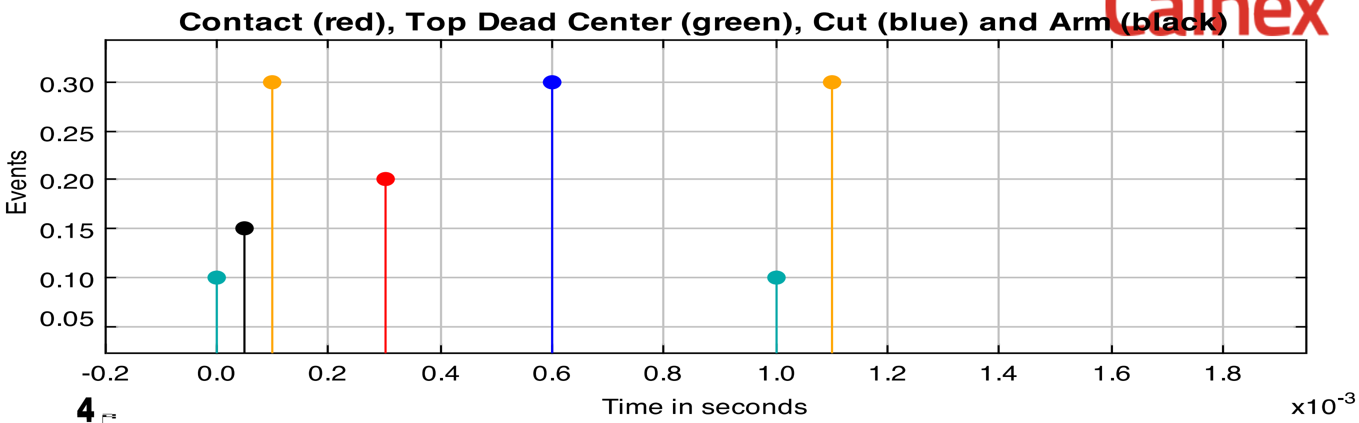


XMOS

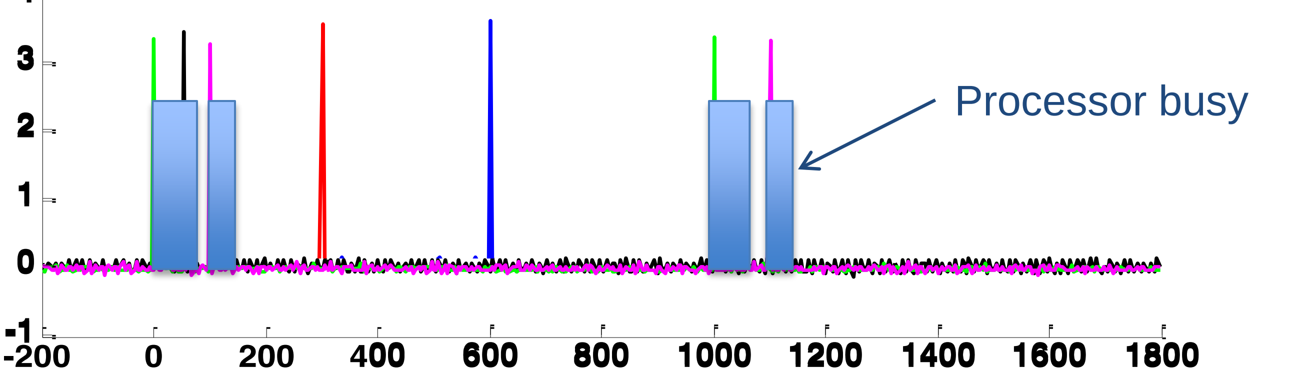


Renesas vs. XMOS: Busy vs. Idle Time

Simulation

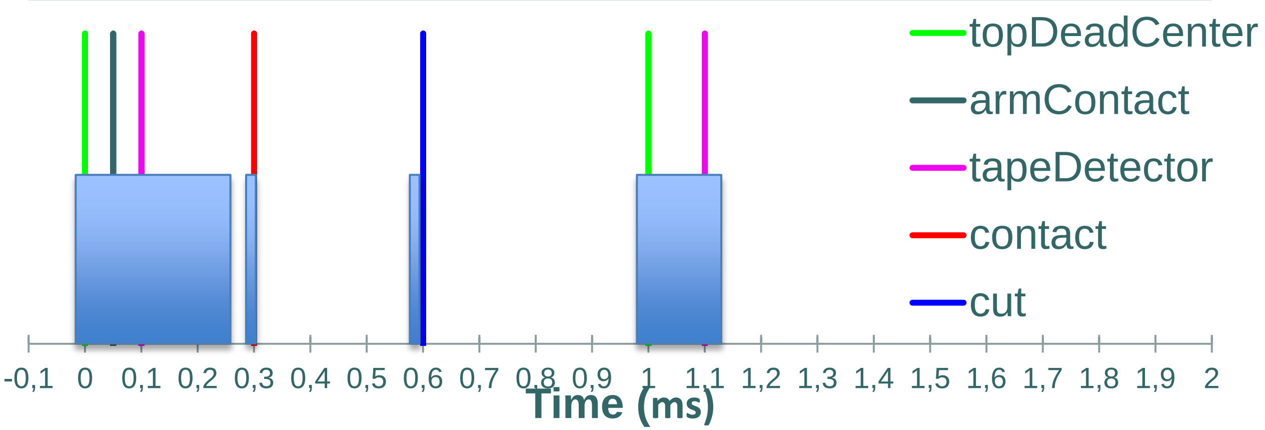


Renesas



Processor busy

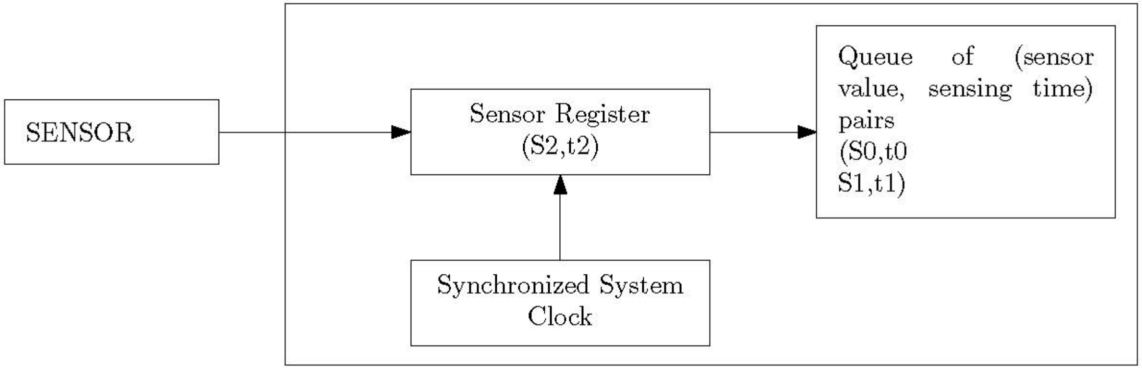
XMOS (single core execution)



Lessons learned from the Berkeley project

Sensor or input event timing support

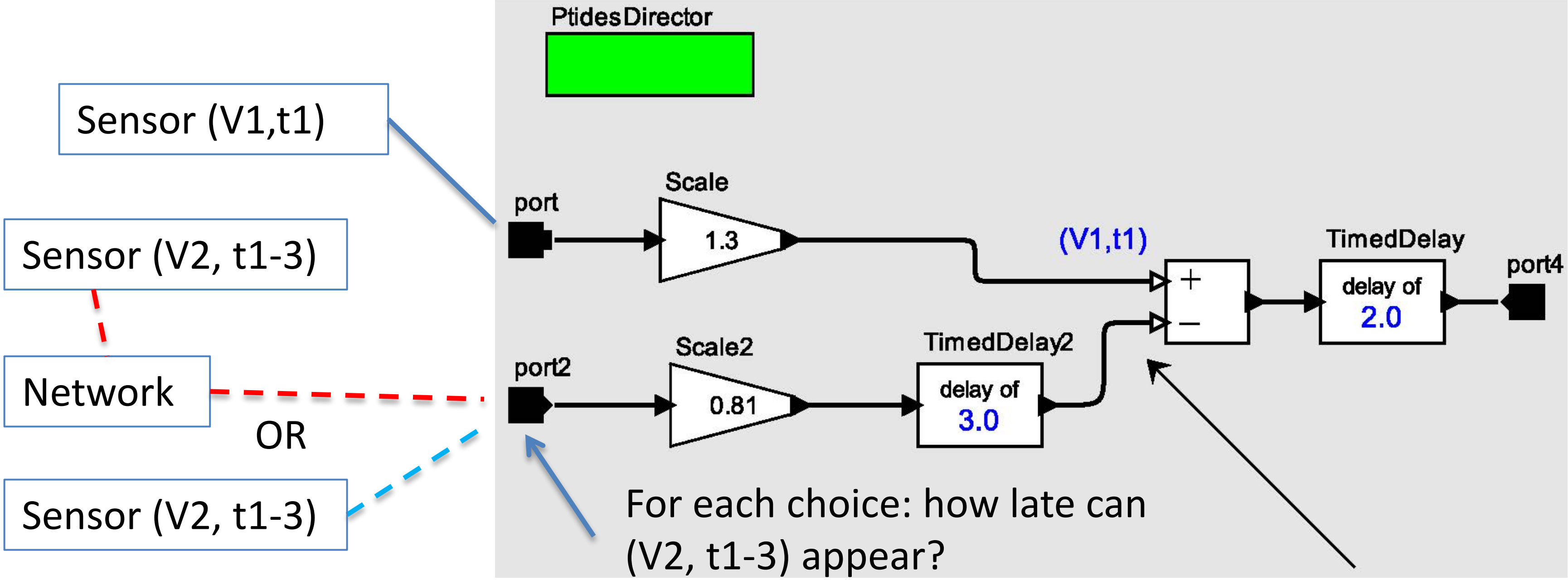
- How to trigger the sensor
- How to throttle external events


SENSOR
Sensor Register (S2,t2)
Queue of (sensor value, sensing time) pairs (S0,t0 S1,t1)
Synchronized System Clock

Lessons learned from the Berkeley project

Safe to process timing support

- When can the add:subtract actor execute?=> at t1-3 since if a token is to arrive with timestamp t1 it must appear at port 2 by t1-3
- Need notification when t=t1-3 + any external delays, e.g. network
    - Should not require polling
    - Should be with respect to the synchronized system clock
    - low latency for efficiency



Sensor (V1,t1)

Sensor (V2, t1-3)

Network

OR

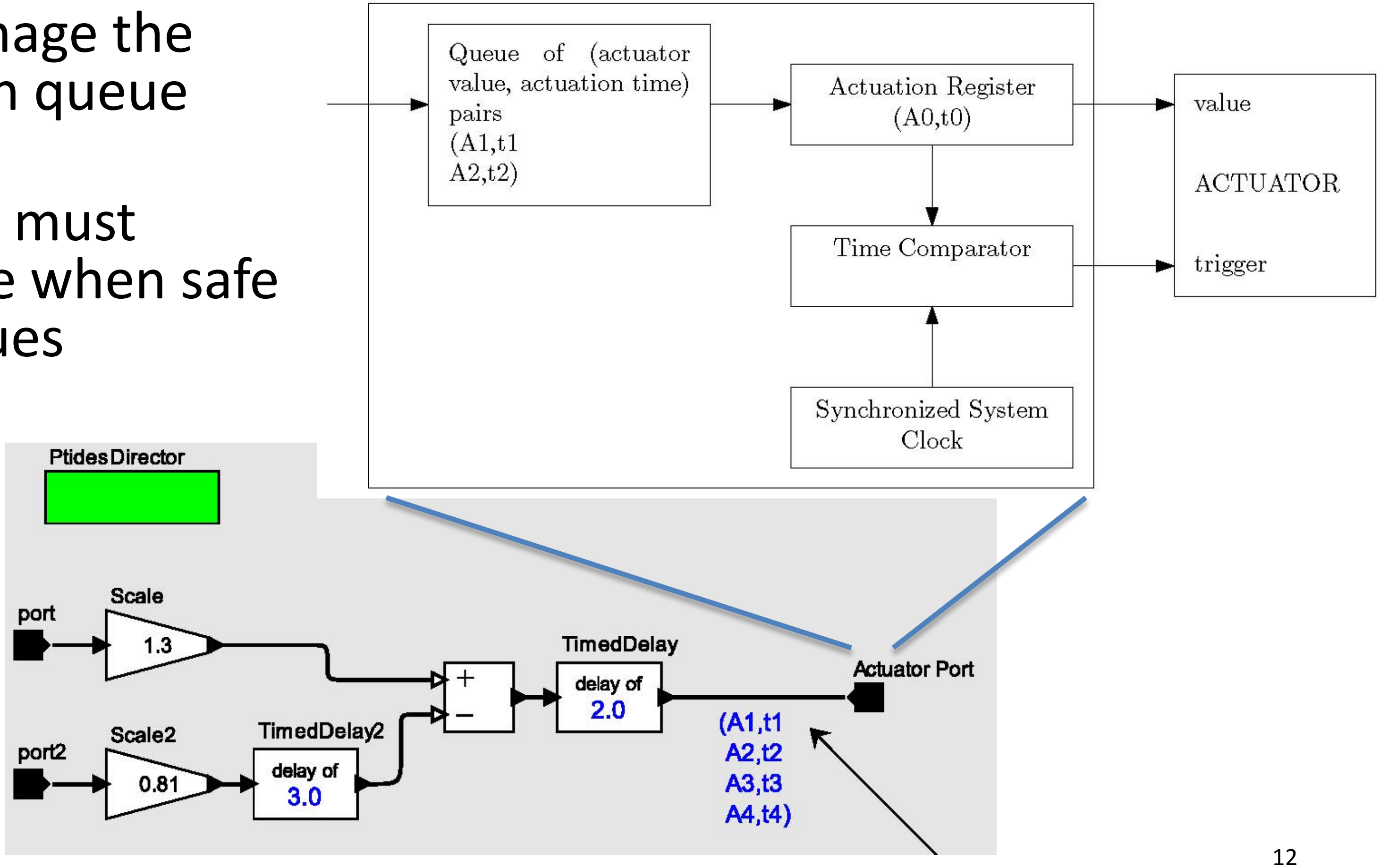
Sensor (V2, t1-3)

For each choice: how late can (V2, t1-3) appear?

Lessons learned from the Berkeley project

Actuation queue and timing support

- How to manage the difference in queue depths
- Notification must include time when safe to pop queues



Conclusions

- Follow the outcomes from both the NIST Public Working Group and TAACCS
- Timing that is “correct by construction” is possible
- Lots to learn about implementation trade-offs and requirements to successfully realize “correct by construction timing”

Calnex

Thanks for your attention!