Timing in Cyber-Physical Systems

Marc Weiss, Ph.D.

mweiss@nist.gov

NIST, Time and Frequency Division

WSTS 2015

Timing in Cyber-Physical Systems: Outline

- The term Timing used here as a general term: frequency, phase or time sync or source

- Expected massive growth in the Internet of Things (IoT)
- NIST has organized a Public Working Group (PWG)
  - The near-final timing framework for CPS
  - Timing future in CPS: Technology Roadmap
- Among other efforts related to timing in the IoT

GE White Paper

Figure 2. Rise of the Industrial Internet

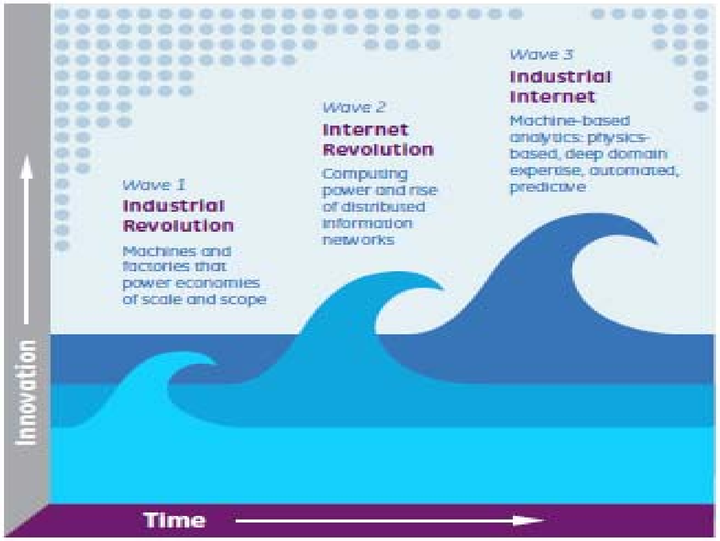
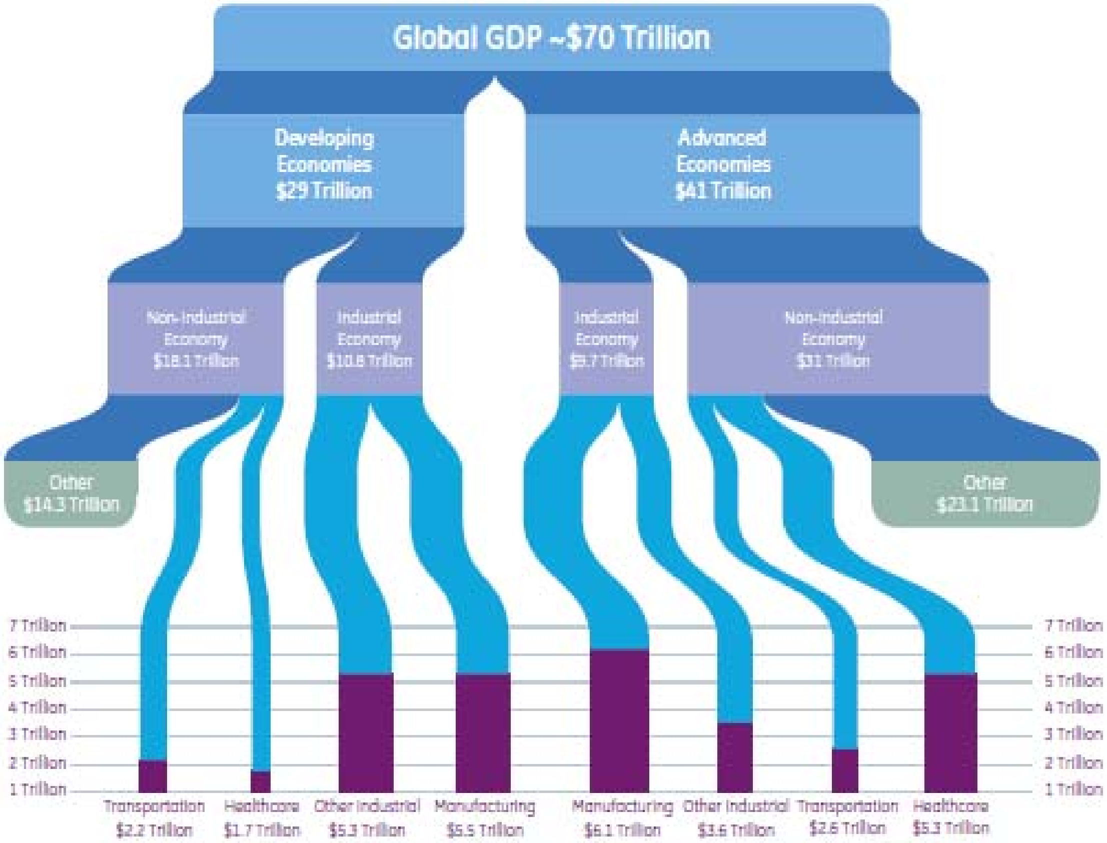

Wave 1
Industrial Revolution
Machines and factories that power economies of scale and scope
Wave 2
Internet Revolution
Computing power and rise of distributed information networks
Wave 3
Industrial Internet
Machine-based analytics: physics-based, deep domain expertise, automated, predictive
Innovation
Time

Figure 5. Industrial Internet Potential GDP Share

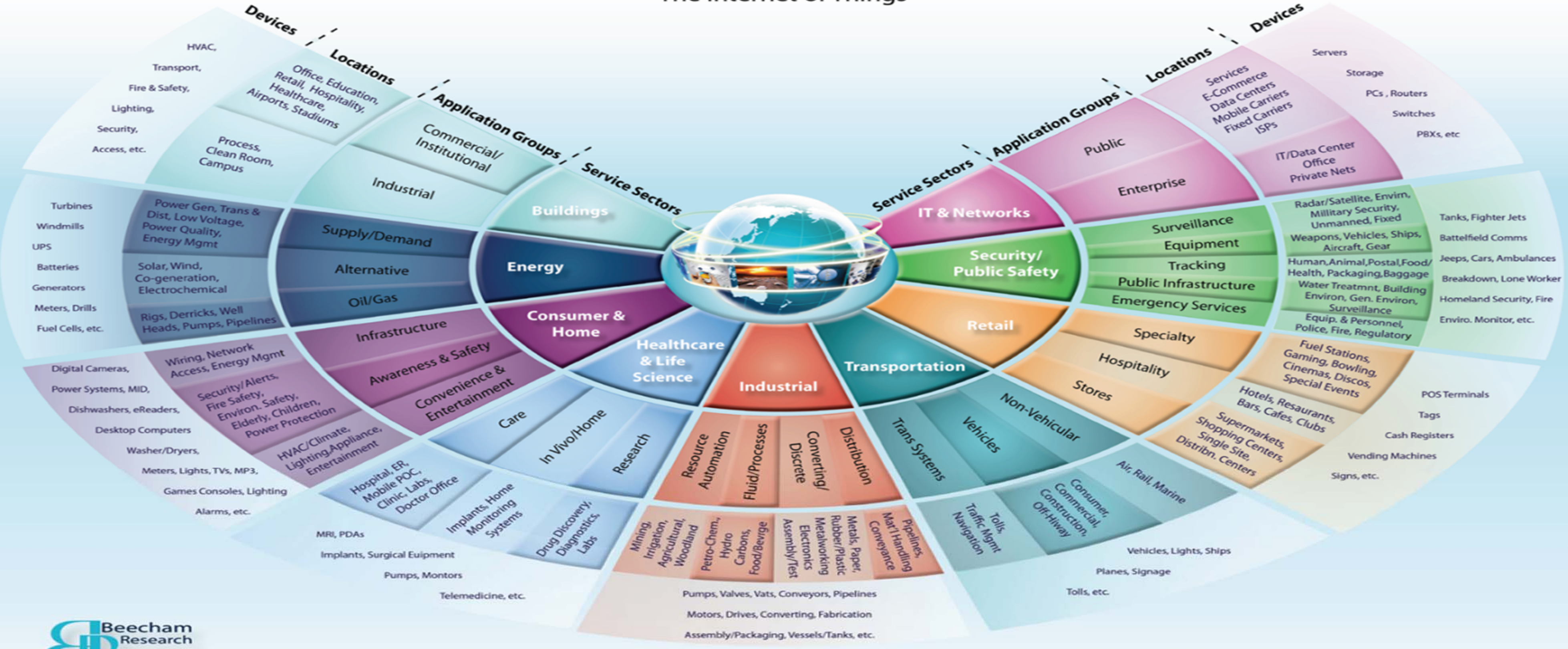


Industrial Internet opportunity ($32.3 Trillion) 46% share of global economy today

Source: World Bank, 2011 and General Electric

M2M World of Connected Services

The Internet of Things



Devices

Locations

Application Groups

Service Sectors

Buildings

Commercial/Institutional

Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums

HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.

Industrial

Process, Clean Room, Campus

Energy

Supply/Demand

Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy Mgmt

Alternative

Solar, Wind, Co-generation, Electrochemical

Oil/Gas

Rigs, Derricks, Well Heads, Pumps, Pipelines

Turbines

Windmills

UPS

Batteries

Generators

Meters, Drills

Fuel Cells, etc.

Consumer & Home

Infrastructure

Wiring, Network Access, Energy Mgmt

Awareness & Safety

Security/Alerts, Fire Safety, Environ. Safety, Elderly, Children, Power Protection

Convenience & Entertainment

HVAC/Climate, Lighting,Appliance, Entertainment

Digital Cameras,

Power Systems, MID,

Dishwashers, eReaders,

Desktop Computers

Washer/Dryers,

Meters, Lights, TVs, MP3,

Games Consoles, Lighting

Alarms, etc.

Healthcare & Life Science

Care

Hospital, ER, Mobile POC, Clinic, Labs, Doctor Office

In Vivo/Home

Implants, Home Monitoring Systems

Research

Drug Discovery, Diagnostics, Labs

MRI, PDAs

Implants, Surgical Euipment

Pumps, Montors

Telemedicine, etc.

Industrial

Resource Automation

Fluid/Processes

Converting/Discrete

Distribution

Mining, Irrigation, Agricultural, Woodland

Petro-Chem, Hydro Carbons, Food/Bevrge

Metalworking Electronics Assembly/Test

Metals, Paper, Rubber/Plastic

Pipelines, Mat'l Handling Conveyance

Pumps, Valves, Vats, Conveyors, Pipelines

Motors, Drives, Converting, Fabrication

Assembly/Packaging, Vessels/Tanks, etc.

Transportation

Trans Systems

Tolls, Traffic Mgmt Navigation

Vehicles

Consumer, Commercial, Construction, Off-Hiway

Non-Vehicular

Air, Rail, Marine

Vehicles, Lights, Ships

Planes, Signage

Tolls, etc.

Retail

Specialty

Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events

Hospitality

Hotels, Resaurants, Bars, Cafes, Clubs

Stores

Supermarkets, Shopping Centers, Single Site, Distribn. Centers

POS Terminals

Tags

Cash Registers

Vending Machines

Signs, etc.

Security/Public Safety

Surveillance

Radar/Satellite, Envirn, Military Security, Unmanned, Fixed

Equipment

Weapons, Vehicles, Ships, Aircraft, Gear

Tracking

Human,Animal,Postal,Food/Health, Packaging,Baggage

Public Infrastructure

Water Treatmnt, Building Environ, Gen. Environ, Surveillance

Emergency Services

Equip. & Personnel, Police, Fire, Regulatory

Tanks, Fighter Jets

Battelfield Comms

Jeeps, Cars, Ambulances

Breakdown, Lone Worker

Homeland Security, Fire

Enviro. Monitor, etc.

IT & Networks

Public

Services E-Commerce Data Centers Mobile Carriers Fixed Carriers ISPs

Enterprise

IT/Data Center Office Private Nets

Servers

Storage

PCs , Routers

Switches

PBXs, etc

Beecham Research

Boston | London

info@beechamresearch.com

+44 (0)845 533 1758

www.beechamresearch.com

Timing in Cyber-Physical Systems (CPS): Outline

- The term Timing used here as a general term: frequency, phase or time sync or source

- Expected massive growth in the Internet of Things (IoT)
- NIST has organized a Public Working Group (PWG)
  - The near-final timing framework for CPS
  - Timing future in CPS: Technology Roadmap
- Among other efforts related to timing in the IoT

The NIST CPS PWG

- Accelerate progress in cyber-physical systems across all domains.
- Currently lack a unified technical foundation for broad collaboration.
- The CPS-PWG will address this need by developing a shared foundation for progress: a **Framework Document**
- NIST provides a neutral perspective, technical expertise, and convening capability.

Q: When will key milestones be reached?

- June 30, 2014: Kick-off webinar
- August 11-12, 2014: First face-to-face workshop at NIST
- December, 2014: Initial Sub-group reports complete
- March, 2015: Release the integrated framework for public review
- Spring, 2015: Integrated CPS framework complete
- April 7-8, 2015: Second workshop to launch Technology Roadmap effort
- Fall, 2015: Technology Roadmap complete

NIST CPS PWG Subgroups and Framework Document Sections

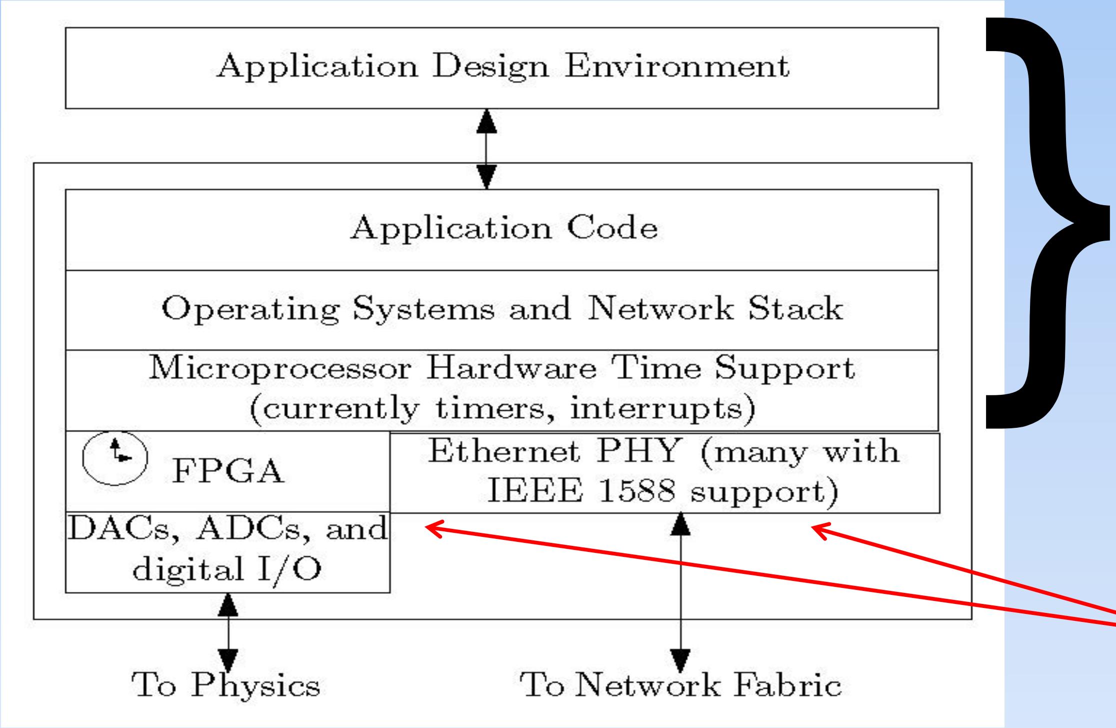
- Each subgroup has an industry, academia, and NIST co-chair

- Reference Architecture
- Cybersecurity
- Data Integration
- Timing
- Use Cases

CPS PWG Framework Timing Section

- Timing subgroup cochairs
  - Marc Weiss – NIST
  - Hugh Melvin – National University of Ireland, Galway (NUIG)
  - Sundeep Chandhoke, National Instruments (NI)
- Timing Section of Framework
  - Introduction
  - Time-Awareness
  - Timing and Latency
  - Timing Security

Time Awareness: CPS Node and Environment, Currently

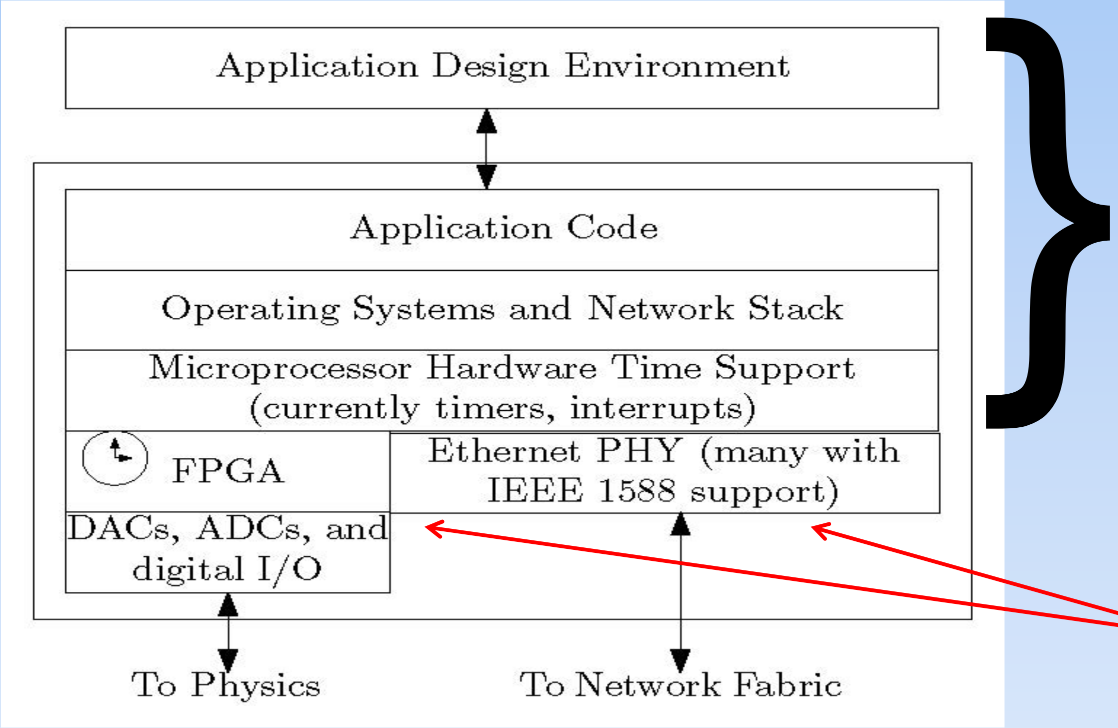

Application Design Environment
Application Code
Operating Systems and Network Stack
Microprocessor Hardware Time Support (currently timers, interrupts)
FPGA
Ethernet PHY (many with IEEE 1588 support)
DACs, ADCs, and digital I/O
To Physics
To Network Fabric

- No semantics of accurate time neither in design, nor languages
- Possibly bounded TIs
- Almost never stable (deterministic)
- Hence robust, correct by construction solutions cannot be done here!

- Precise TIs
- Can be accurate (traceable to SI second or TAI)
- Hence robust, correct by construction is possible (but not very flexible)

This slide based on ones by John Eidson

Time Awareness: CPS Node and Environment Potential Future with Correct by Construction



Application Design Environment

Application Code

Operating Systems and Network Stack

Microprocessor Hardware Time Support (currently timers, interrupts)

FPGA

Ethernet PHY (many with IEEE 1588 support)

DACs, ADCs, and digital I/O

To Physics

To Network Fabric

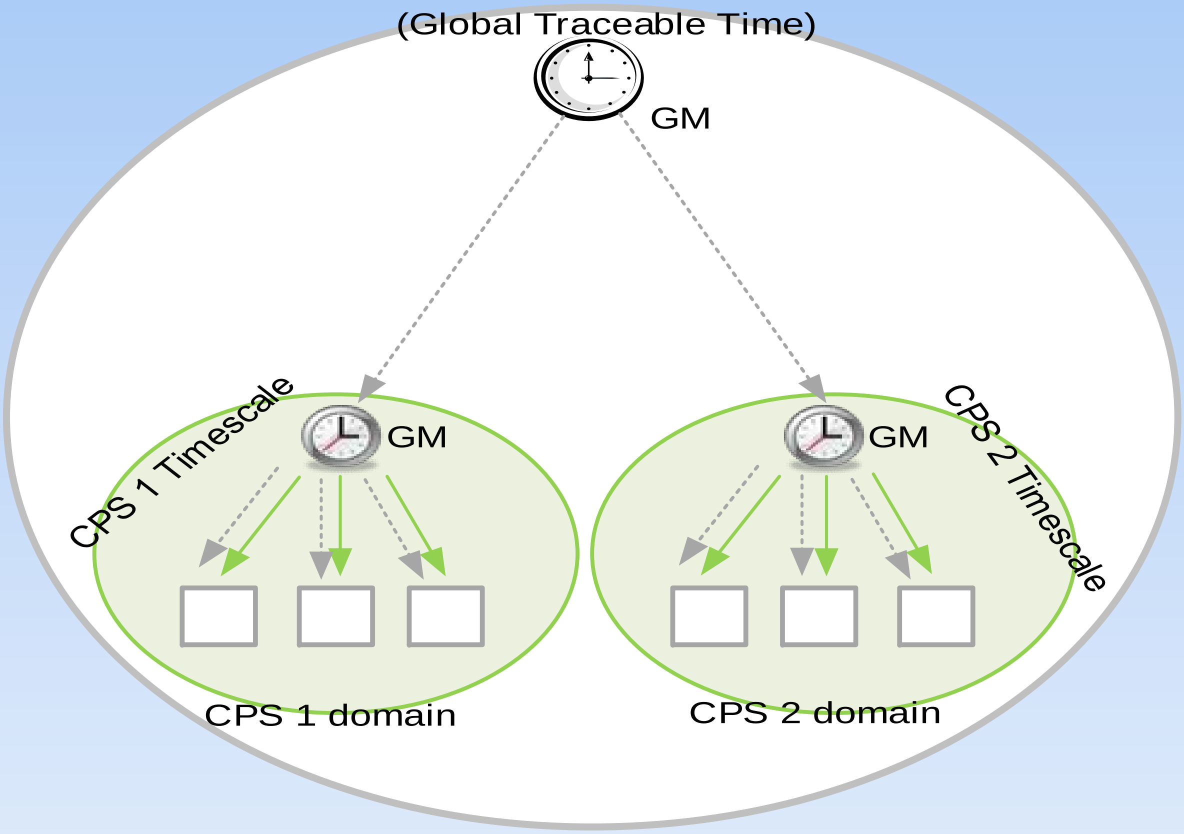
- Time can be specified as abstraction in model
- Code is Bounded and Time explicit
- I/O is Time sensitive, explicit, and precise
- CPU clock is precise and if needed accurate
- Hence robust, correct by construction solutions can be done here!

- Precise TIs
- Can be accurate (traceable to SI second or TAI)
- Hence robust, correct by construction is possible (but not very flexible)

This slide based on ones by John Eidson

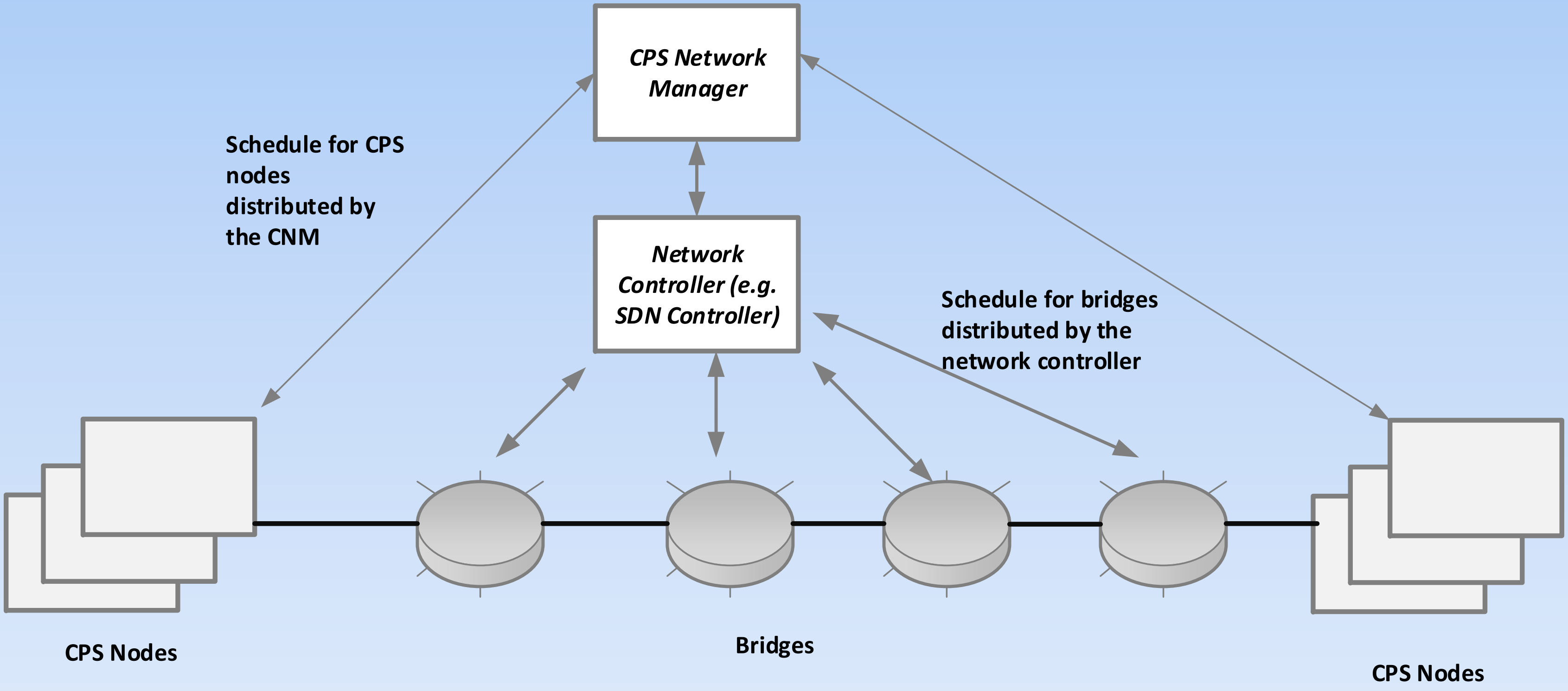
Timing and Latency: Domains and Multiple Time-scales in Time-aware CPSs

Source: Sundeep Chandhoke, National Instruments



CPS Network Manager configuring a CPS

Source: Sundeep Chandhoke, National Instruments



CPS Network Manager

Network Controller (e.g. SDN Controller)

Schedule for CPS nodes distributed by the CNM

Schedule for bridges distributed by the network controller

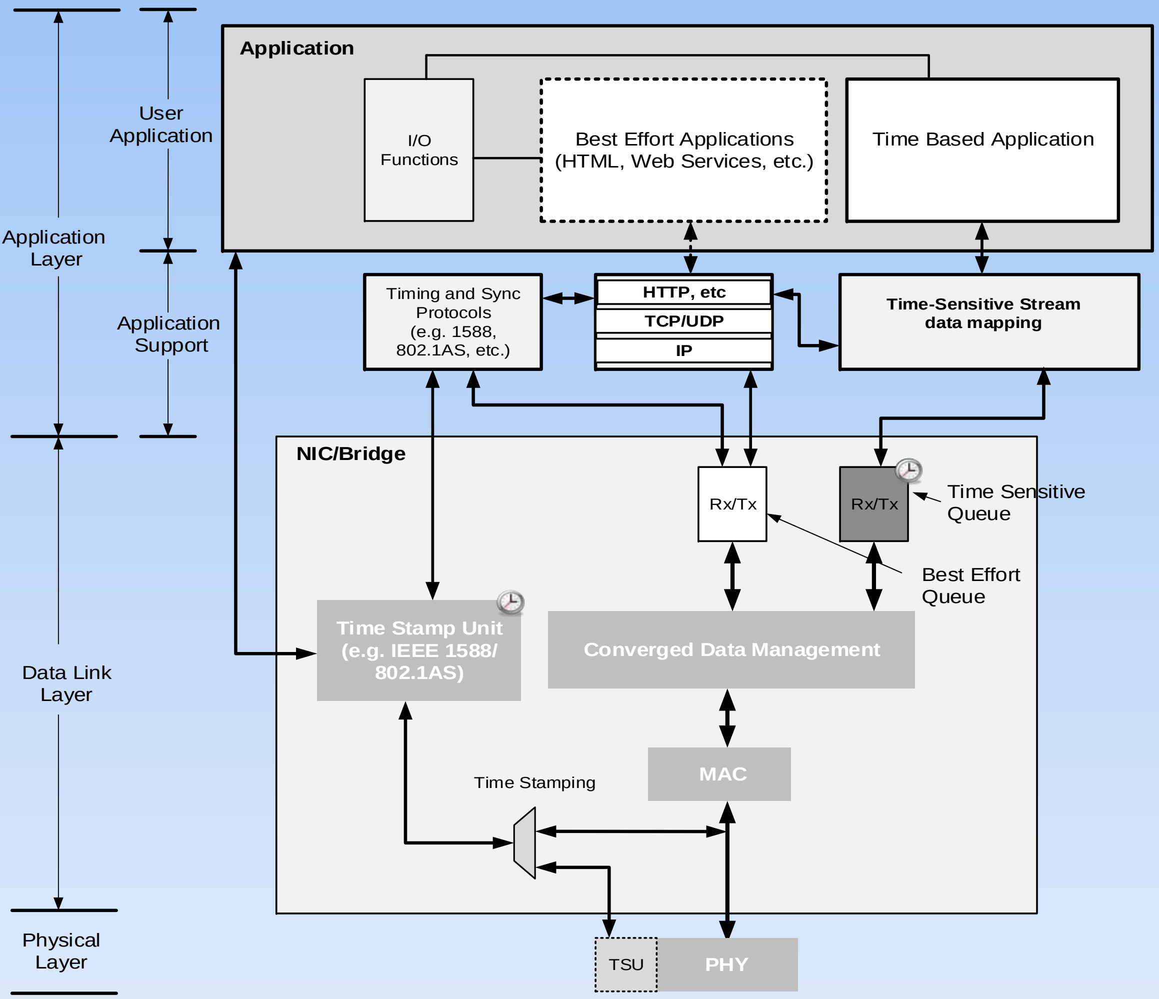
CPS Nodes

Bridges

CPS Nodes

Time-Aware CPS Device Model: Convergence of **Best Effort** and **Time Sensitive** Systems

Source: Sundeep Chandhoke, National Instruments



Elements of Secure Timing: assurance

Source channel assurance	Opportunities to verify that timing information is delivered via an undistorted channel whose expected behavior is well characterized to ensure any deviations can be quickly detected. Distortion of the time-transfer channel may be driven by natural events (e.g. solar weather), unintentional actions (e.g. physically bumping an antenna), or intentional manipulation (e.g. introducing a time delay via spoofing). The data carried by a time-transfer channel may assist in verifying the channel itself. Enablers of channel verification may include unpredictable bits of a digital signature, or a symmetrically encrypted channel.
Source data assurance	Verification mechanisms to prove timing data are not forged. These may include digital signatures or symmetrically encrypted packets.
User provided assurance	User implemented security to verify unassured timing information. This may include anti-spoof GNSS receiver techniques or additional layers of network security.

Elements of Secure Timing: resilience

Predictable failure	Known CPS failure modes that account for timing denial and other detected timing anomalies.
Diversity & Redundancy	Multiple sources and paths of secure time are available to a CPS. Where possible, sources are verified against each other, and in the event of a denial or spoofing attack on one source or other timing anomaly, a mechanism to switch to a redundant source is available.

Survey of Time Distribution Methods

	Order of Timing	Source Channel Assurance Provided Today	Source Data Assurance Provided Today	Source Channel Assurance Possible via Enhancement	Source Data Assurance Possible via Enhancement
GPS L1 C/A	nanoseconds	No	No	No	No
GPS L2C/L5	nanoseconds	No	No	Yes	Yes
Galileo	nanoseconds	No	No	Yes*	Yes*
PTP [165]	nanoseconds	No	No	Yes	Yes
NTP [166]	milliseconds	No	No	Yes	Yes
eLoran [167]	nanoseconds	No	No	Yes	Yes
WWVB [168]	microseconds	No	No	Yes	Yes

*Galileo is not yet a fully operational GNSS constellation, but has indicated strong support for source channel and data assurance via navigation message authentication.

Achieving secure time

- system detects potential timing compromises
- redundant timing source
  - redundancy and diversity of routes to time and frequency sources as well as holdover capabilities of high stability oscillators
- Today: ensure systems can maintain timing within the tolerance of their application for the duration of a timing compromise
- Future: detect compromises early enough that CPS seamlessly function

Next in CPS PWG: Timing Roadmap, Research and Recommendations

- Timing “Correct-by-Construction” techniques
- Convergence of best-effort with time-sensitive systems
  - IT and OT systems
  - How to (or can one?) include cloud and big data systems in RT control
- Timing in Lightweight devices
- Security
  - Predictable failure vs. switchover
  - GPS Spoofing protection
  - PTP security: redundancy, authentication, timing MitM protection

Timing in Cyber-Physical Systems: Outline

- The term Timing used here as a general term: frequency, phase or time sync or source

- Expected massive growth in the Internet of Things (IoT)
- NIST has organized a Public Working Group (PWG)
  - The near-final timing framework for CPS
  - Timing future in CPS: Technology Roadmap
- Some other efforts related to timing in the IoT

NSF Call for Proposals 15-541

- Research needed to support systems engineering of high-confidence CPS
- CPS have enormous complexity and variations
  - Size of systems from tiny to global
  - Transience of systems
- Goal: to develop the core system science needed to engineer complex cyber-physical systems which people can depend upon

- http://www.nsf.gov/pubs/2015/nsf15541/nsf15541.htm

TAACCS
Time-Aware Applications, Computers, and Communication Systems

http://taaccs.org/

- Face-to-face meetings coming up
  - March 13 immediately after WSTS at Carnegie-Mellon U here in Silicon Valley
  - April 6 immediately before the CPS PWG f2f at NIST, Gaithersburg, MD
- Three current projects
  - WG 110: Seminar on timing APIs, to lead to R&D
  - WG 211: CPS Applications on globally timed platforms
  - WG 212A: Timing support for safety critical systems
- Proposal for NSF call on CPS

The Industrial Internet Consortium (IIC)

- Mission: To accelerate growth of the Industrial Internet by coordinating ecosystem initiatives to connect and integrate objects with people, processes and data using common architectures, interoperability and open standards that lead to transformational business outcomes.
- Open membership, global, nonprofit
- Founded by AT&T, Cisco, GE, IBM and Intel
- Governed by the IIC Steering Committee
  - 10 members
    - 5 permanent seats by Founding companies; 2 members from large enterprise; 1 member from small enterprise; 1 from academia; 1 seat for Executive Director, ex officio
    - Any company can run for an open seat in its category

Thanks for your attention!

Questions?