Time-Awareness in the Internet of Things

NUIG, October 2014

Marc Weiss, NIST Consultant

mweiss@nist.gov ++1-303-497-3261

Outline: Time-Aware Systems in the Internet of Things

- Motivation
  - Anticipated large growth
  - Timing and computing don’t mix!
  - What is Timing?
- Who is Developing Systems that Need Timing
  - Government science foundations
  - Industrial Internet
  - Cyber Physical Systems
- Time-Aware Systems – TAACCS group
  - Oscillators
  - Time transfer
  - Time in networks
  - Hardware/software support
  - Development Environments
  - Applications
- Timing Security
  - General issues
  - Jamming and Spoofing in GPS
- Conclusions

Main Points of this Talk

- Huge growth is expected in the Internet of Everything
- A few groups are addressing timing
- New Paradigms for timing will be needed to wed IT to OT: Time-Aware Systems
  - Example of “Correctness by Design”
  - Timing security leads to different requirements than cybersecurity
- One Area: Cyber-Physical Systems
  - Requirements on time intervals between events
  - Time network management
  - Timing security and resilience
- Timing Security: Protect Both Signal Plus Data
  - Jamming and Spoofing in GPS
  - Similar (yet different!) vulnerabilities in networks

Cisco White Paper

White Paper

Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion

More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience

Joseph Bradley
Joel Barbier
Doug Handler

To get the most value from IoE, business leaders should begin transforming their organizations based on key learnings from use cases that make up the majority of IoE's Value at Stake.

Executive Summary

- The Internet of Everything (IoE) creates $14.4 trillion in Value at Stake — the combination of increased revenues and lower costs that is created or will migrate among companies and industries from 2013 to 2022.
- The five main factors that fuel IoE Value at Stake are: 1) asset utilization (reduced costs) of $2.5 trillion; 2) employee productivity (greater labor efficiencies) of $2.5 trillion; 3) supply chain and logistics (eliminating waste) of $2.7 trillion; 4) customer experience (addition of more customers) of $3.7 trillion; and 5) innovation (reducing time to market) of $3.0 trillion.
- Technology trends (including cloud and mobile computing, Big Data, increased

GE White Paper

Figure 2. Rise of the Industrial Internet

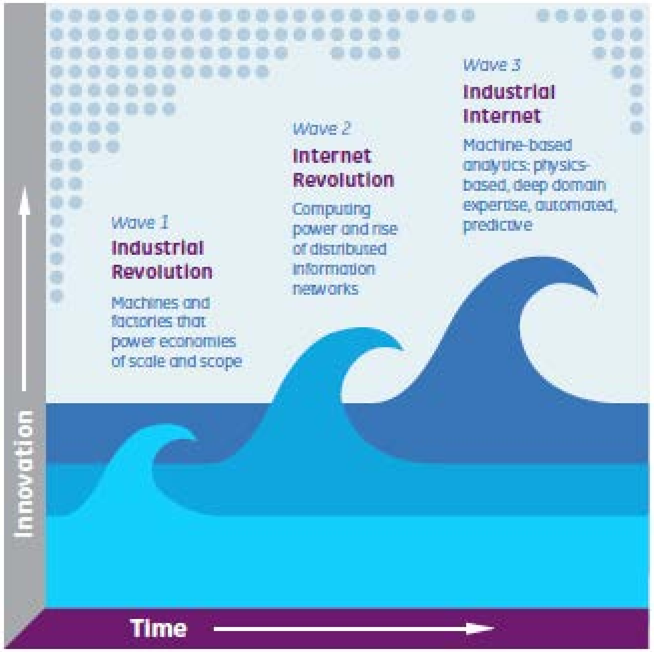
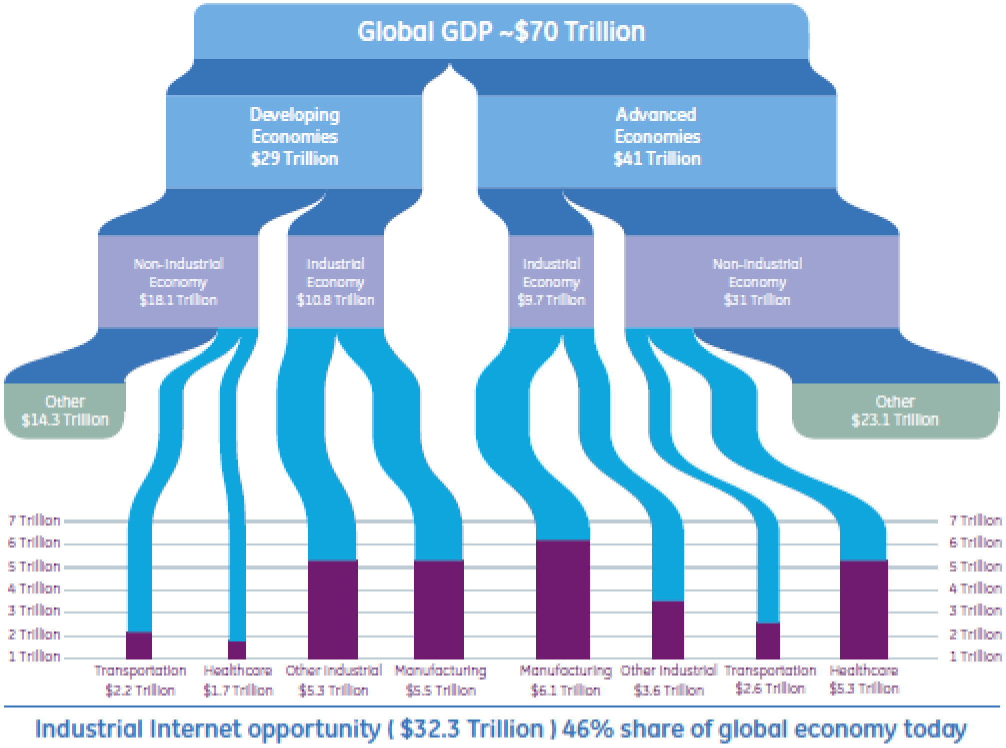


Figure 5. Industrial Internet Potential GDP Share



Source: World Bank, 2011 and General Electric

A Broad Set of Applications

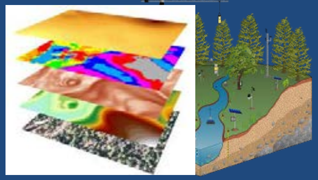
Predictive maintenance

Energy Saving (I2E)

Intelligent Buildings

Defense

Industrial Automation



Enable New Knowledge

Transportation and Connected Vehicles

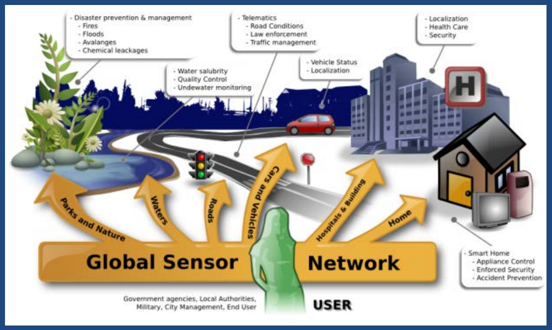
Enhance Safety & Sec

Agriculture

Healthcare

Smart Home

Smart Grid

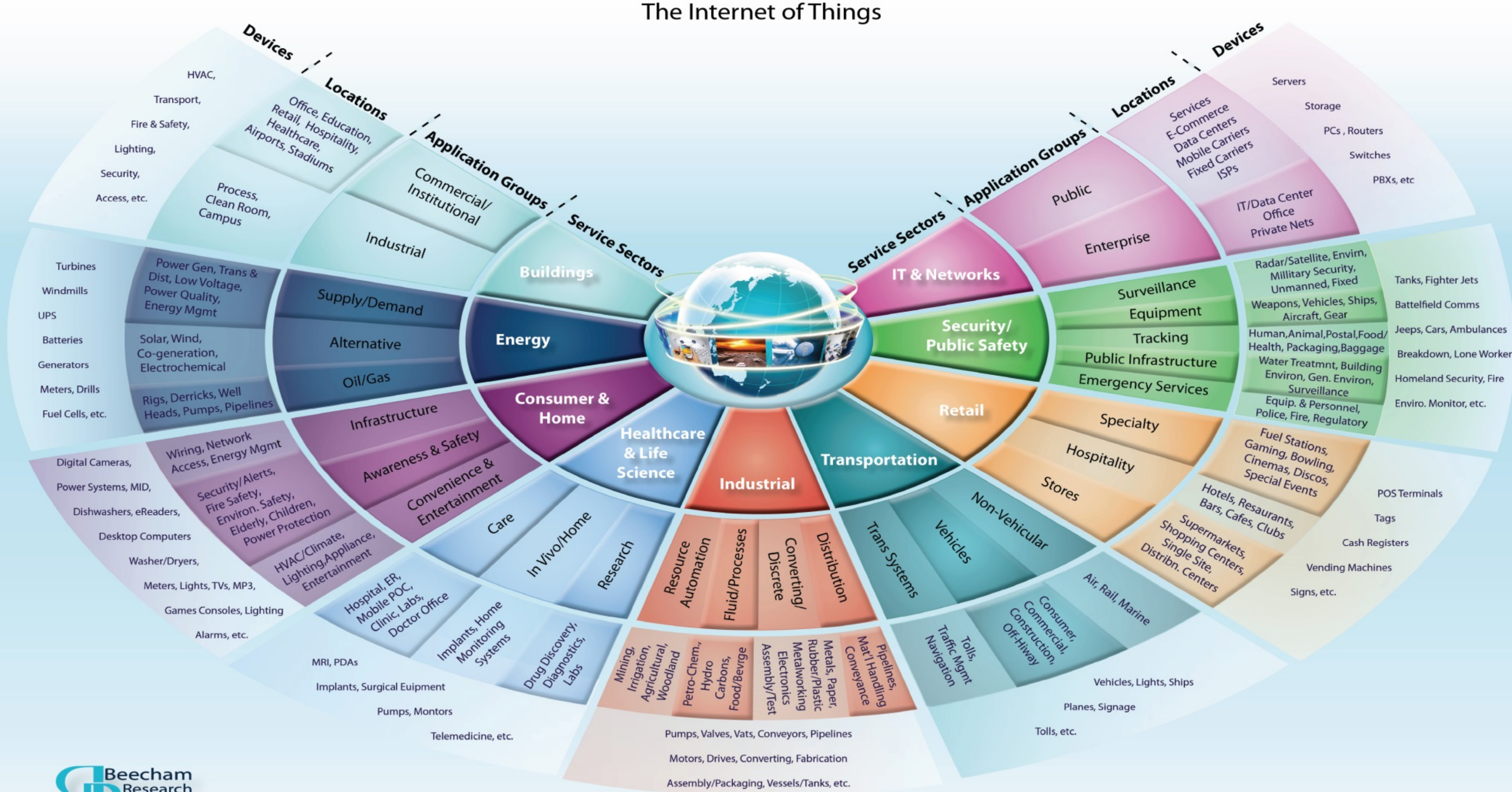


Smart City

Source: Cisco (flavio@cisco.com)

M2M World of Connected Services

The Internet of Things



Beecham Research

Boston | London

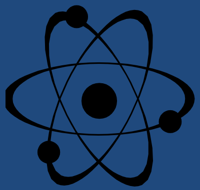
info@beechamresearch.com +44 (0)845 533 1758 www.beechamresearch.com

Systems that Benefit from Precise Time

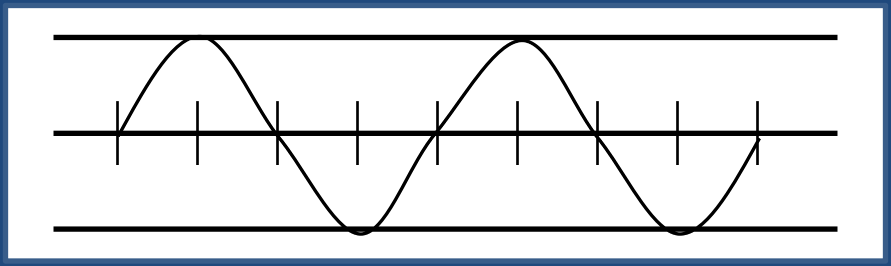
- Audio-visual transmission
- Time stamping of events
  - Correlation for analysis
  - Data aggregation
- Telecom systems
  - Multiplexing
  - Wireless access
- Optimal use of wireless spectrum
- Cyber-Physical Systems (CPS)
  - Local systems
  - Global systems
- Temporal determinism in software
  - Optimizes energy usage and resource allocation
  - Supports CPS timing (sensing to actuation)
  - Allows increased regulation in trades
- Location-based services
  - 1 ns = 1 foot
- Many, many more…

Time and Frequency Sources

- A clock is a frequency device based on physics



- Electronic systems count cycles for time interval

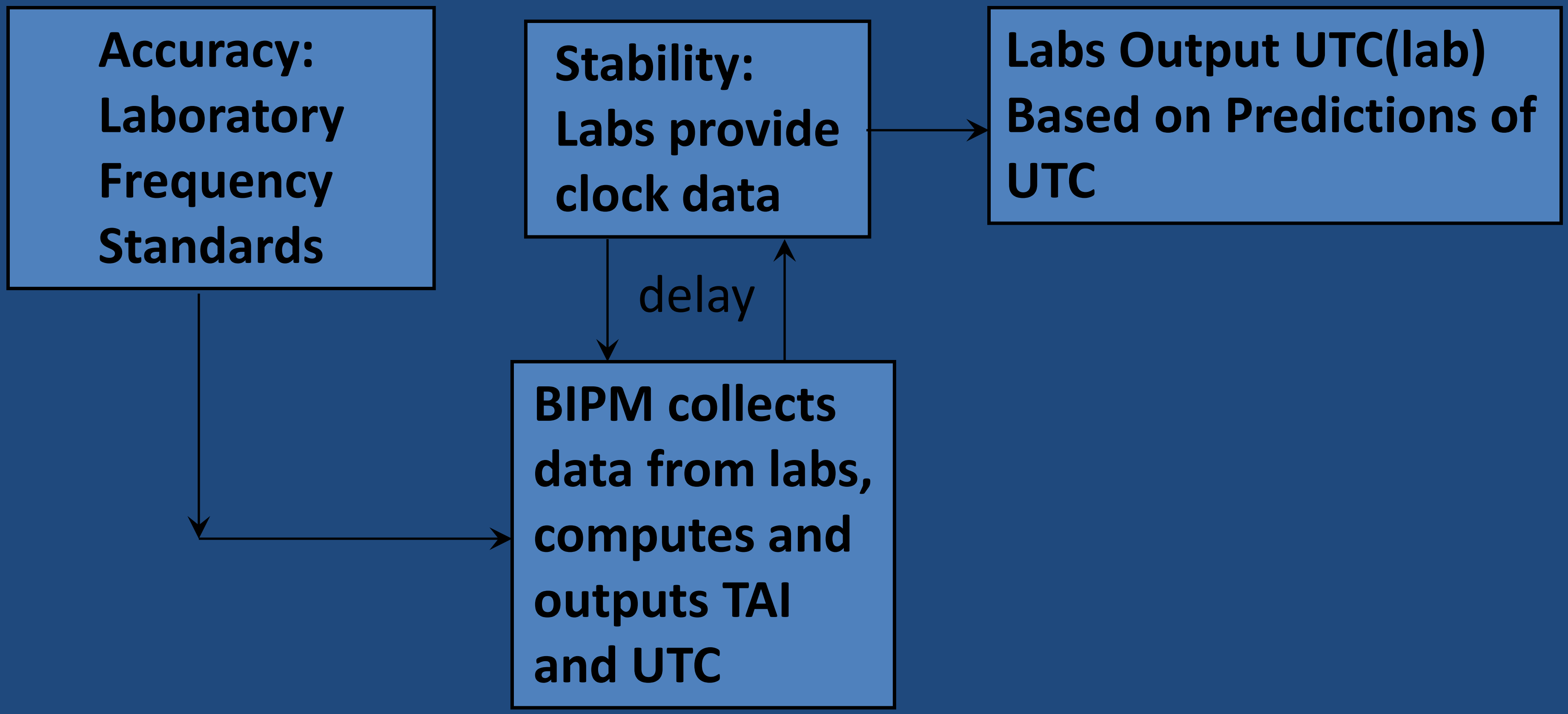


- Time is steered to UTC

Three Types of Sync

- Frequency
  - Match the rate only – syntonization
  - Usually inexpensive oscillator locked to a reference
  - Used e.g. for multiplexing
- Phase
  - Match epochs
  - Ensure simultaneity of control or logging
- Time
  - Same year-month-day, hour-minute-second
  - Refer to external time scale, e.g. UTC
  - Used e.g. for synchrophasors in electrical network

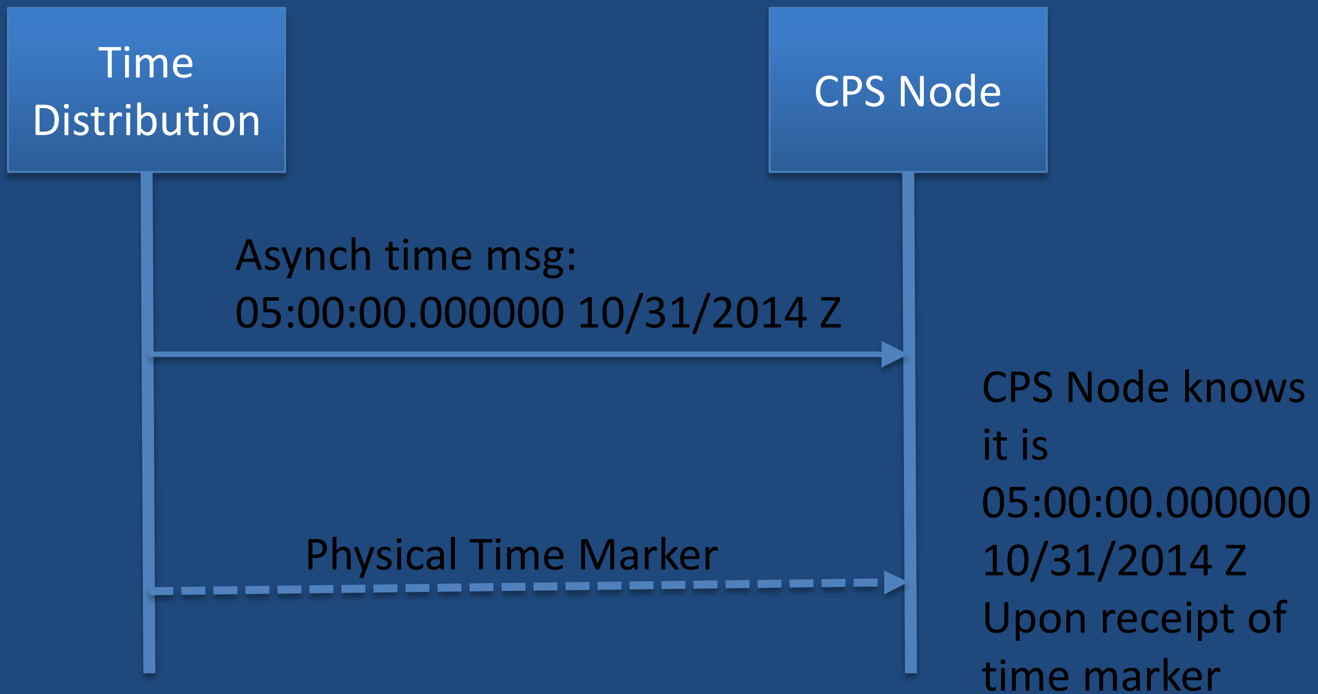
The Generation of UTC: Time Accuracy
Any Real Time UTC is only a Prediction
A PLL with a one-month delay



Time and Frequency Needs Signals!

- Signals are Physical with data
  - Accuracy and stability are no better than the physical layer
  - Data layers disrupt the T & F signals
  - Interference to the physical signal blocks access to T & F
  - Data modifies the signal, but does not require sync
- Communications systems are layered with devices only connected to the neighboring layers
  - Sync gets worse farther from the physical layer

Time Signal Plus Data



Two Issues Here

- Since a clock is a frequency device, the best clock exhibits only white noise on frequency, hence a random walk in phase. Even the best clocks will walk off unboundedly in time.

- Since the time standard is artificial, time MUST be transferred from the relevant time standard
  - There is often confusion with the human experience of time vs. metrological time. Standard time is a signal plus data
  - Often what is needed is synchronization among locations, not UTC per se, though that is often the most efficient way to achieve sync

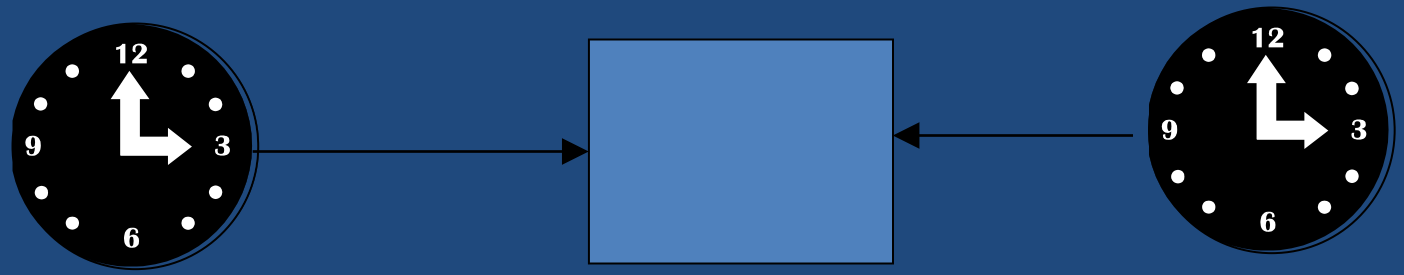
The IoT Will Need Synchronization

- Since optimal data techniques obstruct synchronization

- Internet of Things requires New Paradigms for combining Time and Data
  - Need to be able to design time correctness independent of hardware
  - Need determinism and security in networks

One-Way Dissemination or Comparison System

Clock 1 **Clock 2**



Clock 1 Systematics and Noise

Delay, Perturbations, and Measurement Noise

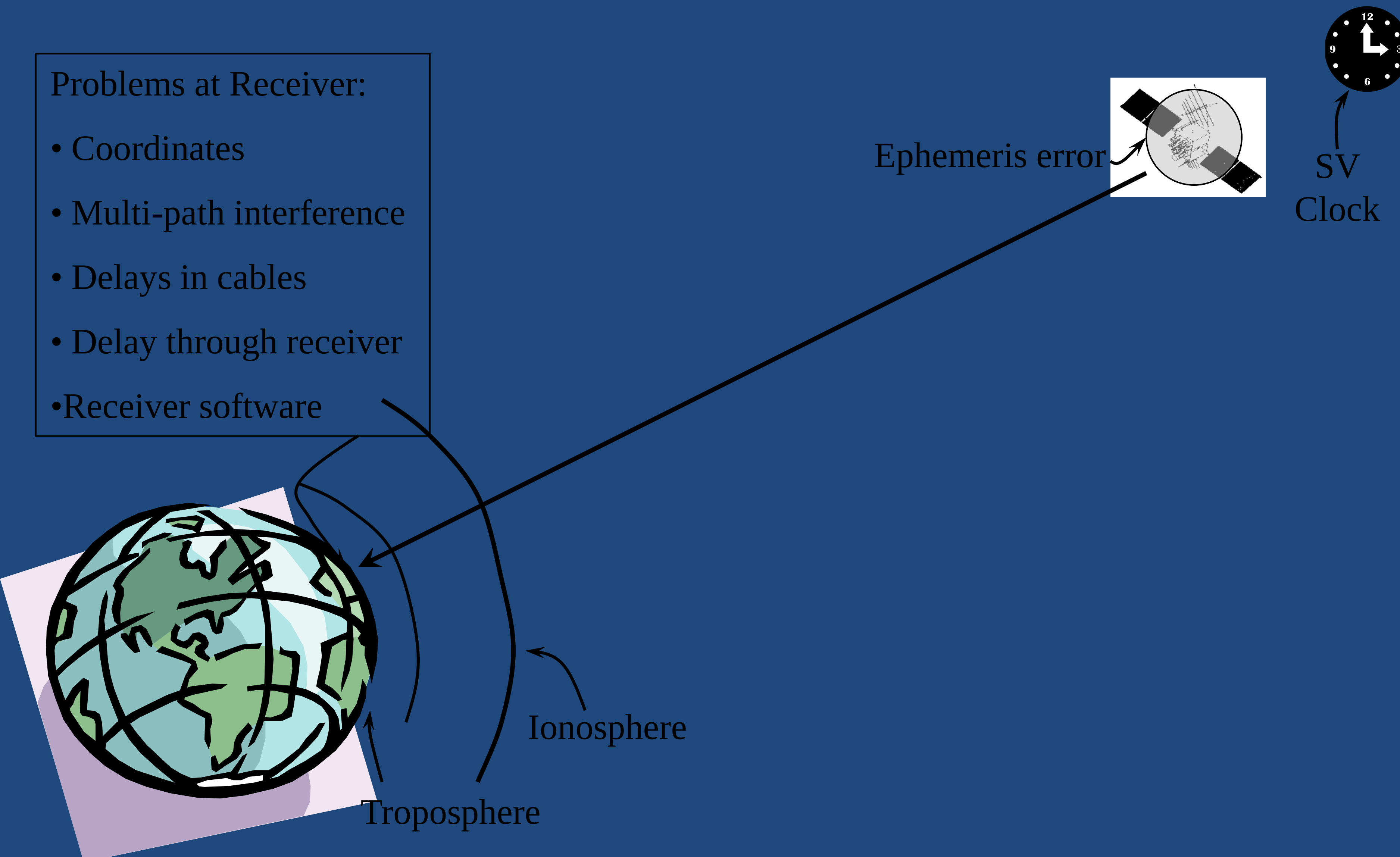
Clock 2 Systematics and Noise

One-way Time Transfer requires determining and removing the Delay

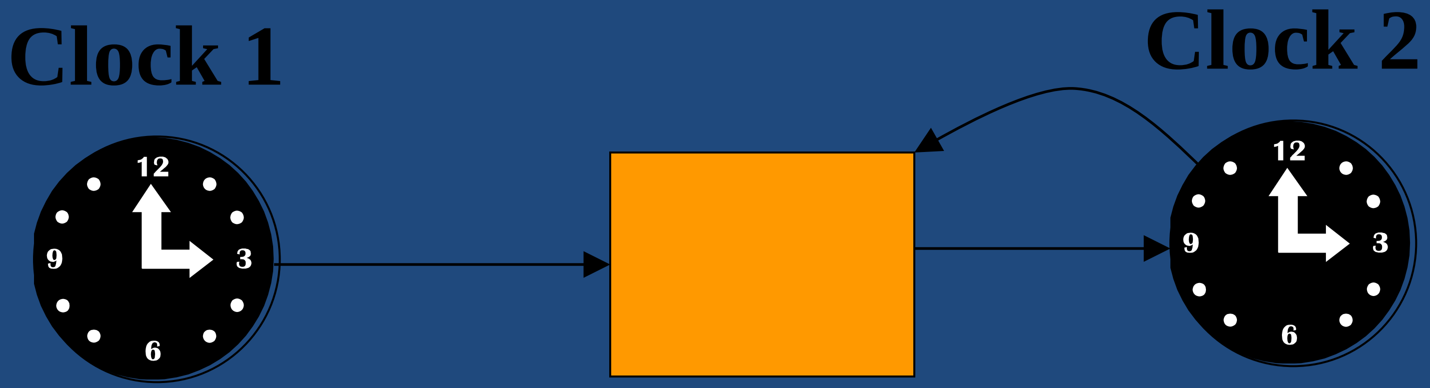
One-Way Time Transfer: GPS

Problems at Receiver:

- Coordinates
- Multi-path interference
- Delays in cables
- Delay through receiver
- Receiver software



Clock Hierarchies

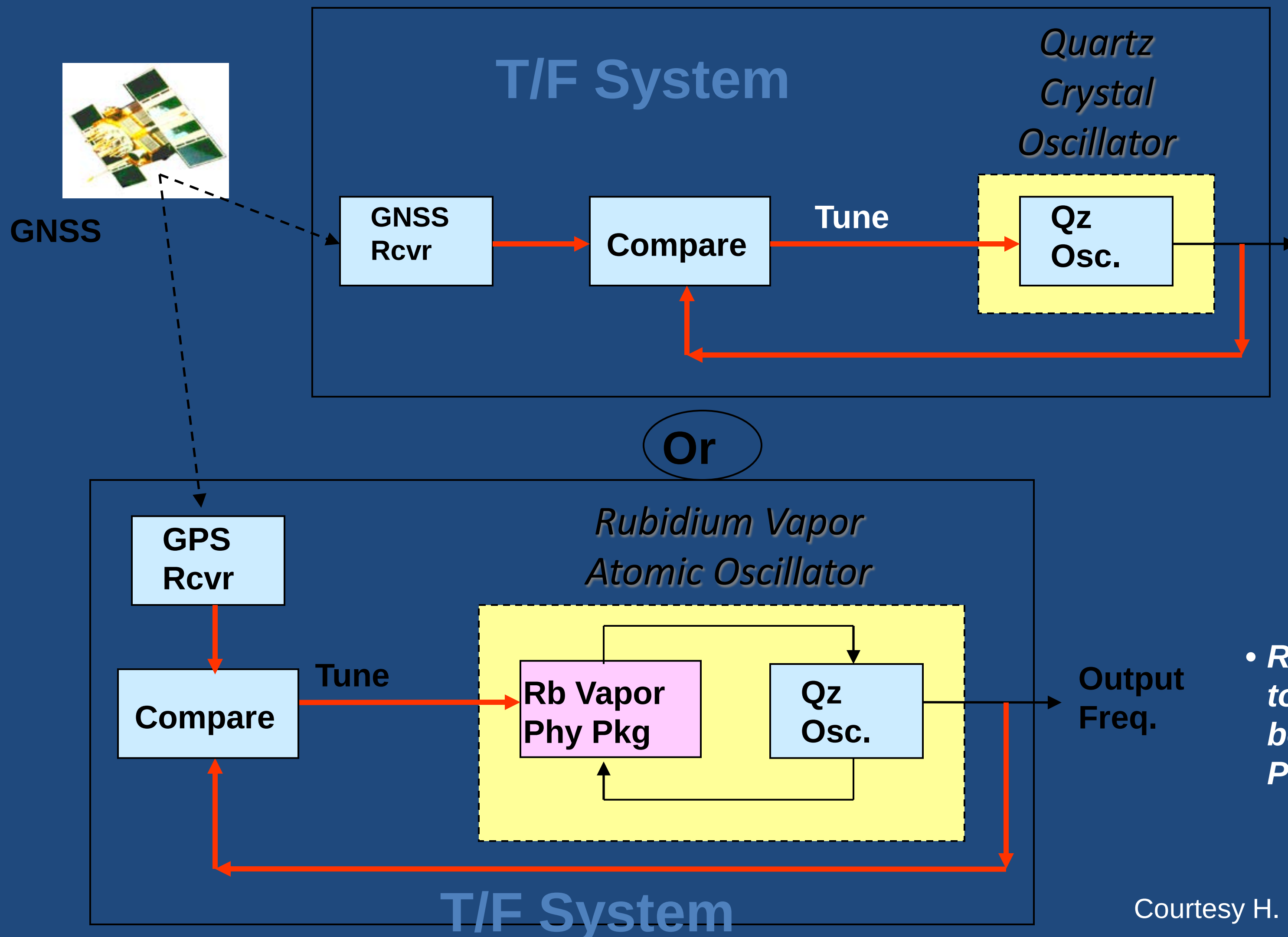


Clock 1 Systematics and Noise

Lock Loop Systematics and Noise: Contributions from Measurement Noise and Path Perturbations

Clock 2 Systematics and Noise

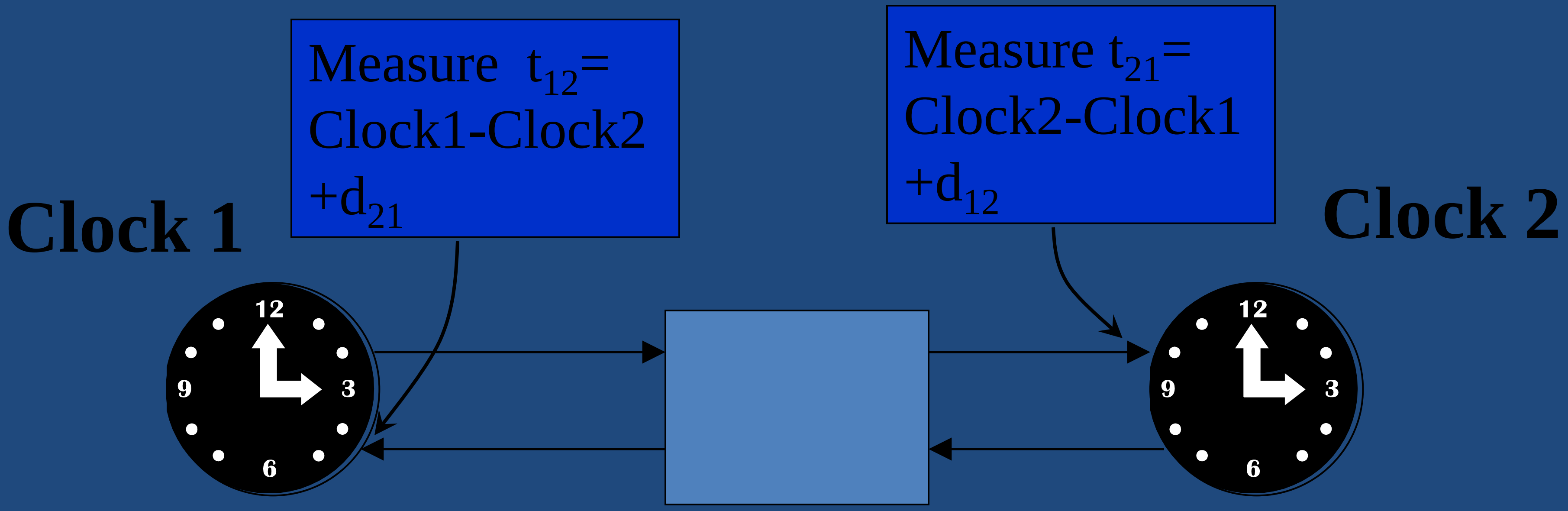
GNSS-aided Time and Frequency Systems: Lock Local Oscillator to GPS



- ***Rb oscillator 100 to 1000 times better Holdover Performance***

Courtesy H. Fruehauf, ViaLogy LLC

Two -Way Comparison System



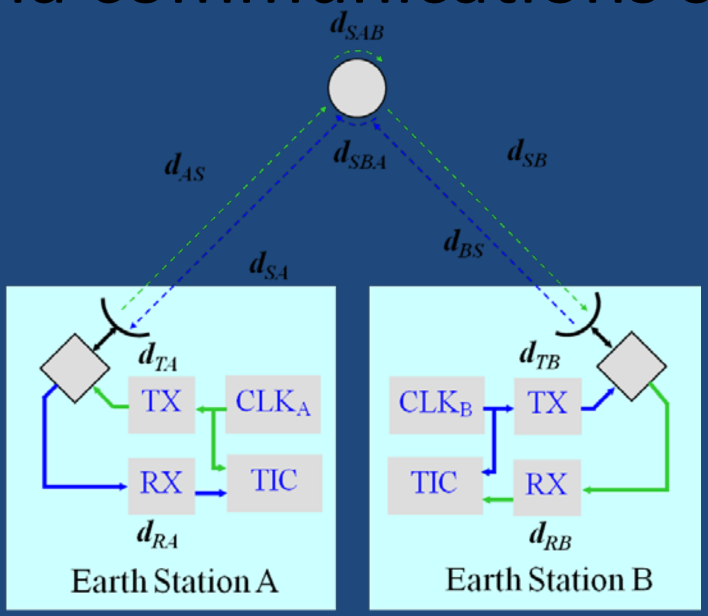
Clock 1 Systematics and Noise

Two-way transfer depends on the Path being Reciprocal: $d_{21} = d_{12}$

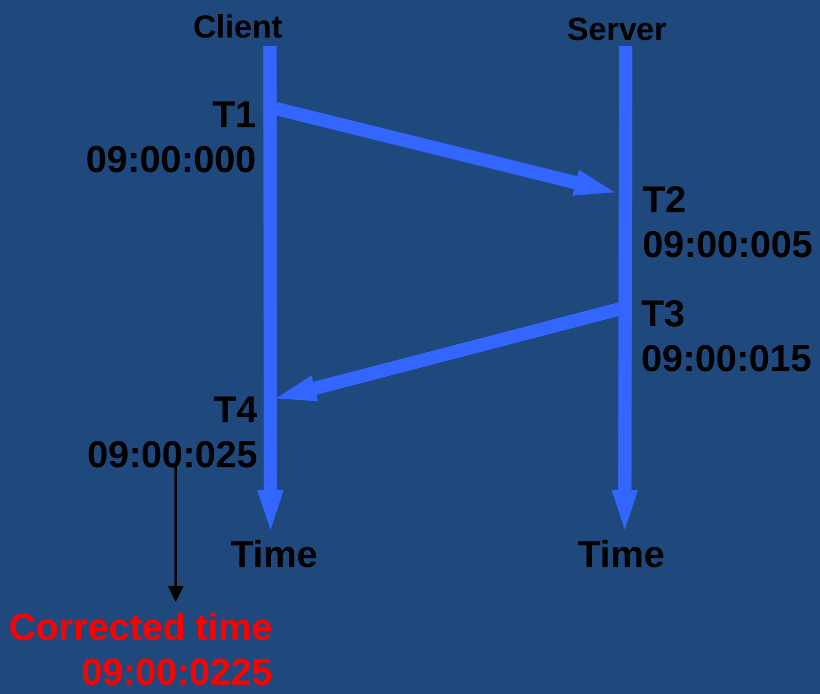
Clock 2 Systematics and Noise

Two-Way Time Transfer

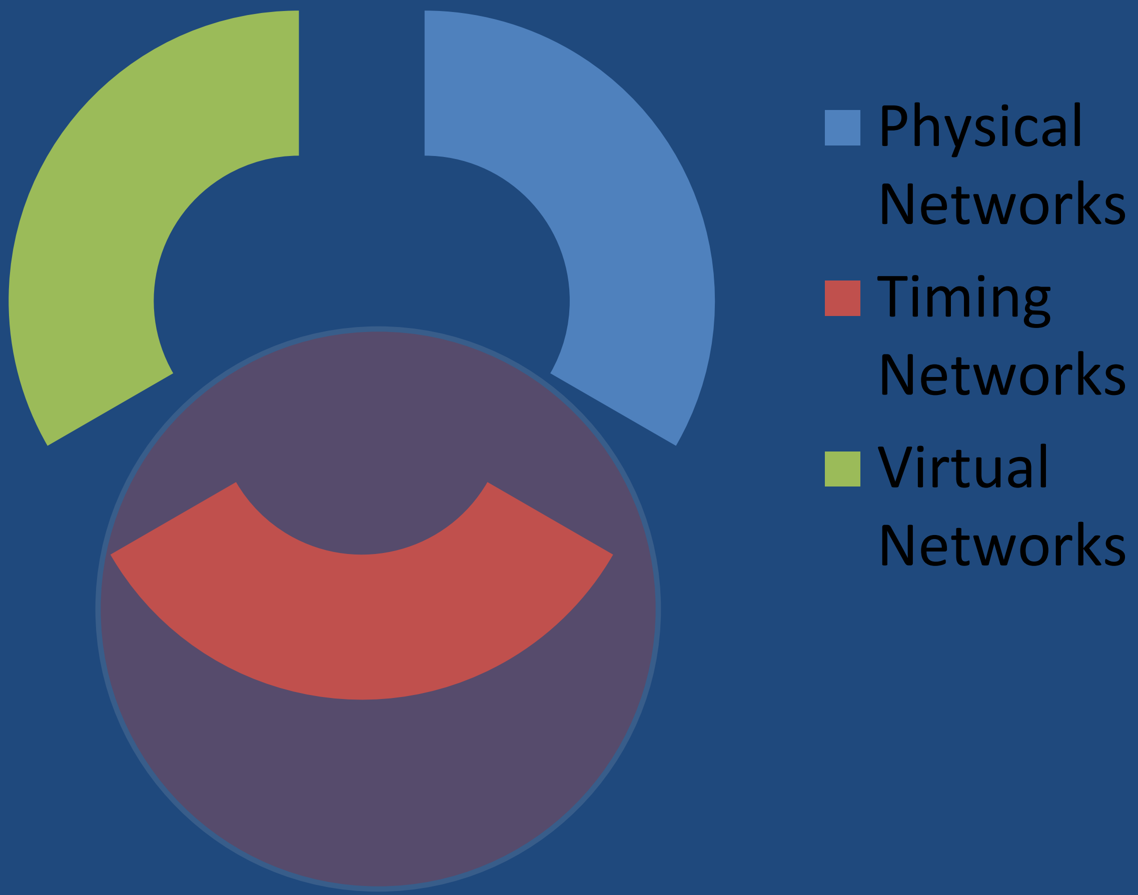
- Via communications satellite



- In networks
  - NTP
  - PTP



We need a new network



Timing Network is both Physical and Virtual !

Outline: Time-Aware Systems in the Internet of Things

- Motivation
  - Anticipated large growth
  - Timing and computing don't mix!
  - What is Timing?
- Who is Developing Systems that Need Timing
  - Government science foundations
  - Industrial Internet
  - Cyber Physical Systems
- Time-Aware Systems – TAACCS group
  - Oscillators
  - Time transfer
  - Time in networks
  - Hardware/software support
  - Development Environments
  - Applications
- Timing Security
  - General issues
  - Jamming and Spoofing in GPS
- Conclusions

Press Release 14-074
Revolutionizing how we keep track of time in cyber-physical systems

New five-year, $4 million Frontier award aims to improve the coordination of time in networked physical systems

NSF announces five-year, $4 million award to tackle the challenge of time in cyber-physical systems.
Credit and Larger Version

June 13, 2014

The National Science Foundation (NSF) today announced a five-year, $4 million award to tackle the challenge of synchronizing time in cyber-physical systems (CPS)--systems that integrate sensing, computation, control and networking into physical objects and infrastructure.

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

IIC Announcement – March 27, 2014

industrial internet CONSORTIUM

AT&T, CISCO, GE, IBM AND INTEL FORM INDUSTRIAL INTERNET CONSORTIUM TO IMPROVE INTEGRATION OF THE PHYSICAL AND DIGITAL WORLDS

Technology leaders drive industry ecosystem to accelerate more reliable access to big data to unlock business value

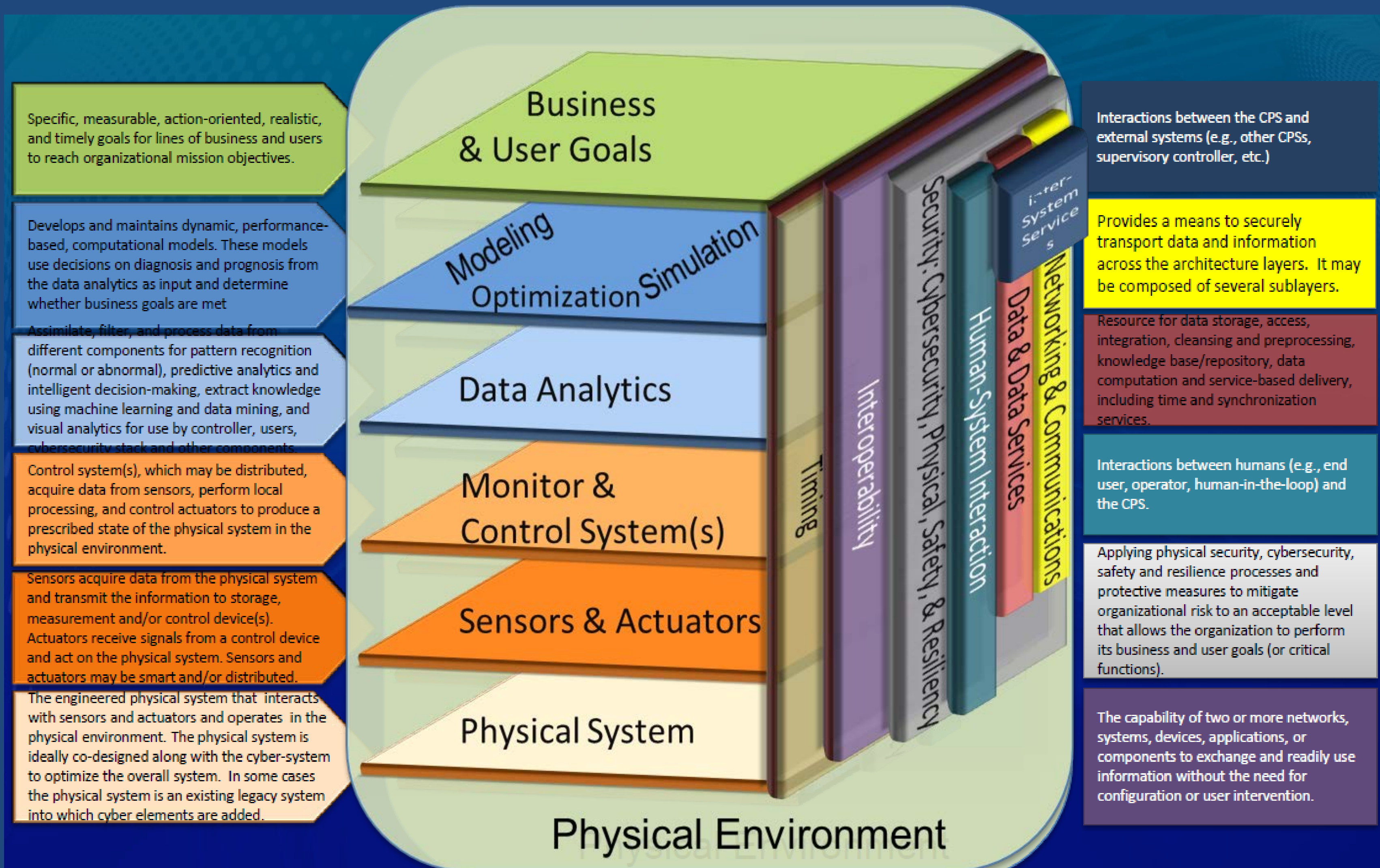
- Identify requirements for open interoperability standards and define common architectures to connect smart devices, machines, people, processes and data
- Open membership for any public or private business, organization or entity interested in driving global market development for the Industrial Internet

March 27, 2014 – Boston, MA – AT&T, Cisco, GE, IBM and Intel today announce the formation of the Industrial Internet Consortium (IIC), an open membership group focused on breaking down the barriers of technology silos to support better access to big data with improved

<u>Announcement highlights</u>

- 150+ articles to date
  - Business, technology and industry publications
  - Press release viewed over 24,000 times
- Hundreds of social media posts
  - Estimated audience of 3.6 million within first 24 hours
- 93% neutral-positive sentiment

Cyber Physical Systems



NIST CPS Public Working Group

Public Collaboration of Government, Academia, and Industry

NIST CPS Public Working Group

- The CPS PWG is composed of five initial sub-working groups, each with Government, Academic, and Industrial Co-Chairs
  - Vocabulary and Reference Architecture
  - Use Cases
  - **Timing and Synchronization**
    - **Co-Chairs: Marc Weiss, NIST—Government, Hugh Melvin, NUIG—Academic, Sundeep Chandhoke, NI—Industrial**
  - Cybersecurity and Privacy
  - Data Interoperability

Outline: Time-Aware Systems in the Internet of Things

- Motivation
  - Anticipated large growth
  - Timing and computing don't mix!
  - What is Timing?
- Who is Developing Systems that Need Timing
  - Government science foundations
  - Industrial Internet
  - Cyber Physical Systems
- Time-Aware Systems – TAACCS group
  - Oscillators
  - Time transfer
  - Time in networks
  - Hardware/software support
  - Development Environments
  - Applications
- Timing Security
  - General issues
  - Jamming and Spoofing in GPS
- Conclusions

TAACCS Initiative

www.taaccs.org

- A new initiative started with a face-to-face meeting in June 2014
- 50+ experts in timing focused on needed research

Critical Research Needs: New Paradigms

1. **Oscillators** in the network will require a range of performance and cost, as well as ensembling methods, that challenge the state-of-the art
2. **Time Transfer Systems** will need to deliver signals to orders of magnitude more endpoints than currently, with both specified accuracy and integrity, and by traversing both wired and wireless systems
3. **Time Aware Networks** will need development in a number of areas:
    1. **Network equipment** hardware and software will need designs that support and utilize time awareness
    2. Development of time aware and controlled networks requires research in both **propagating and using timing signals**
    3. Time awareness is a critical factor in **controlling latency** in networks, which is crucial to tele-surgery, online gaming, the financial industry and other areas
    4. Timing and analysis for **performance monitoring** is a challenge for maintenance
    5. **Spectrum bandwidth utilization** can be optimized with precision timing

Critical Research Needs: New Paradigms

4. **Timing support** for applications will need cross-discipline research in the following areas:

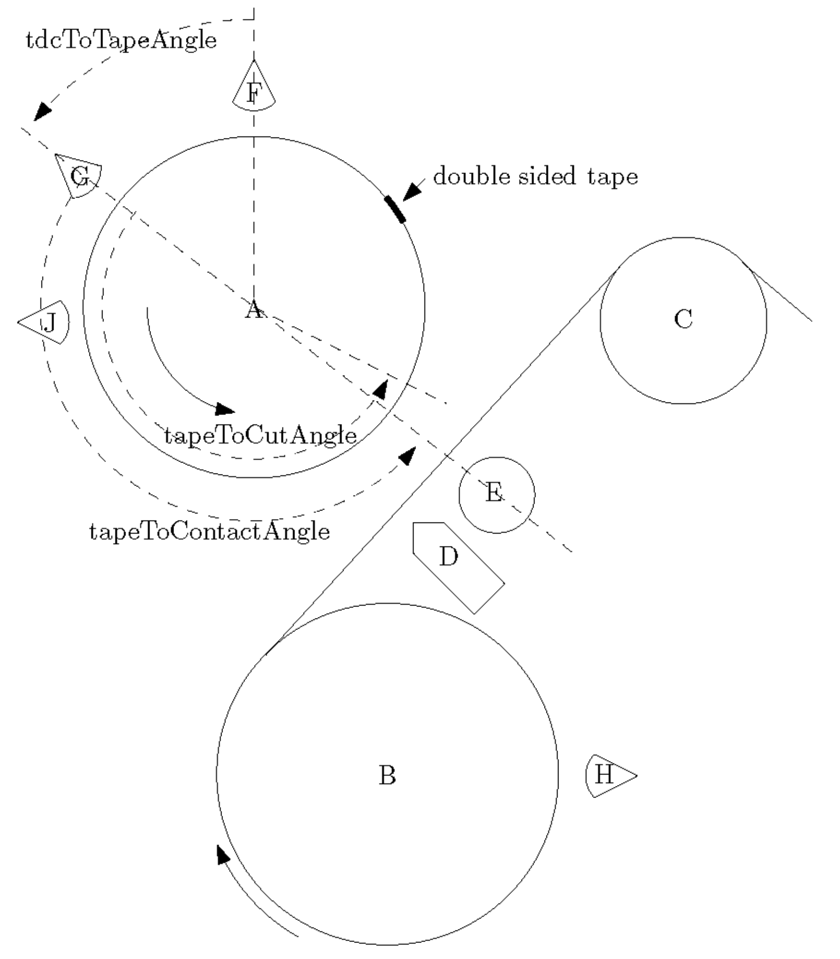
Focus in next slides

   1. Hardware and software support of **predictable execution** will need to balance the depth of change in systems with cost and implementation
   2. Timing across **interfaces** will require standards and latency control both between CPU and in crossing network domains
   3. **Scale** issues in supplying time to large numbers of systems

5. **Development environments** will need the ability to specify timing accuracy independent of the hardware that systems are running on
6. **Applications** can make innovative use of time, and will further stimulate the development of these other items.

An example of a system with critical timing requirements- The “Flying Paster”

(next 2 slides from “Using Ptides and Synchronized Clocks to Design Distributed Systems with Deterministic System-wide Timing”,Derler.et.al., ISPCS 2013-Lemgo)

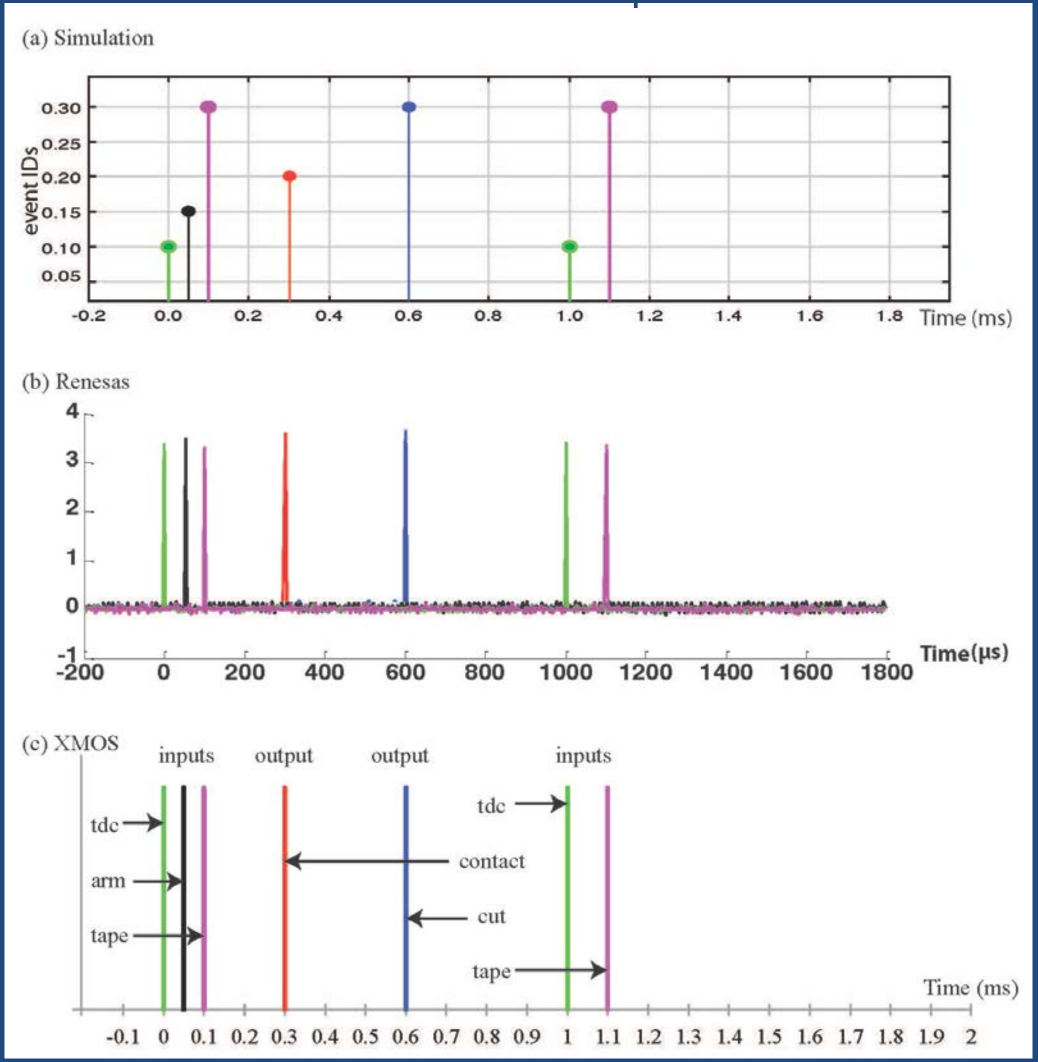


http://www.youtube.com/watch?v=wYRGiXMUzA4

This slide due to John Eidson

Embedded systems- especially distributed systems.

Designers should be able to design, simulate, and code generate for multiple targets with guaranteed timing!



This slide due to John Eidson

Comments on the Flying Paster example

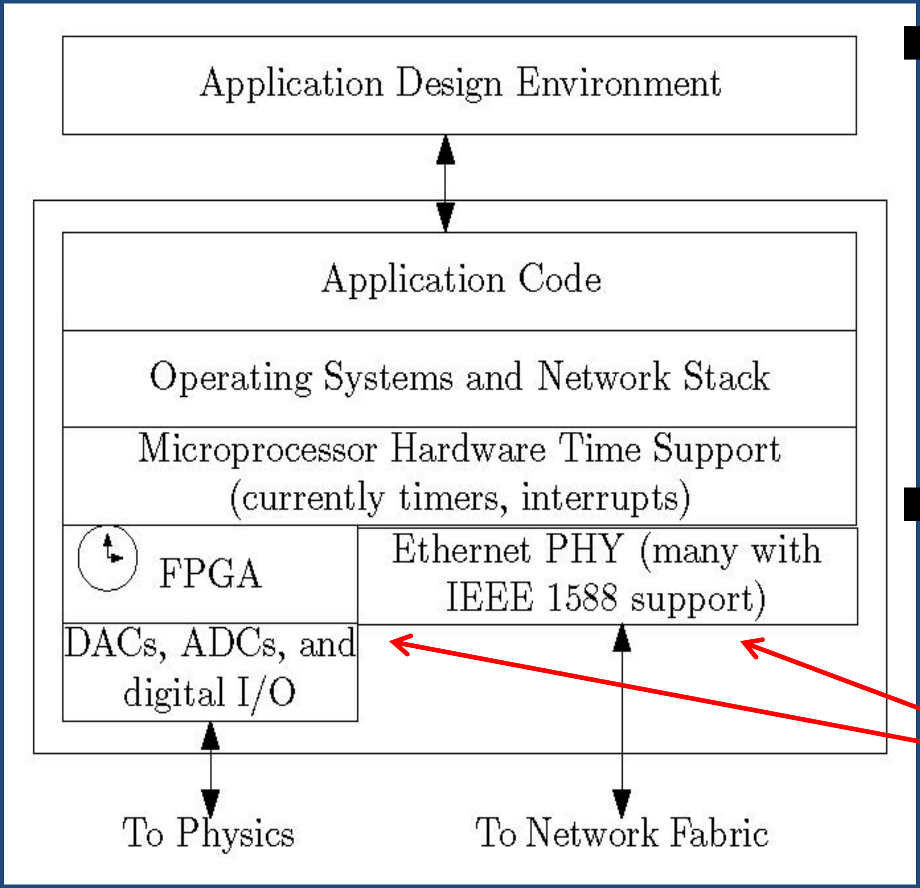
The Ptides implementation shown demonstrates:

- Physical time vs. Model time with correspondence enforced only at key points, e.g. sensors and actuators
- Same design compiled to two different platforms => identical timing to within clock resolution (8ns)

The "You Tube" video no doubt used a time-triggered architecture where a strict: sense, compute, actuate cycle is enforced with hardware supported sense and actuation timing

This slide due to John Eidson

Cyber Physical Systems Node and Environment, Currently

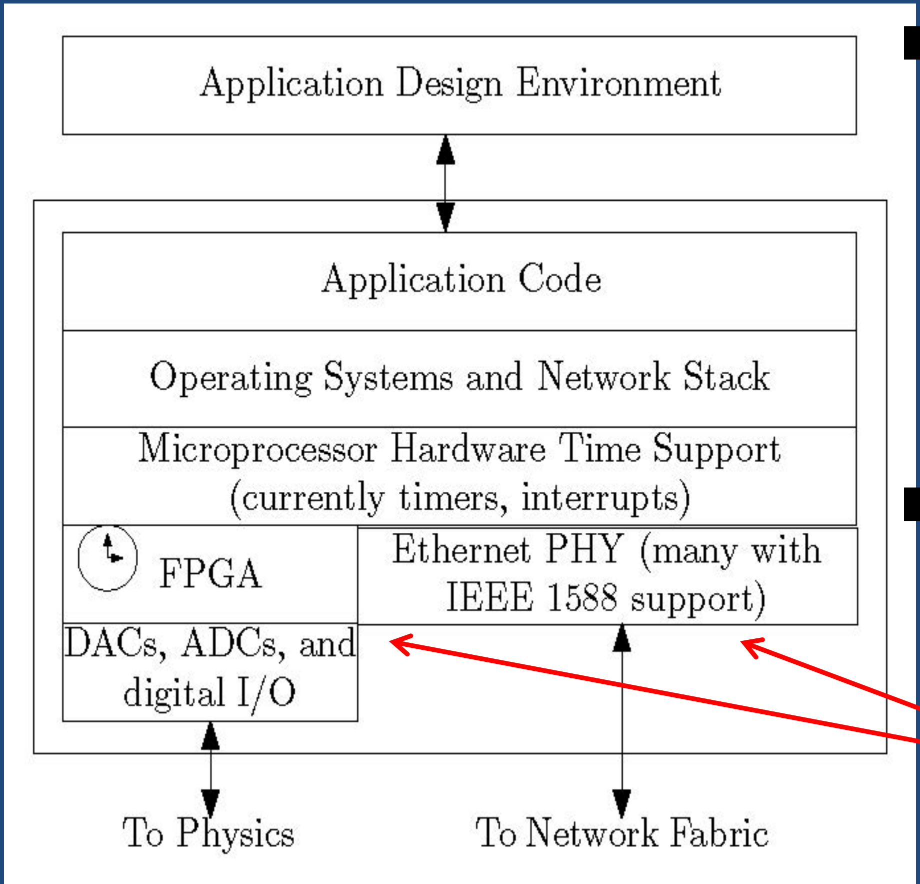


- No semantics of accurate time neither in design, nor languages
- Possibly bounded TIs
- Almost never stable (deterministic)
- Hence robust, correct by construction solutions cannot be done here!

- 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 ones by John Eidson

Cyber Physical Systems Node and Environment with Correct by Construction



- 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 ones by John Eidson

Outline: Time-Aware Systems in the Internet of Things

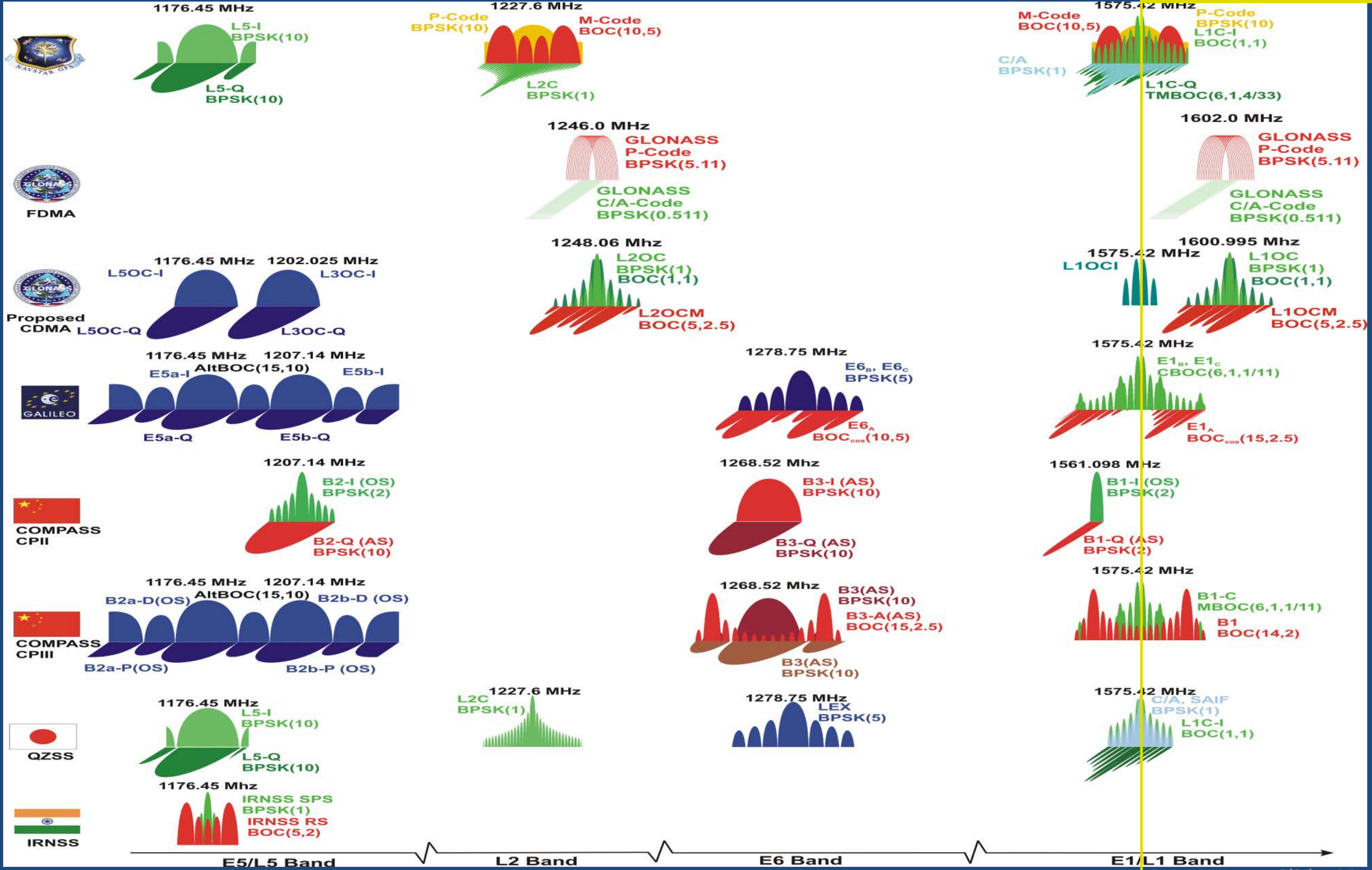
- Motivation
  - Anticipated large growth
  - Timing and computing don't mix!
  - What is Timing?
- Who is Developing Systems that Need Timing
  - Government science foundations
  - Industrial Internet
  - Cyber Physical Systems
- Time-Aware Systems – TAACCS group
  - Oscillators
  - Time transfer
  - Time in networks
  - Hardware/software support
  - Development Environments
  - Applications
- Timing Security
  - General issues
  - Jamming and Spoofing in GPS
- Conclusions

CPS Security and Resilience

- Since timing is both signal and data
  - Security of data is like cybersecurity
  - Security of timing signal is new
- Resilience generally means redundancy
- Time accuracy, UTC, generally comes from GNSS, which is vulnerable to interference
  - We focus on jamming and spoofing in GPS
  - Similar (yet Different!) vulnerabilities appear in networks

Spectra of GNSS's

Primary Commercial Signal

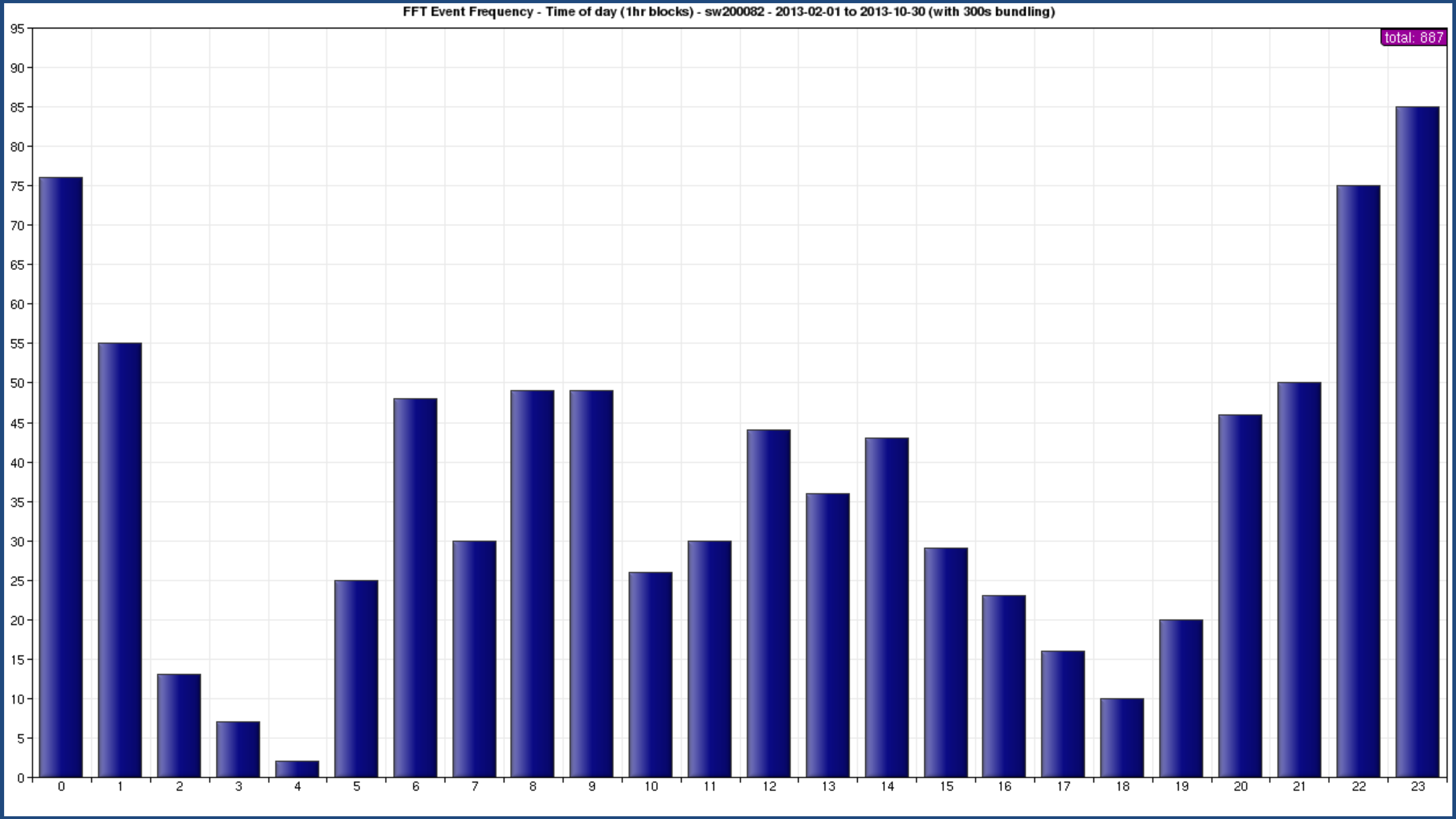


GNSS Vulnerability

- GNSS best feature and worst problem: it is extremely reliable
- Jamming Power Required at GPS Antenna
  - On order of a Picowatt (10^{-12} watt)
- Many Jammer Models Exist
  - Watt to MWatt Output – Worldwide Militaries
  - Lower Power (<100 watts); “Hams” Can Make

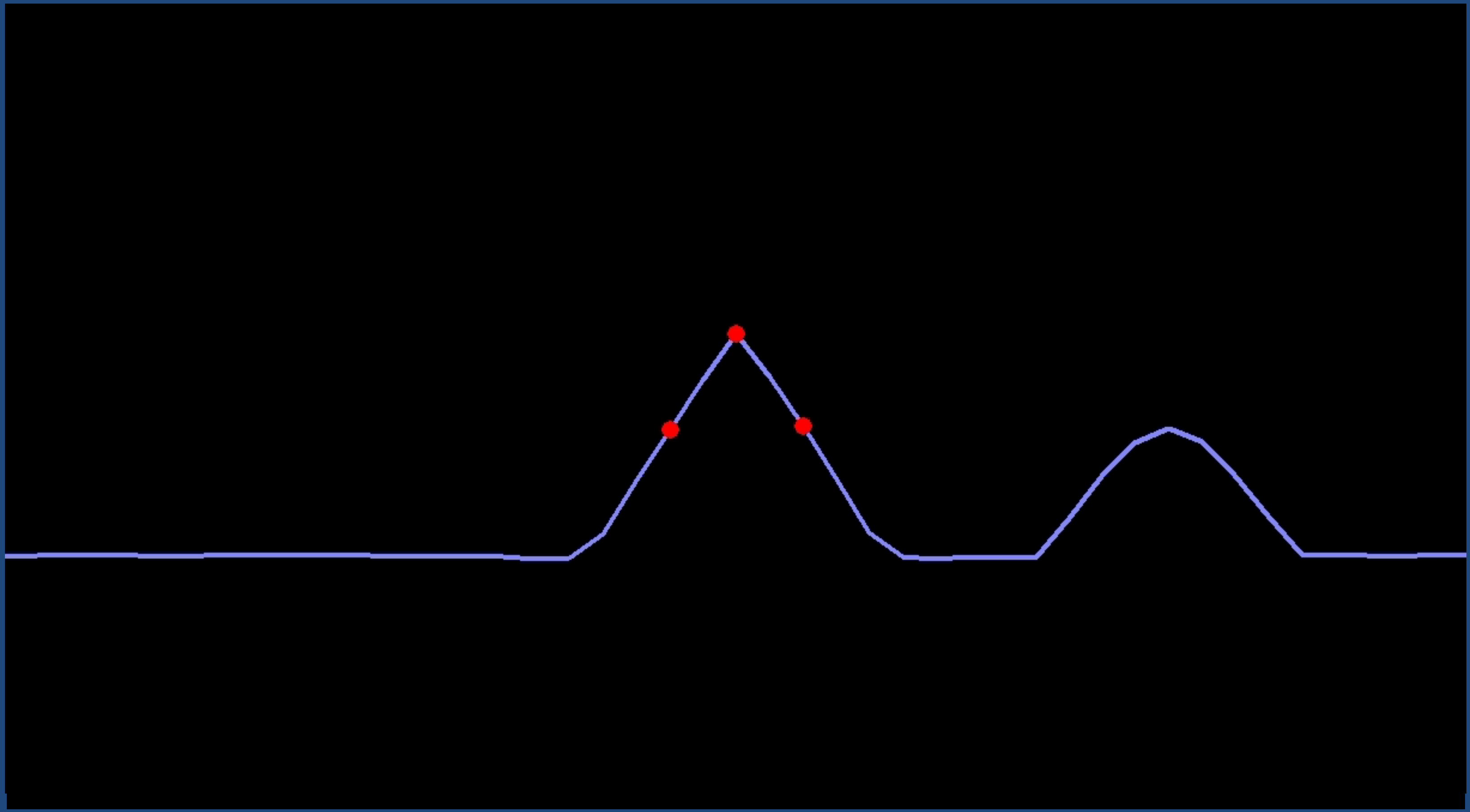


Jamming Events Each Hour, Feb – Oct 2013: London Financial District



Data and image courtesy of Charles Curry, Chronos Technology Ltd and the SENTINEL Research Project

GNSS Spoofer



Slide courtesy of Kyle D. Wesson, The University of Texas at Austin

Civil GPS Spoofing Threat Continuum*

Simplistic ***Intermediate*** ***Sophisticated***

Commercial signal simulator

Portable software radio

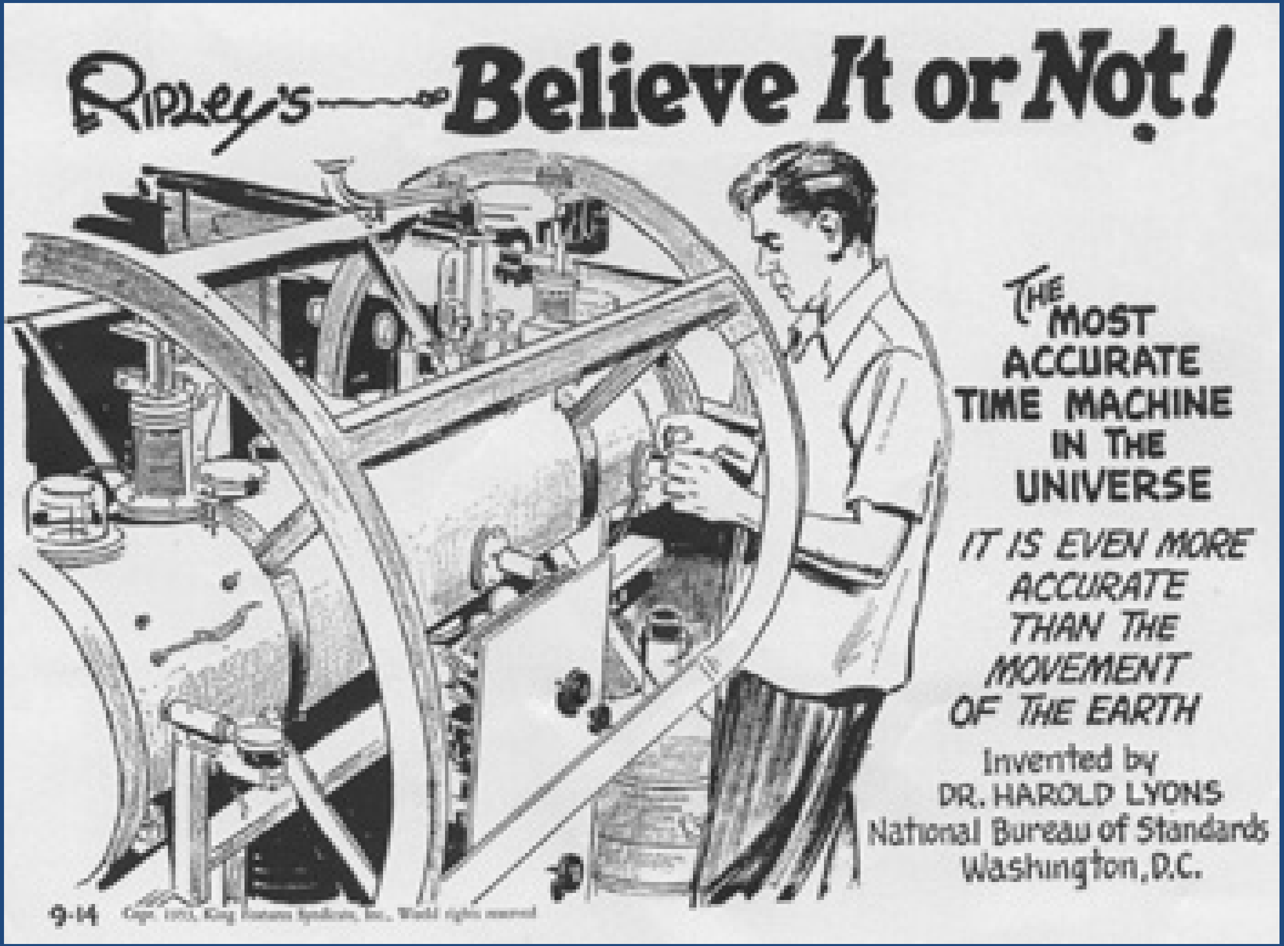
Coordinated attack by multiple phase-locked spoofers

* Courtesy of Coherent Navigation, Inc

Conclusions

- Huge growth expected in the IoT will require new paradigms for timing
- Many different groups are working on timing
- New timing paradigms
  - Time Awareness is key
  - Correct-by-design is necessary to support large growth and change
  - Designs for control in CPS
  - Timing Security requires securing both the signal and data

And that's all



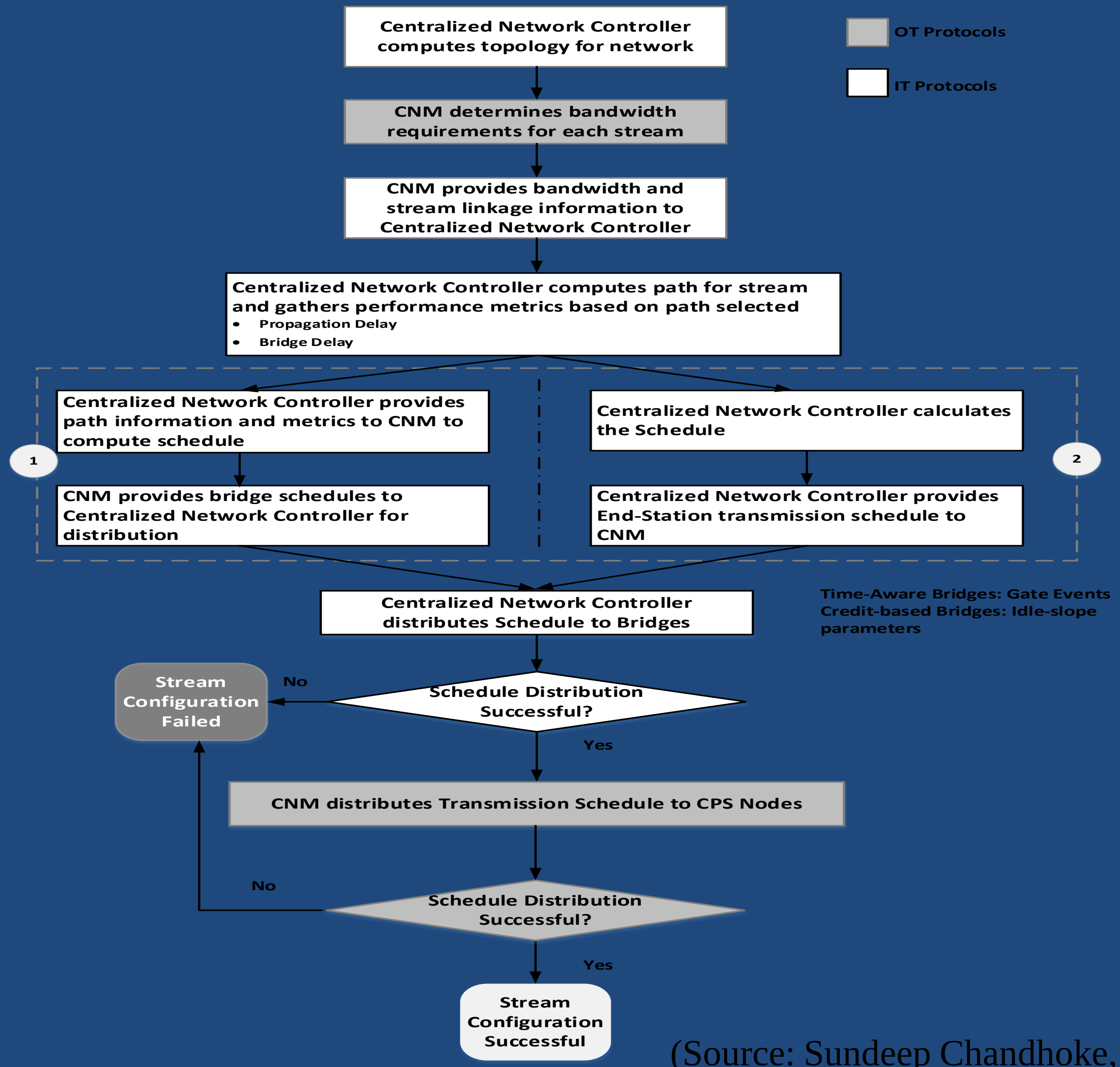
- Thank you for your interest

Extra Slides

Collaborative Research Needed:

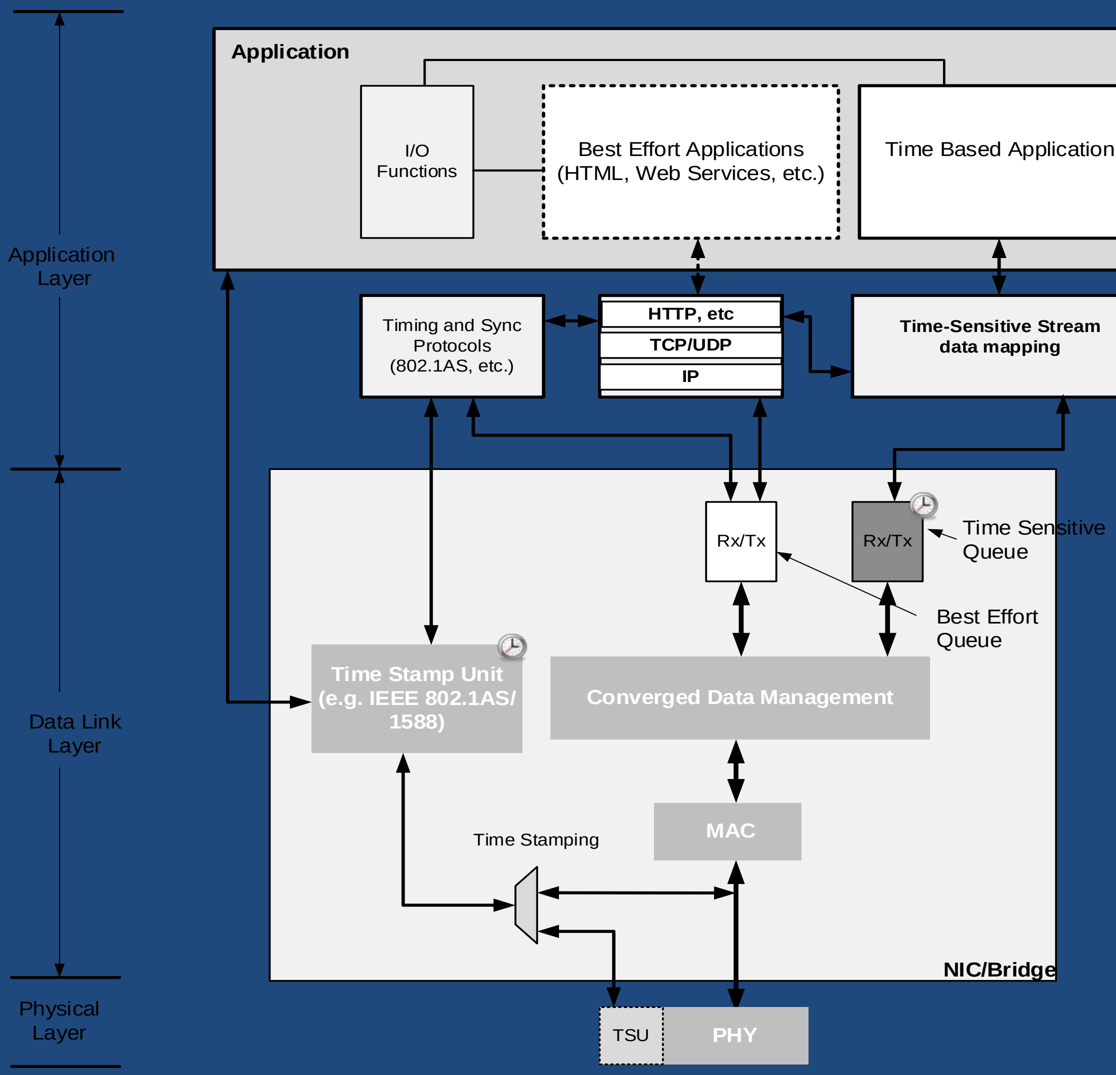
- Industry-Government-Academia
  - Broad range of goals
  - Different priorities and resources
- Communications Systems need Sync research
  - NIST group has expertise in time transfer issues
  - NIST WSTS has a basis for collaboration with industry

Time in networks: CPS Schedule Generation and Distribution

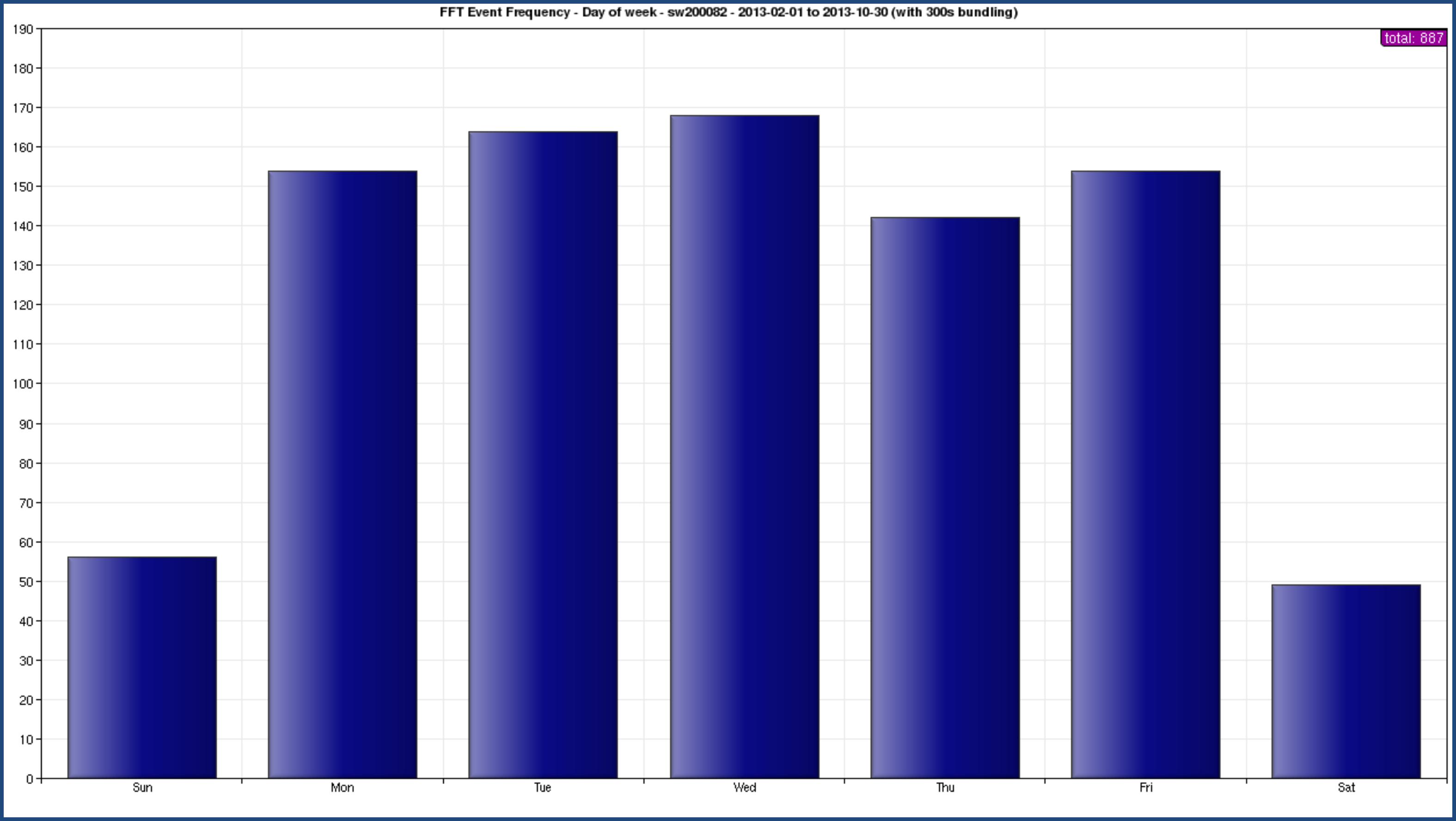


(Source: Sundeep Chandhoke, National Instruments)

Time in networks: Time-Aware CPS Device Model



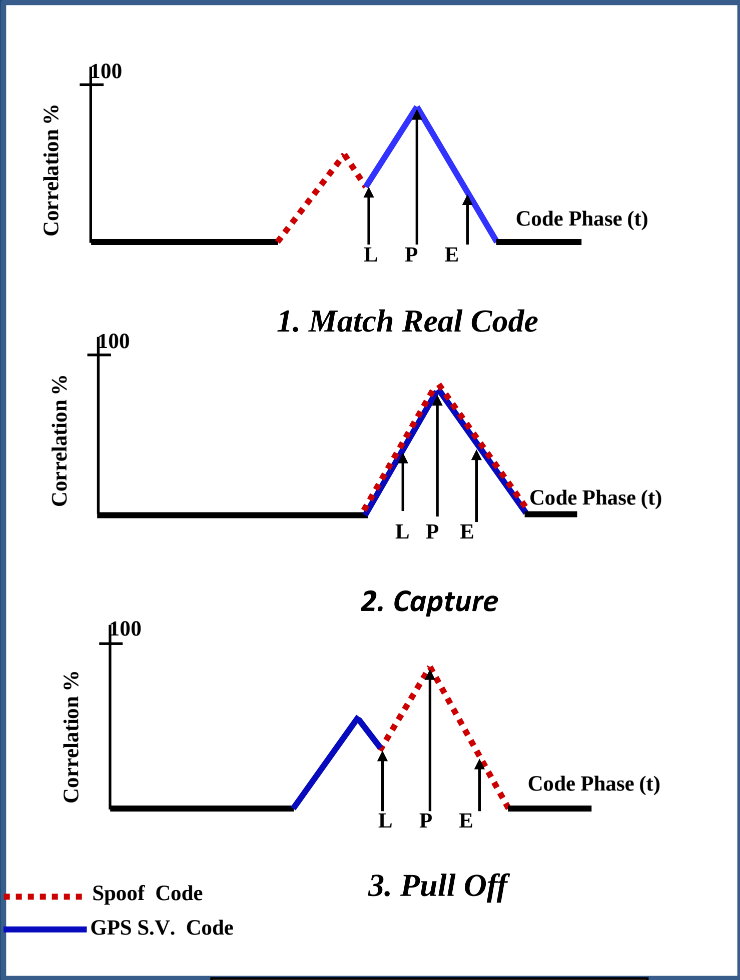
Jamming Events Day of Week, Feb – Oct 2013: London Financial District



Data and image courtesy of Charles Curry, Chronos Technology Ltd and the SENTINEL Research Project

Disruption Mechanisms - Spoofing/Meaconing

- Spoof – Counterfeit GNSS Signal
  - C/A Code Short and Well Known
  - Widely Available Signal Generators
- Meaconing – Delay & Rebroadcast
- Possible Effects
  - Long Range Jamming
  - Injection of Misleading PVT Information
- No "Off-the-Shelf" Mitigation



Successful Spoof

Conclusions

- GNSS provide all three types of sync: Time and Frequency and Phase
- GNSS accuracy meets PRTC and PRC specs
- GNSS are growing internationally
- GNSS are Vulnerable,

  best feature and worst problem:

  extremely reliable

Secure Timing

Source channel assurance	**Opportunities to verify that the timing information is coming from a legitimate source. 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.
Predictable failure	Known CPS failure modes that account for timing denial and detected timing spoofing.
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, a mechanism to switch to a redundant source is available.

Resilience in Timing: Multiple Timing Sources

	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	nanoseconds	No	No	Yes	Yes
NTP	milliseconds	No	No	Yes	Yes
Low Frequency Signals (eLORAN, WWVB, DCF77, …)	nanoseconds	No	No	Yes	Yes
***Galileo is not yet a fully operational GNSS constellation, but has indicated strong support for source channel and data assurance.**					

Principal attack vectors in an unsecured time network

Attack Type	Attack Characteristic	Impact	Example
Packet Manipulation	Modification (Man in the Middle (MitM))	False time	In-flight manipulation of time protocol packets
Replay Attack	Insertion / Modification (MitM or injector)	False time	Insertion of previously recorded time protocol packets
Spoofing	Insertion (MitM or injector)	False time	Impersonation of legitimate master or clock
Rogue Master (or Byzantine Master) Attack	Insertion (MitM or injector)	False time	Rogue master manipulates the master clock election process using malicious control packets, i.e. manipulates the best master clock algorithm
Interception and Removal	Interruption (MitM)	Reduced accuracy, depending on precision of local clock	Time control packets are selectively filtered by attacker
Packet Delay Manipulation	Modification (in widest sense) (MitM)	Reduced accuracy, depending on precision of local clock	Intermediate / transparent clock relays packets with non-deterministic delay
Flooding-based general DoS or Time Protocol DoS	Insertion (MitM or injector)	• Impairment of entire (low-bandwidth) network • Limited or no availability of target (service)	• Rogue node floods 802.15.4 network with packets • Rogue node overwhelms single victim with time protocol packets
Interruption-based general DoS or Time Protocol DoS	Interruption (MitM or possibly injector)	• Impairment of entire network communication • Limited or no availability of target	• Rogue node jams network • Rogue node jams selectively certain time protocol packets
Master Time Source Attack	• Interruption (MitM or injector) • Insertion (MitM or injector)	• Reduced accuracy • False time	• GPS jamming • GPS spoofing
Cryptographic. Performance Attack	Insertion (MitM or injector)	Limited or no availability of target	Rogue node submits packets to master that trigger execution of computational expensive cryptographic algorithm (like the validation of a digital certificate)