# On Some Confluences of Computing and Security in Theory and Practice


**Kalyan Perumalla**

*Distinguished R&D Staff Member, ORNL*
*Joint Professor, University of Tennessee Knoxville*

*Adjunct Professor, Georgia Institute of Technology*
*Adjunct Professor, University of Nebraska-Lincoln*

*Chair, ACM SIGSIM*


**Geek Brief | National Security Sciences Directorate |** May 12, 2021

# Selected References


- [**Zero-Energy Computing**] K. Perumalla, "Introduction to Reversible Computing (book)," Chapman & Hall/CRC, ISBN 978-1439873403, 2014 www.amazon.com/Introduction-Reversible-Computing-Chapman-Computational/dp/1439873402
- [**Zero-Energy Computing**] K. Perumalla, "Normalcy, Magic, Miracle and Error: Emergence along a Reversibility Spectrum," Insights journal, Durham University, 2019 https://www.osti.gov/pages/servlets/purl/1737650
- [**CYVET** and **Deep CYBERIA**] K. Perumalla, "Trust-but-Verify in Cyber-Physical Systems," ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, 2021
- [**CYVET**] K. Perumalla, J. Lopez, M. Alam, O. Kotevska, M. Hempel, H. Sharif, "A Novel Vetting Approach to Cybersecurity Verification in Energy Grid Systems," IEEE Kansas Power and Energy Conference (KPEC), 2020
- [**CYVET**] K. Ameri, M. Hempel, H. Sharif, J. Lopez, K. Perumalla, "Smart Semi-Supervised Accumulation of Large Repositories for Industrial Control Systems Device Information," 16th International Conference on Cyber Warfare and Security, 2021
- [**Deep CYBERIA**] K. Perumalla, S. Yoginath, J. Lopez, "Detecting Sensors and Inferring their Relations at Level-0 in Industrial Cyber-Physical Systems," IEEE International Symposium on Technologies for Homeland Security, 2019
- [**Naming Game**] K. Perumalla, "Concurrent conversation modeling and parallel simulation of the naming game in social networks," Winter Simulation Conference, 2017

# Bird's Eye View (One of Many Such Projections)

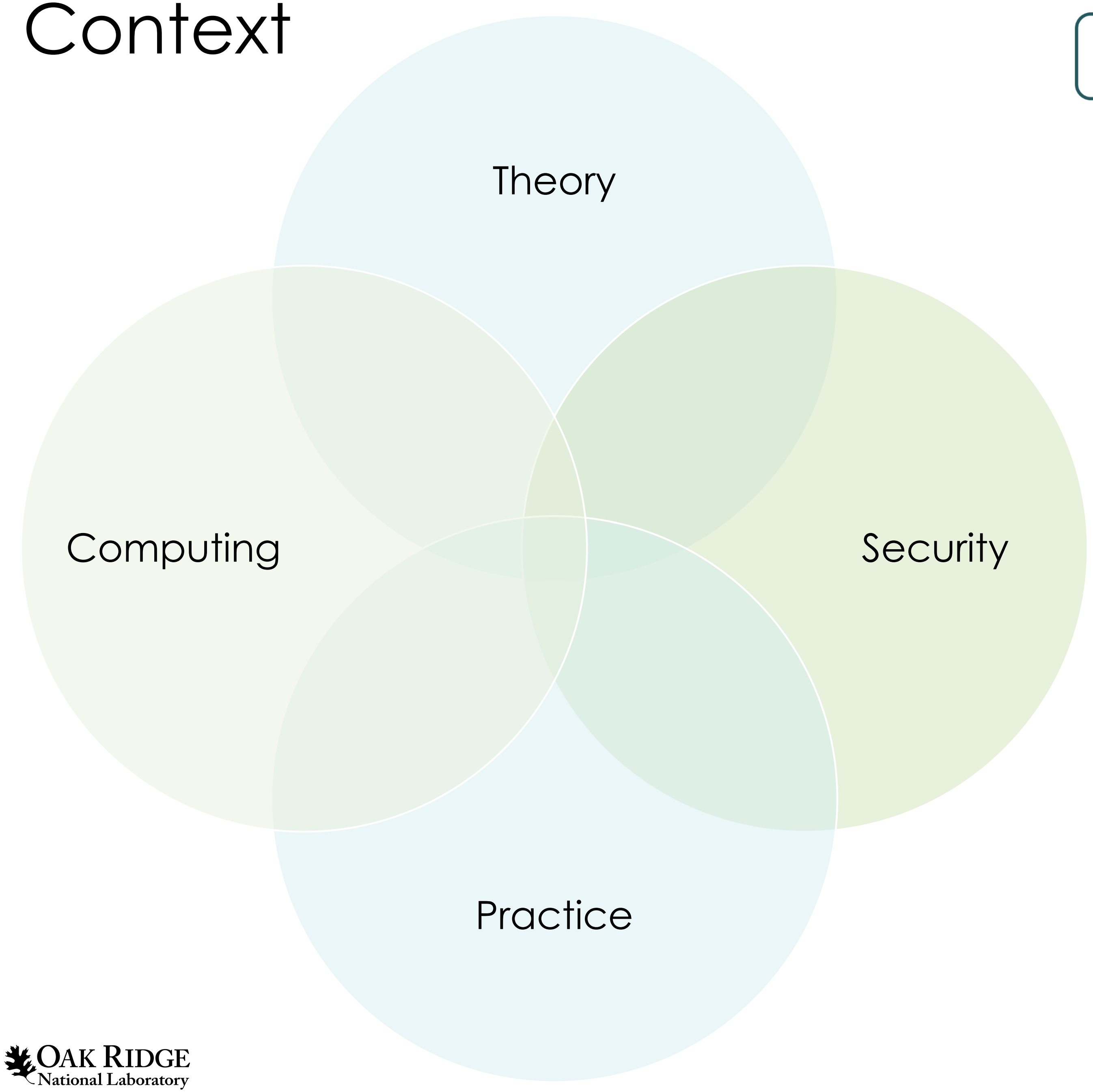
## Computing

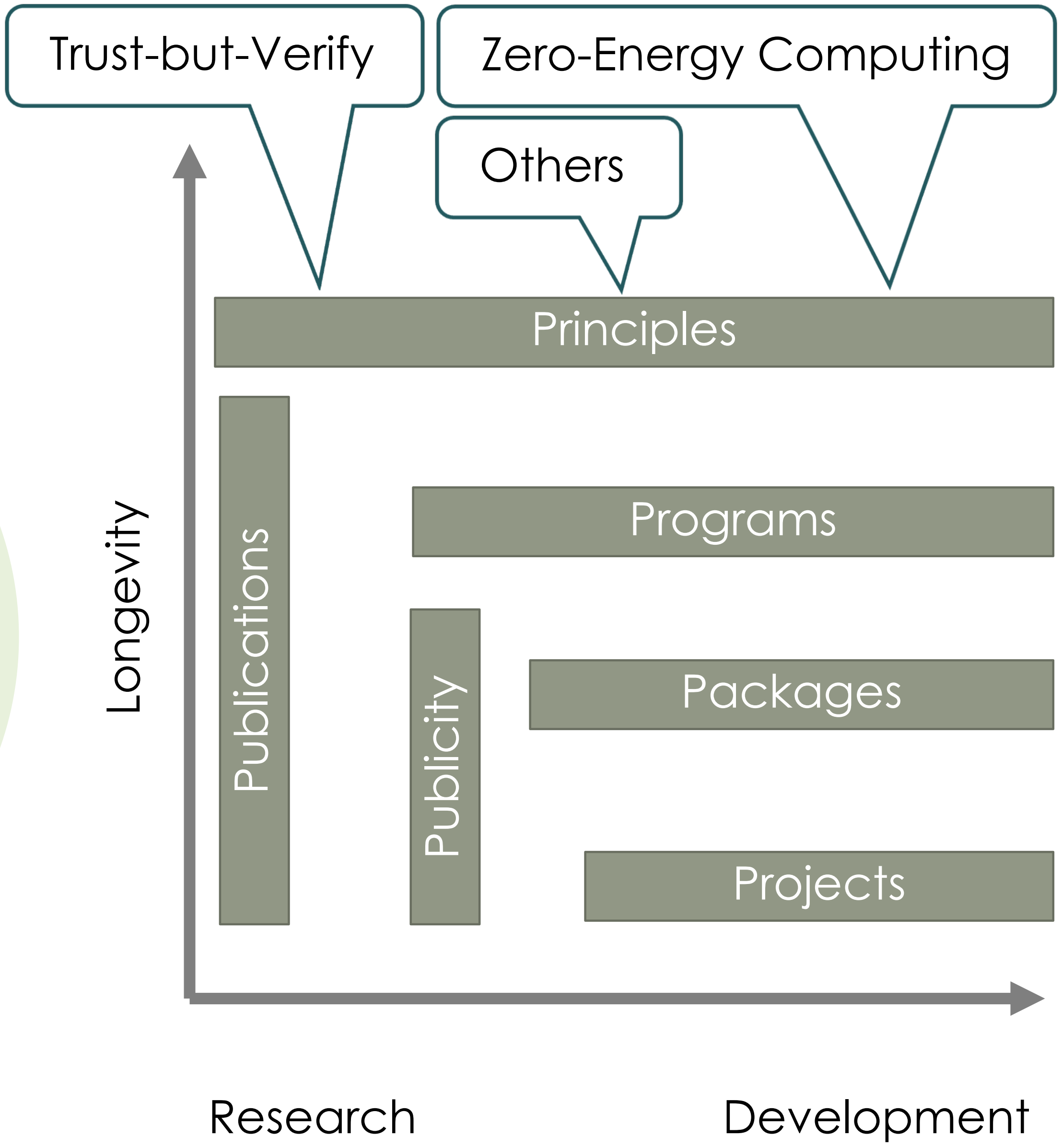
- HPC, GPU, FPGA, DSP, ASIC, My-Own-Chip
- M&S, AI/ML, DT, Commoditized SW blocks
- UNS, 5G, WiFi, 1G/10G, Fat pipe
- Cloud, On-prem, Hybrid, Edge, Instant Comp
  - Storage, SAAS, VMs, Containers
- HCI, HMI, Alternative/augmented Reality

## Security

- Social frenzy (catch-all)
- IT Ignorance
- Malleability of Truth
  - Authentic fakes,
- Human-Physical-Electronic Alloy
  - $4^{th}$-Dimensional Proximity
  - $4^{th}$-Dimensional Distance

# Context


Theory
Computing
Security
Practice

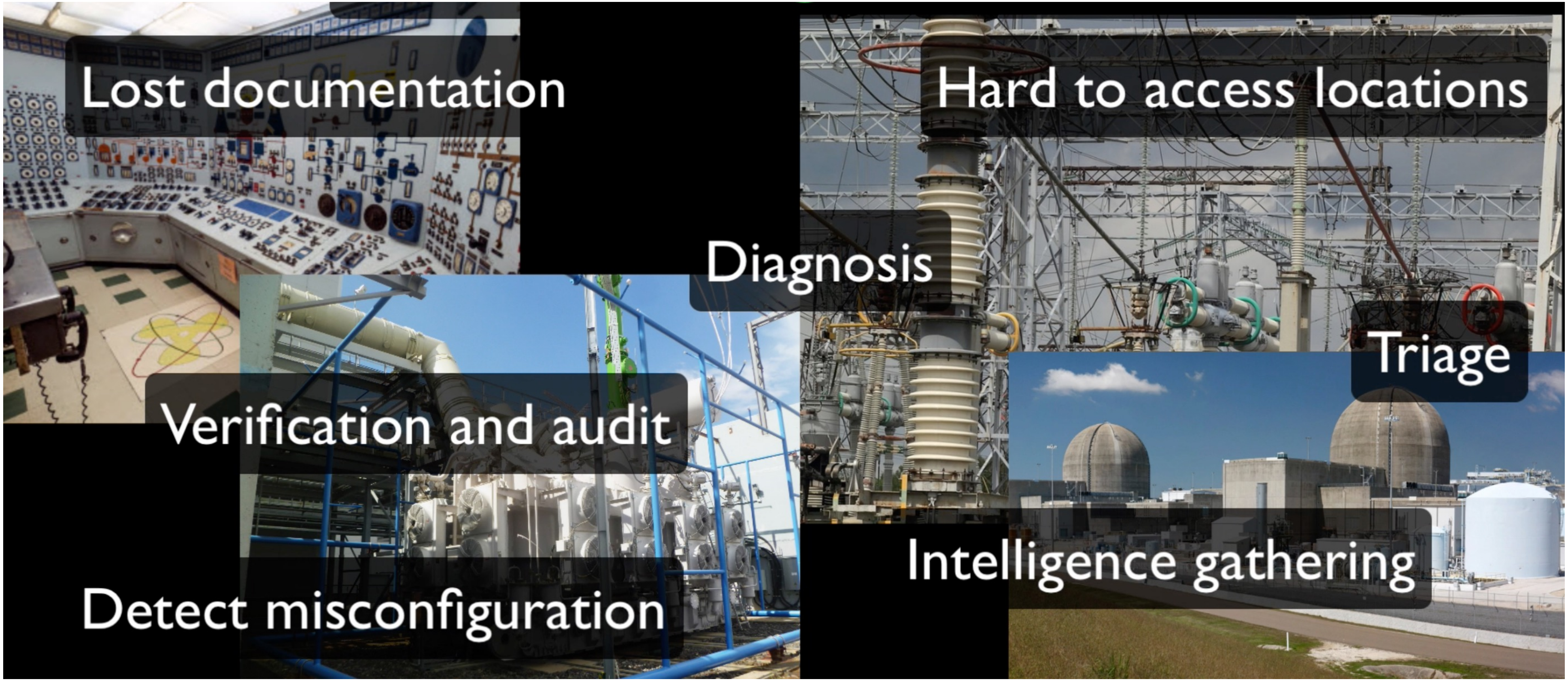

Trust-but-Verify
Zero-Energy Computing
Others
Principles
Publications
Programs
Publicity
Packages
Projects
Longevity
Research
Development

# Outline of This Geek-Brief

| 1. Trust-but-Verify | 2. Zero-Energy Computation | 3. Others |
| --- | --- | --- |
| • Practice in Active Projects<br>• Some Theory | • Asymptotically adiabatic / Reversible computing<br>• Applications<br>– Space<br>– Information Leakage | • Naming Game<br>– Networked Truths<br>• Grand challenge<br>– "Is anyone watching?"<br>– "When no one is watching…" |
| Small R<br>Big D | Big R<br>Small D | Big R<br>Big D |

# Trust-but-Verify

# “I **trust** you, but I need to **verify** what you have and how well it is”



# Trust-but-Verify: Trust by Default, Add Verification

| Ground Truth | Claims | Operation |
|---|---|---|
| • Verify ground truth | • Verify claims | • Verify operation |

This provides better *overall* value in energy and defense sectors

- Handles legacy well
- Lowers up-front costs
- Scales in complexity



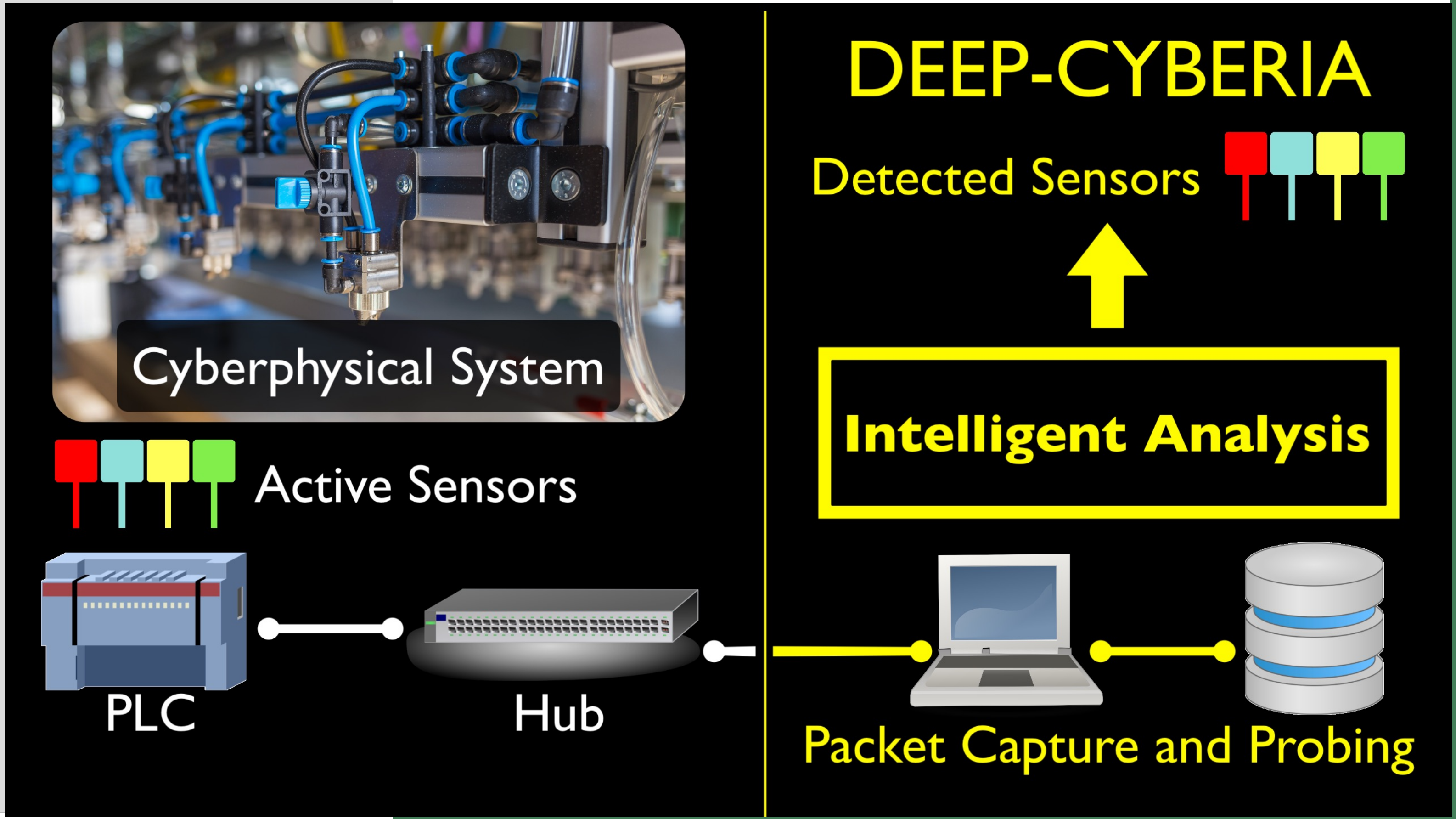
OAK RIDGE National Laboratory

# Question #1: What's out there?

## Deep CYBERIA

- Sensor Detection
- Sensor Identification
- Sensor Mapping
- Sensor Correlation

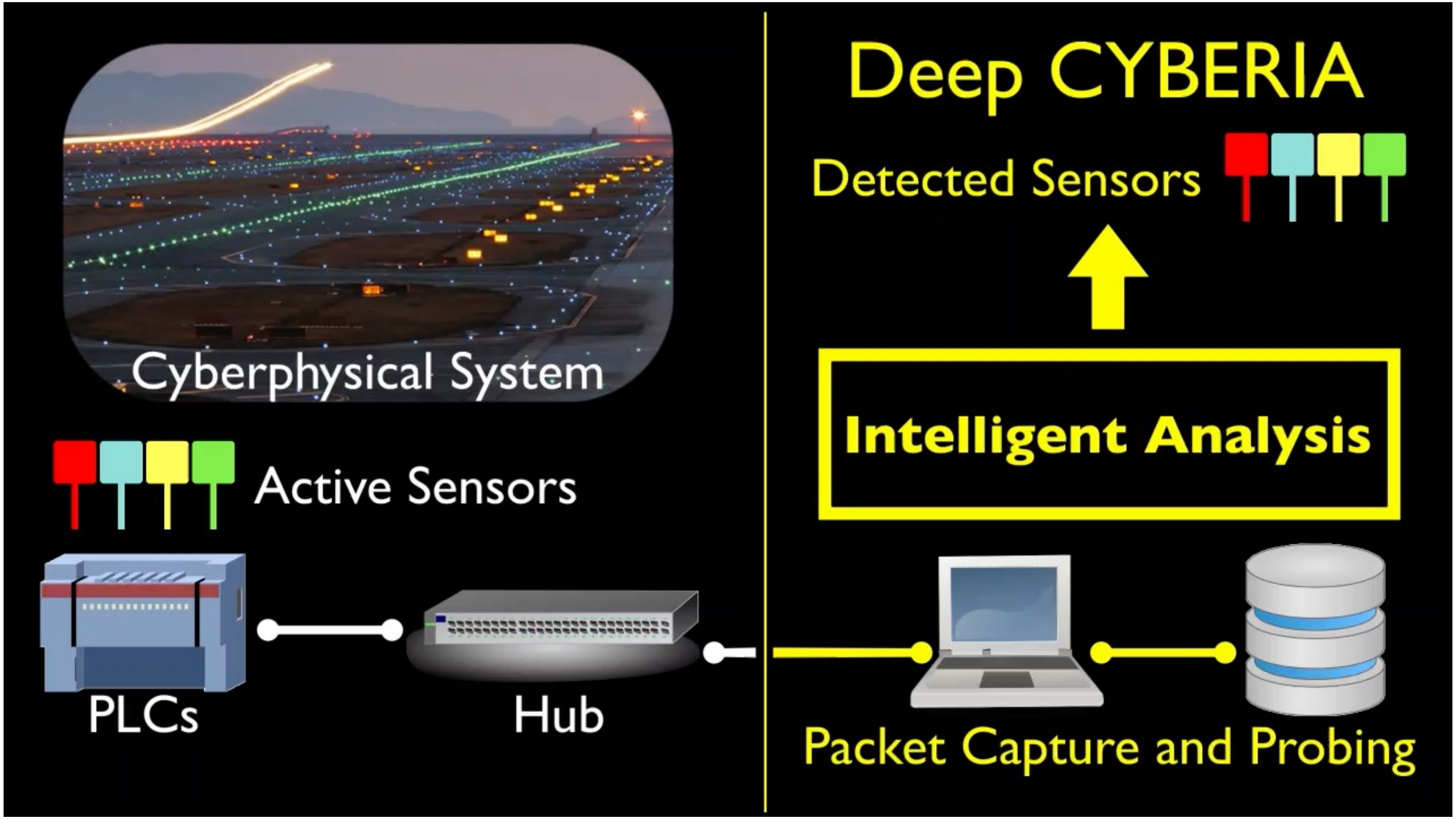
- Passive, Active, Hybrid




**With Dr. Juan Lopez and team**
Maksudul Alam, Joel Asiamah, Nicholas Guerra, Ryan Styles, Lance Wetzel

# Trust-but-Verify with Deep CYBERIA: What's out there?

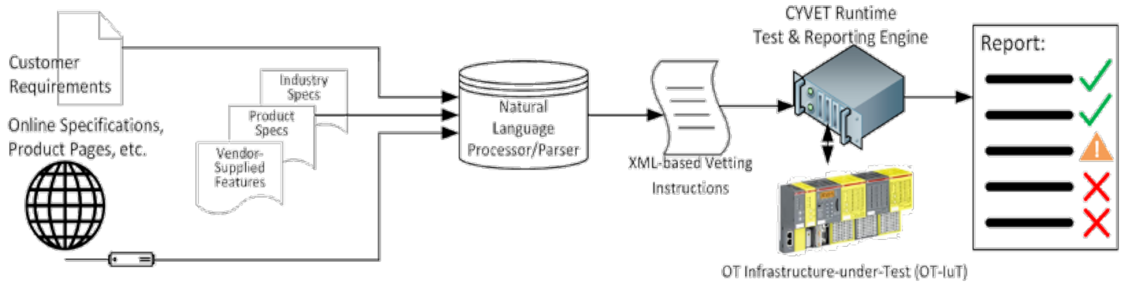
**Watch Video**



# Question #2: How robust is it?

**CYVET**

A Cyber-Physical Security Assurance Framework Based on a Semi-Supervised Vetting

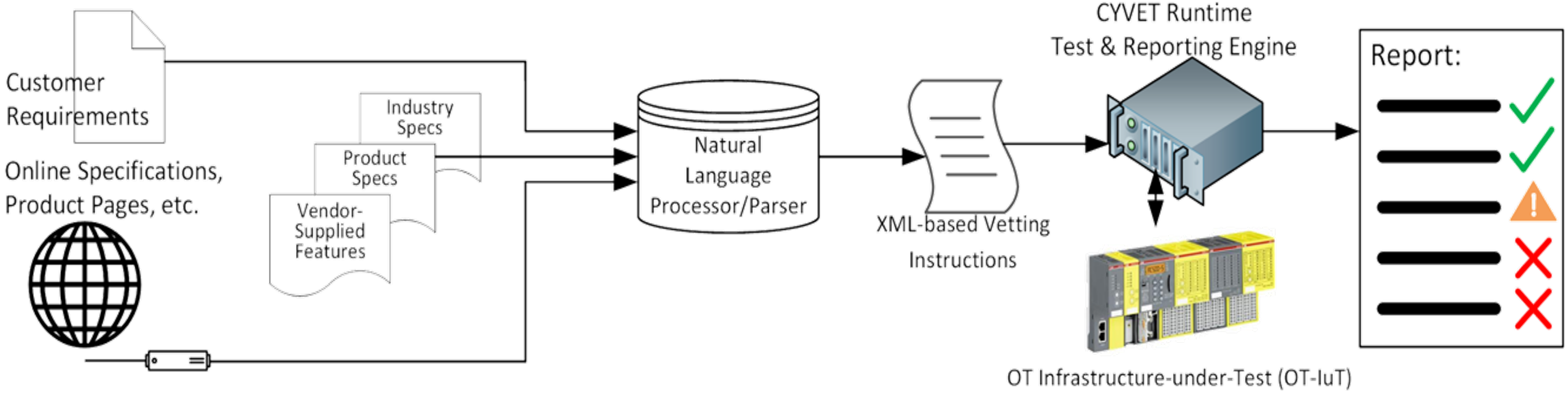



**With Dr. Juan Lopez and team across ORNL, UNL, industry partners**

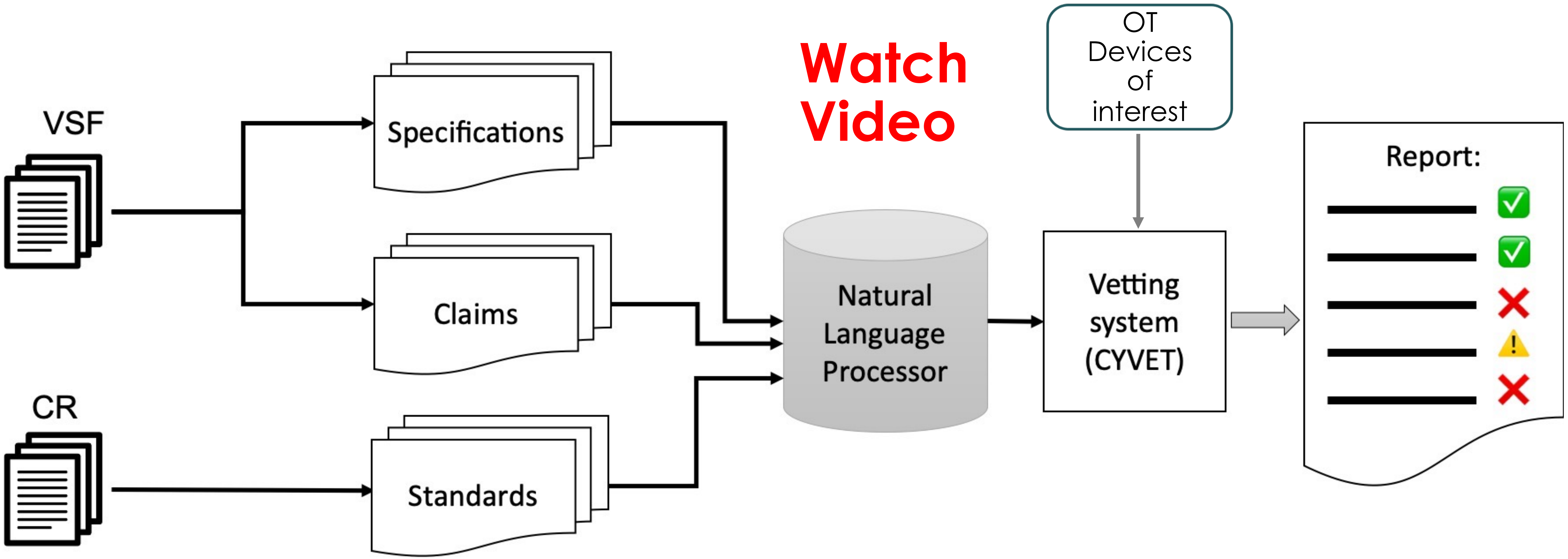
# Trust-but-Verify with **CYVET**

**Goal**: To develop verification capabilities to vet vendor-supplied features against cybersecurity requirements

- **Verification**: Synthesis and reconciliation of cybersecurity requirements (CR) and vendor supplied features (VSF)
- **Validation**: Generation, execution, and presentation of testing scripts of verified security features
- **Application**: Apply the developed technology capabilities for verification and validation at relevant end-user facilities in the energy sector.



# CYVET Verification: Putting it all together

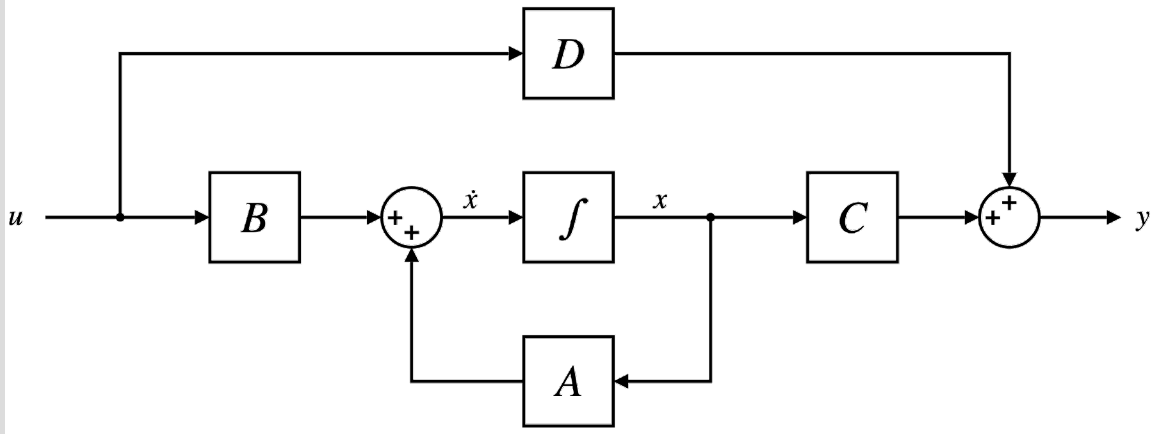



- K. Perumalla, J. Lopez, M. Alam, O. Kotevska, M. Hempel, and H. Sharif, “A Novel Vetting Approach to Cybersecurity Verification in Energy Grid Systems” IEEE Kansas Power and Energy Conference (KPEC)
- K. Ameri, M. Hempel, H. Sharif, J. Lopez, and K. Perumalla, “Smart Semi-Supervised Accumulation of Large Repositories for ICS Device Information” Intl Conference on Cyber Warfare and Security (ICCWS)

# Question #3: How well is it doing?

**DT**

Digital Twins and Triplets for Dynamic Monitoring for Trust-but-Verify



# Trust-but-Verify Dynamically: Online Digital Twin/Triplet

**Input**
U

Controls

CPS

**State**
x

**Process Noise**
w

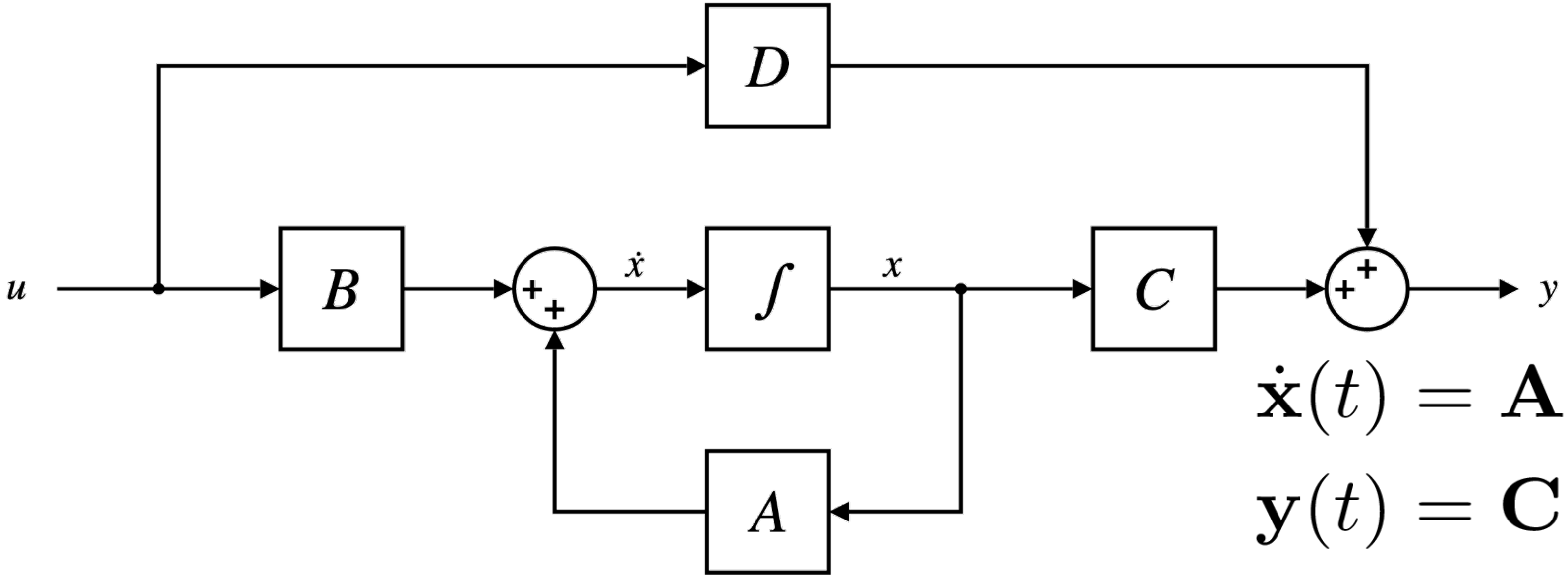
**Measurement Noise**
v

**Observable**
y

Sensors

**Uses**

- **Twin**: Track function with data
- **Twin**: Determine function from unknown design
- **Triplet**: Detect deviations from known design




Linear state-space representation

$$\dot{\mathbf{x}}(t) = \mathbf{A}(t)\mathbf{x}(t) + \mathbf{B}(t)\mathbf{u}(t) + \mathbf{w}(t)$$

$$\mathbf{y}(t) = \mathbf{C}(t)\mathbf{x}(t) + \mathbf{D}(t)\mathbf{u}(t) + \mathbf{v}(t)$$

# Zero-Energy Computing

- Asymptotically adiabatic computing
- Reversible Computing
- …Quantum Computing…

# My Book for Reference

www.amazon.com/Introduction-Reversible-Computing-

## Product Details

**Series:** Chapman & Hall/CRC Computational

**Hardcover:** 325 pages

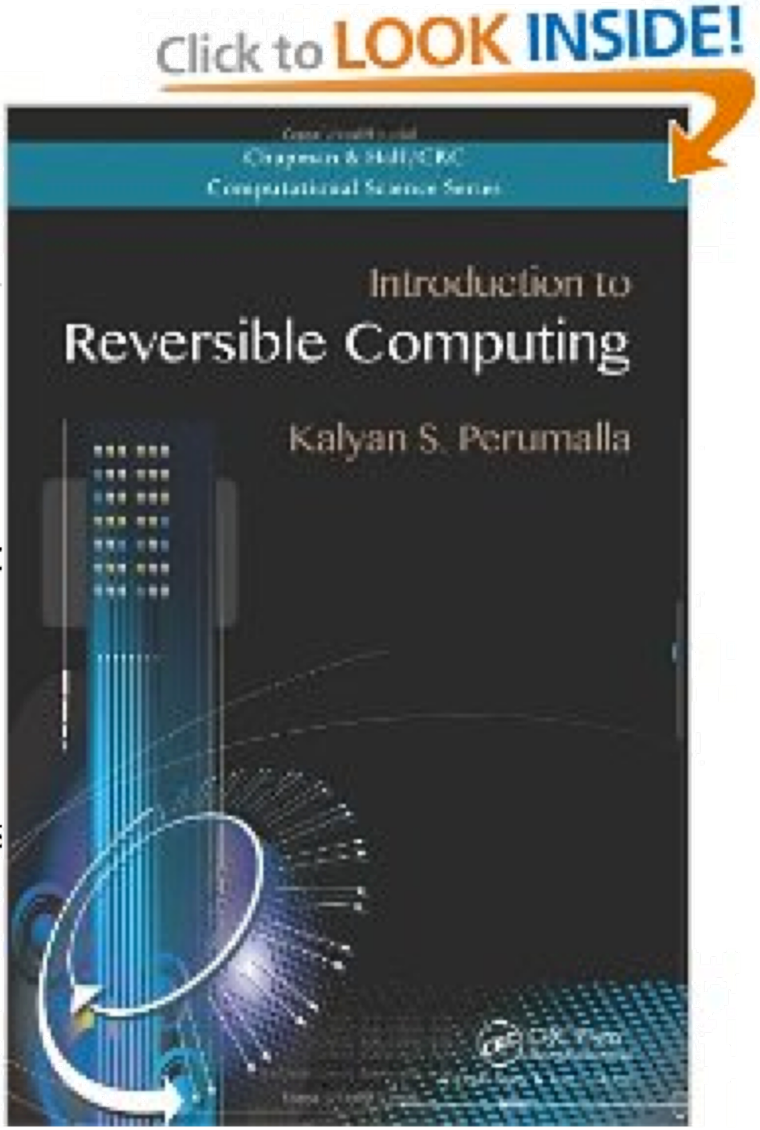
**Publisher:** Chapman and Hall/CRC (Septemb

**Language:** English

**ISBN-10:** 1439873402

**ISBN-13:** 978-1439873403

**Product Dimensions:** 9.3 x 6.2 x 0.9 inches




Introduction to
(Chapman & H
Science) [Hard

Kalyan S. Perumalla

Be the first to review th

List Price: ~~$89.95~~

Price: $83.92

You Save: $6.03 (7%

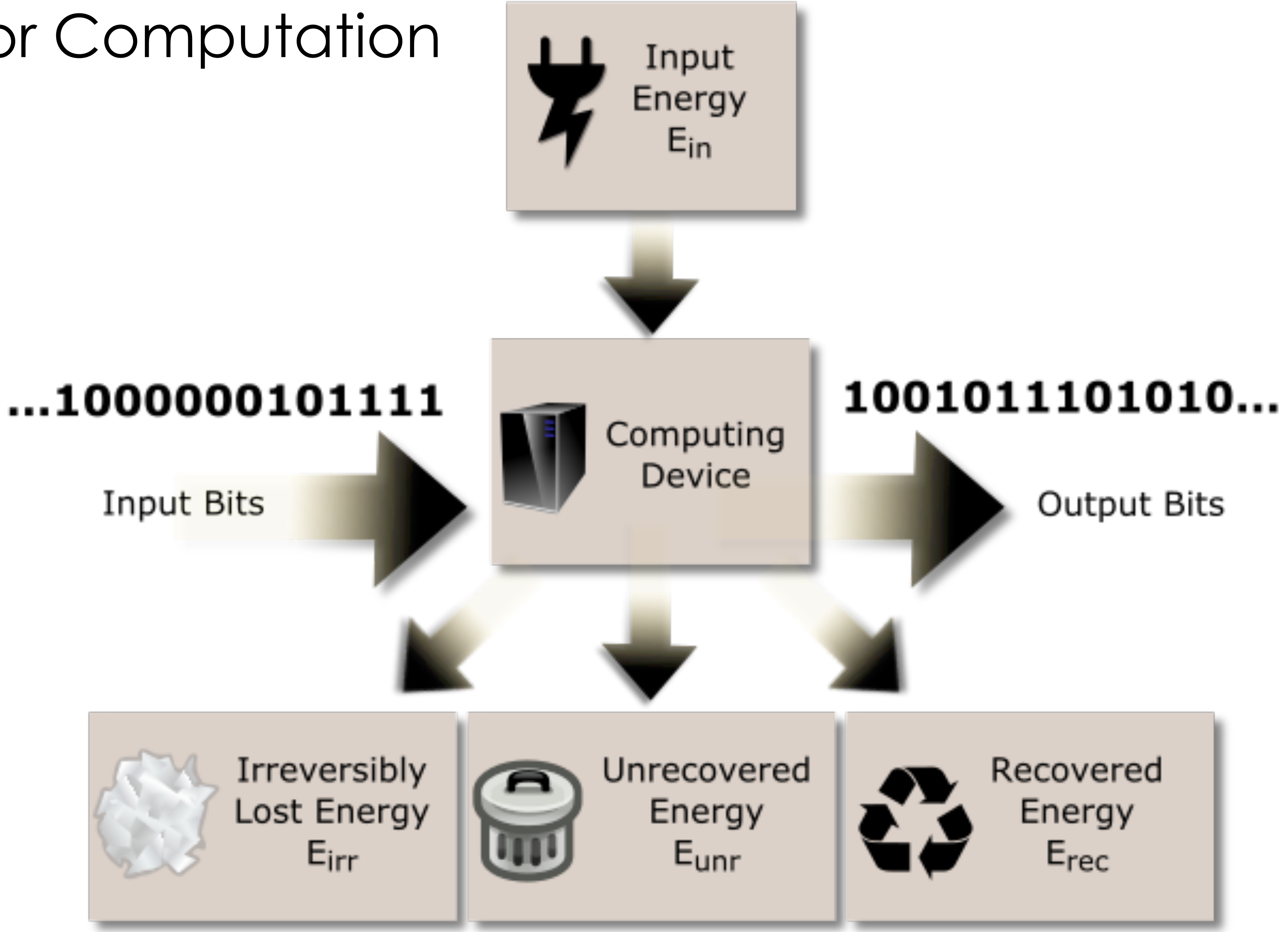
**Only 4 left in s**

Ships from and sold

**Want it Friday, July**
choose **One-Day Sh**

37 new from $78.97

# Energy for Computation






Geek Brief: Kalyan Perumalla, ORNL

# Fundamental Questions about Energy for Computing

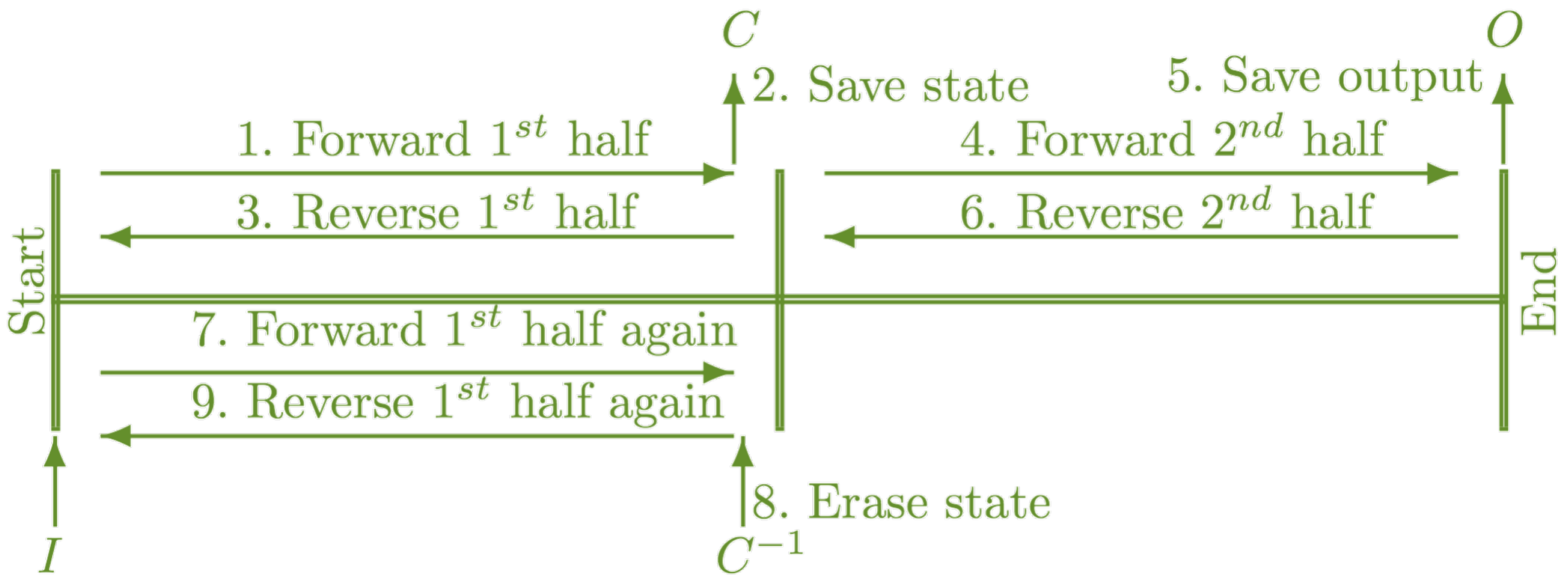
## Initial Question

- What is the minimum energy needed/dissipated to "compute?"
- **First thought**
  Every ***bit-operation*** dissipates a unit of energy ($kT$ ln2)
- **Next thought**
  Not ***bit-operation***, but ***bit-erasure*** dissipates a unit of energy ($kT$ ln2).

## Final Question

- What is the minimum number of **bit-erasures** to "compute?"
- **Initial guess**
  A non-zero, computation-specific number
- **Surprising solution**
  ***Zero bit-erasures***!
  - Bennett's "compute-copy-uncompute" algorithm avoids *all* bit erasures for *any* arbitrary (Turing) program

# Reversible Simulation of Irreversible Turing Machines




1. Forward execution from initial state with input $I$ to midpoint
2. Saving the half-way state $C$
3. Reverse execution from midpoint back to initial state
4. Forward execution from midpoint to final state with output $O$
5. Saving the final output $O$
6. Reverse execution from final state back to midpoint
7. Forward re-execution from initial state with input $I$ to midpoint
8. Reversibly erasing $C$ with $C^{-1}$
9. Reverse execution from midpoint back to initial state

$$Time(T) = 6Time(\tfrac{T}{2})$$

$$Time(1) = 1,$$

$$Time(T) = 6^{\log_2 T} = T^{\log_2 6} = T^{1+\log_2 3} \approx T^{2.59}$$

$$Space(T) \leq S\log_2 T \leq S\log_2 2^S = S^2$$

# Most Important Implications

## Zero-Energy Computing

- It is theoretically possible to compute with **zero energy**!
- However, execution must be asymptotically slowed down
  - Second Law of Thermodynamics at play
- Yet, ***all*** energy can be theoretically recovered

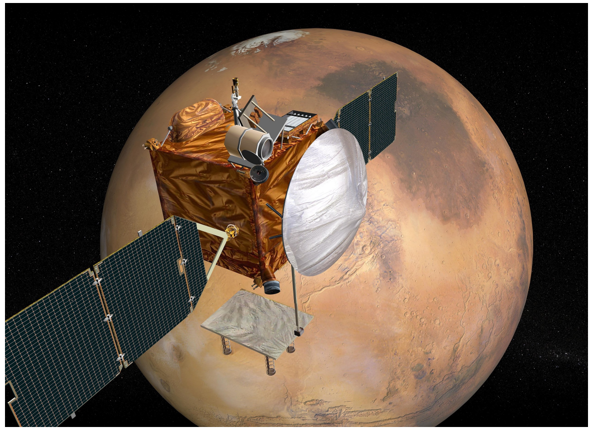
## But Who Cares?

- This is important
  - When energy is extremely scarce and premium…
  - When energy dissipation becomes information leakage…

# What are some applications for zero-energy computing?

## Space

- Energy sources are extremely low
  - Reduce, reuse, recycle energy
- Time durations are extremely long
  - Immense leisure means GHz not needed
  - Asymptotically slow processing permissible

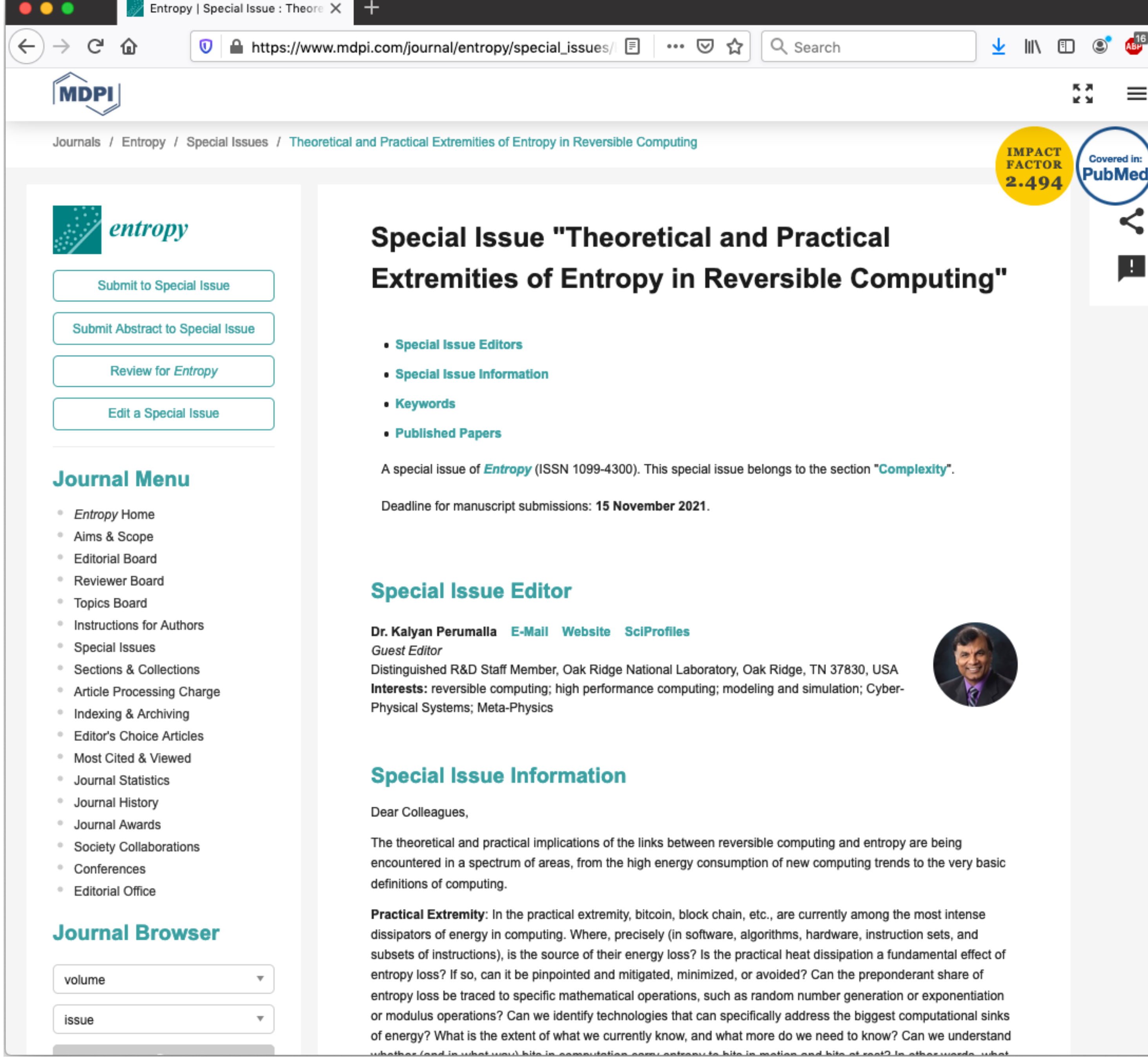


## Security

- At low energy computing, any energy dissipation is information leakage
- Only two choices:
  1. Zero-energy computing leaks no computation
  2. Wasted high-energy can mask computation

# Open Special Issue of Journal *Entropy*

- Practical Extremity
  - Bitcoin guzzles energy
  - HPC consumes MWs
- Theoretical Extremity
  - Definition of computing
  - Limits of human cognition
  - Fundamental material science
  - Quantum computing





OAK RIDGE National Laboratory
https://www.mdpi.com/journal/entropy/special_issues/Reversible_Computing

# Naming Game

- Networked Truths
- Influencing Truth Propagation
  - Speed
  - Dominance

# Successful Conversation: Common Word

Object
(Painting)

- **Tahiti**

- **Tahiti**

**Tahiti**

Kalyan

Juan

# Failed Conversation: No Common Word

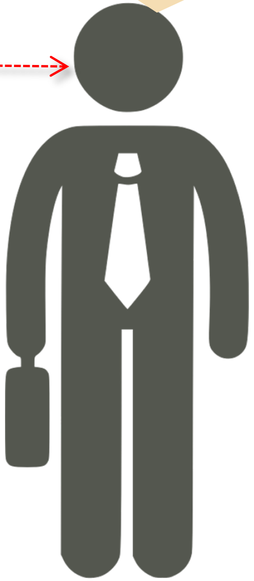
Object
(Painting)

- Paul Gauguin
- **$300 Million**
- Tahiti
- Tiare

Kalyan

**$300 Million**

- Wow
- Hmm
- **$300 Million**

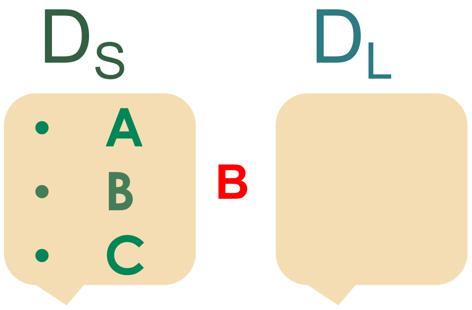


Shaun



Oak Ridge National Laboratory

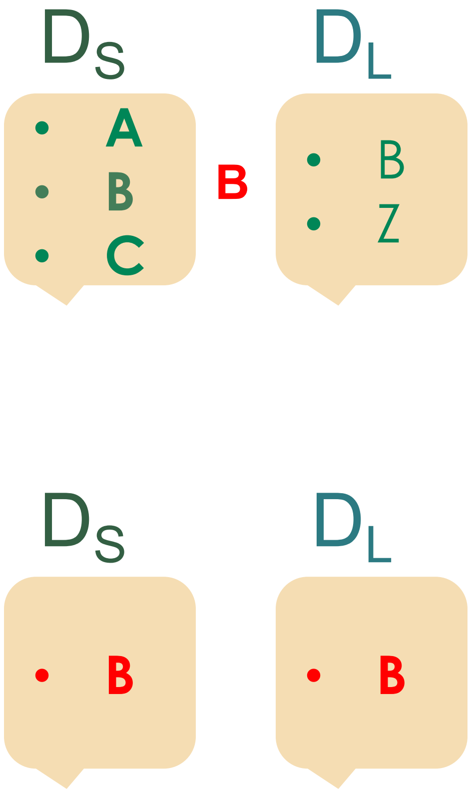
# The Naming Game: Illustration of Each "Conversation"



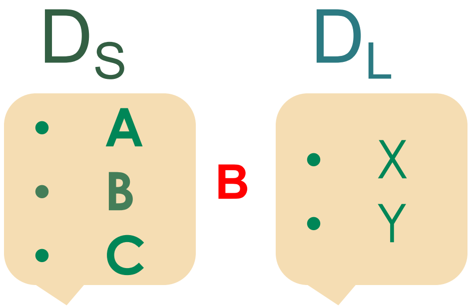

1. Speaker S selects listener L
2. S speaks a word W from own dictionary $D_S$
3. L consults own dictionary $D_L$

# The Naming Game: Illustration of Each “Conversation”

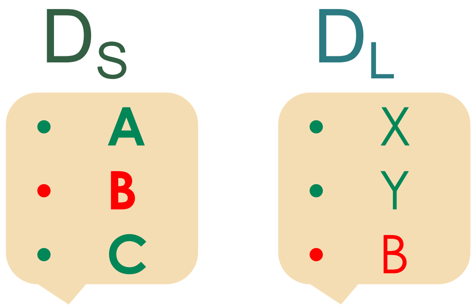
1. Speaker S selects listener L
2. S speaks a word W from own dictionary $D_S$
3. L consults own dictionary $D_L$
4. If W is in $D_L$ **[Success]**
   $D_S$ and $D_L$ are emptied,
   W is added to both



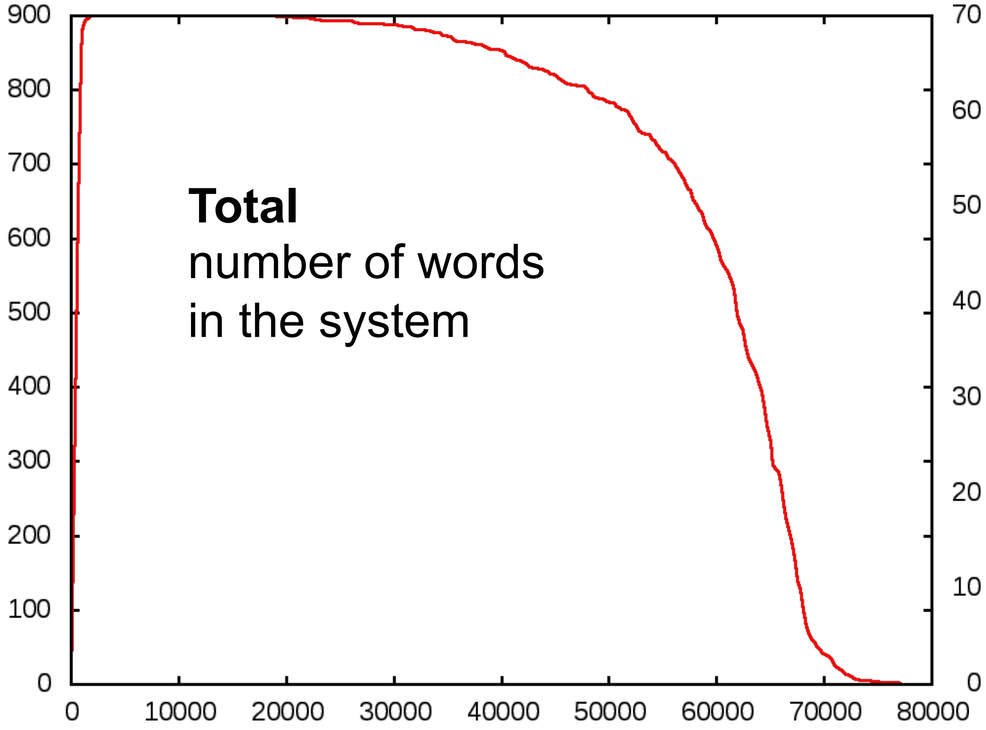
# The Naming Game: Illustration of Each "Conversation"

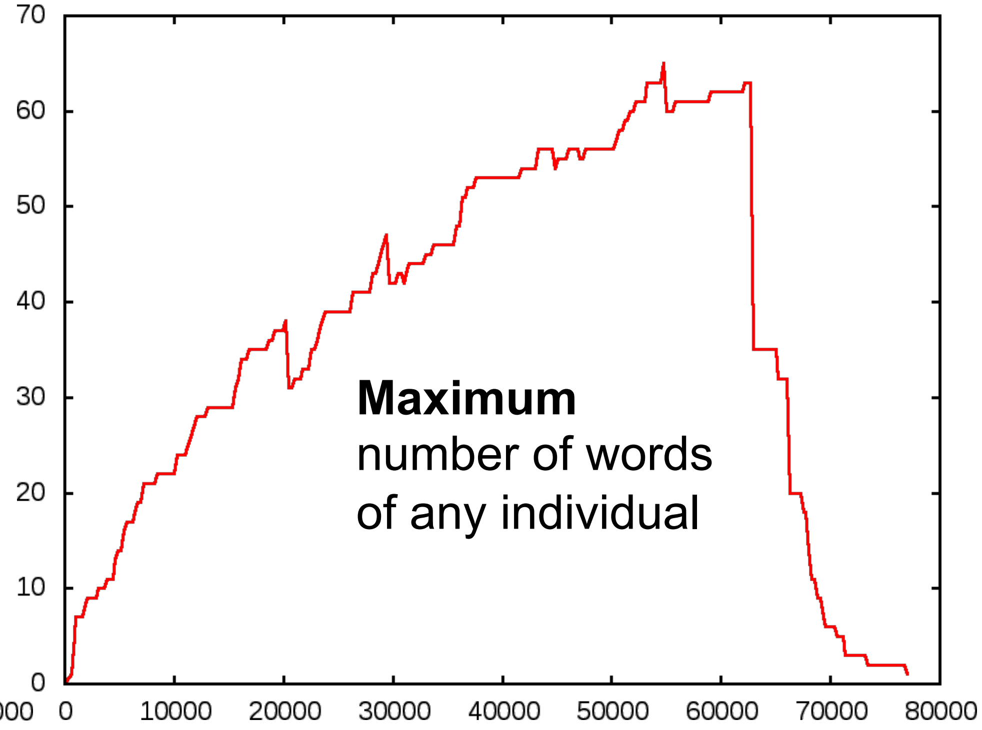



1. Speaker S selects listener L
2. S speaks a word W from own dictionary $D_S$
3. L consults own dictionary $D_L$
4. If W is in $D_L$ [**Success**]
   $D_S$ and $D_L$ are emptied,
   W is added to both
5. Else, if there is no W in $D_L$ [**Failure**]
   W is added to $D_L$

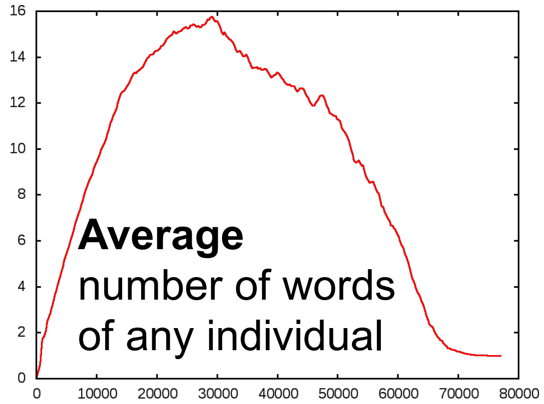


# Classical Evolution of Individual Dictionaries




Number of conversations →



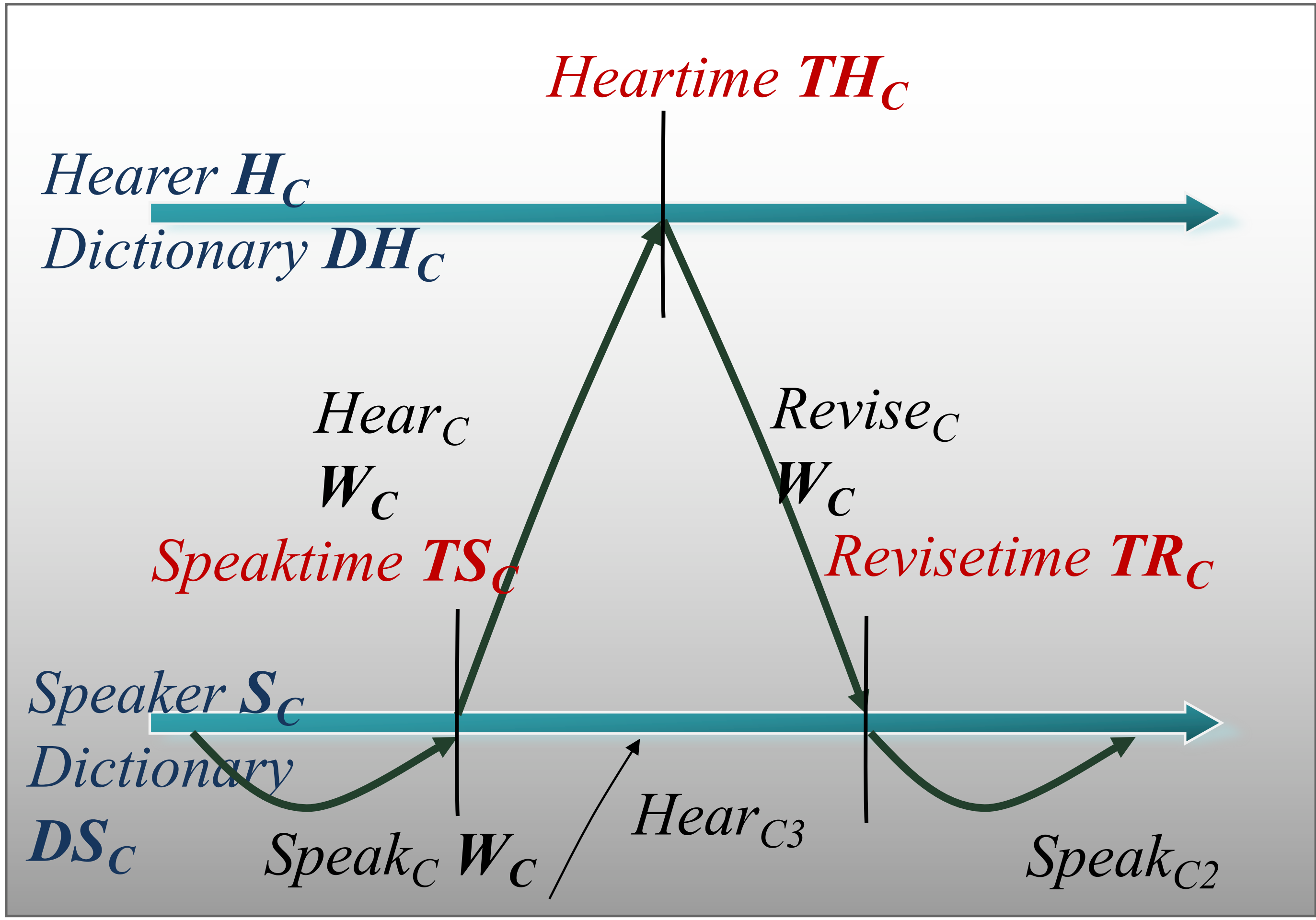

System size **N = 1024**
(number of individuals)

Network = Clique

# Relaxation: Classical to Concurrent Conversations
## Taking the Implicit Components Apart

1. Speaker selection
2. Hearer selection
3. Transmission of word
4. Receipt of word
5. Revision of hearer's dictionary
6. Conversation "time" period
7. Revision of speaker's dictionary
8. Inter-conversation "time" interval

- Split speaking & hearing halves
- Add new semantics
  - Speaker can be hearer **while speaking**
  - Classical = Conversation cannot be interrupted
  - New = Conversations potentially overlap






OAK RIDGE National Laboratory

# Putting it all together…

$$Hear_C : DH_C \leftarrow DH_C \bigcup \{W_C\},\ or\ \{W_C\}$$

$$Revise_C : DS_C \leftarrow DS_C,\ or\ \{W_C\}$$

$$V = Vocabulary = Set\ of\ potential\ words = \{W\}$$

$$DI_C = \{W_i\} \subseteq V = Dictionary\ of\ person\ I\ in\ conversation\ C$$

$$C_C = Conversation_C = \left\langle Speak_C \rightarrow Hear_C \rightarrow Revise_C \right\rangle$$

$$Speak_C = (Speaker\ S_C, Hearer\ H_C, Speaktime\ TS_C \rightarrow Heartime\ TH_C, Word\ W_C)$$

$$Hear_C = (Speaker\ S_C, Hearer\ H_C, Heartime\ TH_C \rightarrow Revisetime\ TR_C, Word\ W_C)$$

$$Revise_C = (Speaker\ S_C, Revisetime\ TR_C, Word\ W_C)$$

$$Game = Simulation\ of\ conversations\ \{C_C\}\ in\ global\ temporal\ order$$

# Security Applications of Naming Game

**Relevance**

- Information wars
- Establishing, chasing, erasing truths
- Opinion formation
- Software reputation, supply chain?
- Peer network infiltration?
- Network pattern effects?

**Computing**

- Computationally very intensive
- Many network models to evaluate
- Many scenarios to cover
- Real-time state infusion
- Large populations

# "When no one is watching…"

- Grand challenge problem

# A Grand Challenge **Security** Problem: Implement the following functionality with **Computing**

- "Is anyone watching me…?"
  - Me=a robotic device

- "When no one is watching, do this…"

Simple technical specification
Extremely complex problem and solution
(ala Watson)

# Thank you

## Q&A


**Kalyan Perumalla**

Distinguished R&D Staff, **Oak Ridge National Lab**
Joint Full Professor, Dept. of ISE, **University of Tennessee**

Adjunct Professor, School of CSE, **Georgia Tech**
Adjunct Professor, Dept. of ECE, **University of Nebraska**
Chair, **ACM SIGSIM**

perumallaks@ornl.gov | 865-241-1315

www.ornl.gov/staff-profile/kalyan-s-perumalla


Complimentary advice to junior staff

Aim to ultimately go from

You are cool because you work at ORNL

to

ORNL is cool because you work at ORNL