Key Analytical Points from the Workshop on Scientific Applications For the Internet of Things (IOT)

Colloquium in Trieste, Italy at:

The Abdus Salam
International Centre
for Theoretical Physics

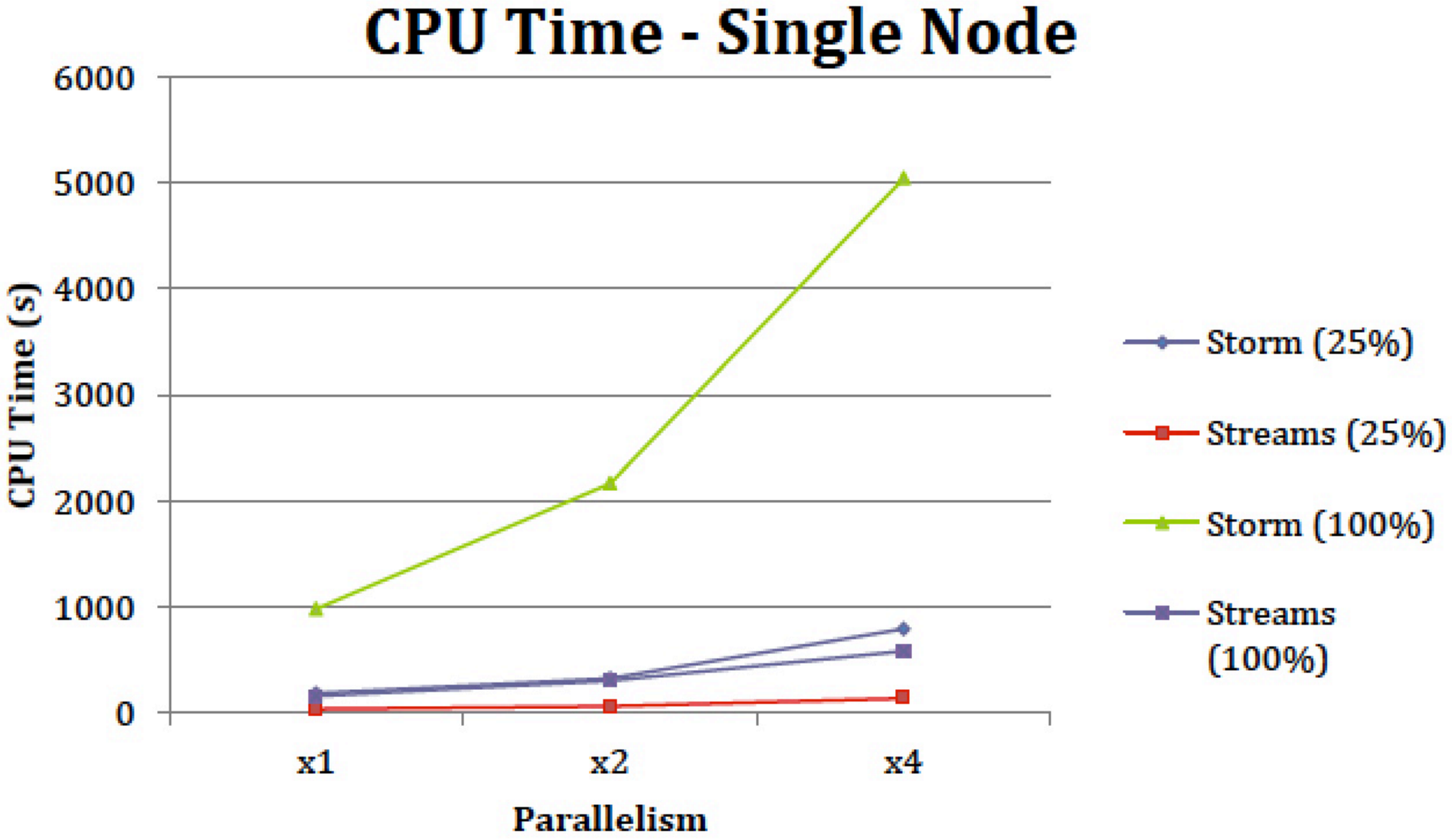
Prof. Steve Chan, PhD
Chair, Swansea University's Cyber Analytics and Network/Relationship Science
Director, Asia-Pacific Institute for Resiliency and Sustainability (AIRS)
Director, IBM Center for Resiliency and Sustainability; Strategic Advisor, IBM Smarter Cities

Storm Core vs. Storm Trident vs. Spark Streaming

	Core Storm	Storm Trident	Spark Streaming
Community	> 100 contributors	> 100 contributors	> 280 contributors
Adoption	***	*	*
Language Options	Java, Clojure, Scala, Python, Ruby, ...	Java, Clojure, Scala	Java, Scala Python (coming)
Processing Models	Event-Streaming	Micro-Batching	Micro-Batching Batch (Spark Core)
Processing DSL	No	Yes	Yes
Stateful Ops	No	Yes	Yes
Distributed RPC	Yes	Yes	No
Delivery Guarantees	At most once / At least once	Exactly Once	Exactly Once
Latency	sub-second	seconds	seconds
Platform	Storm Cluster, YARN	Storm Cluster, YARN	YARN, Mesos Standalone, DataStax EE

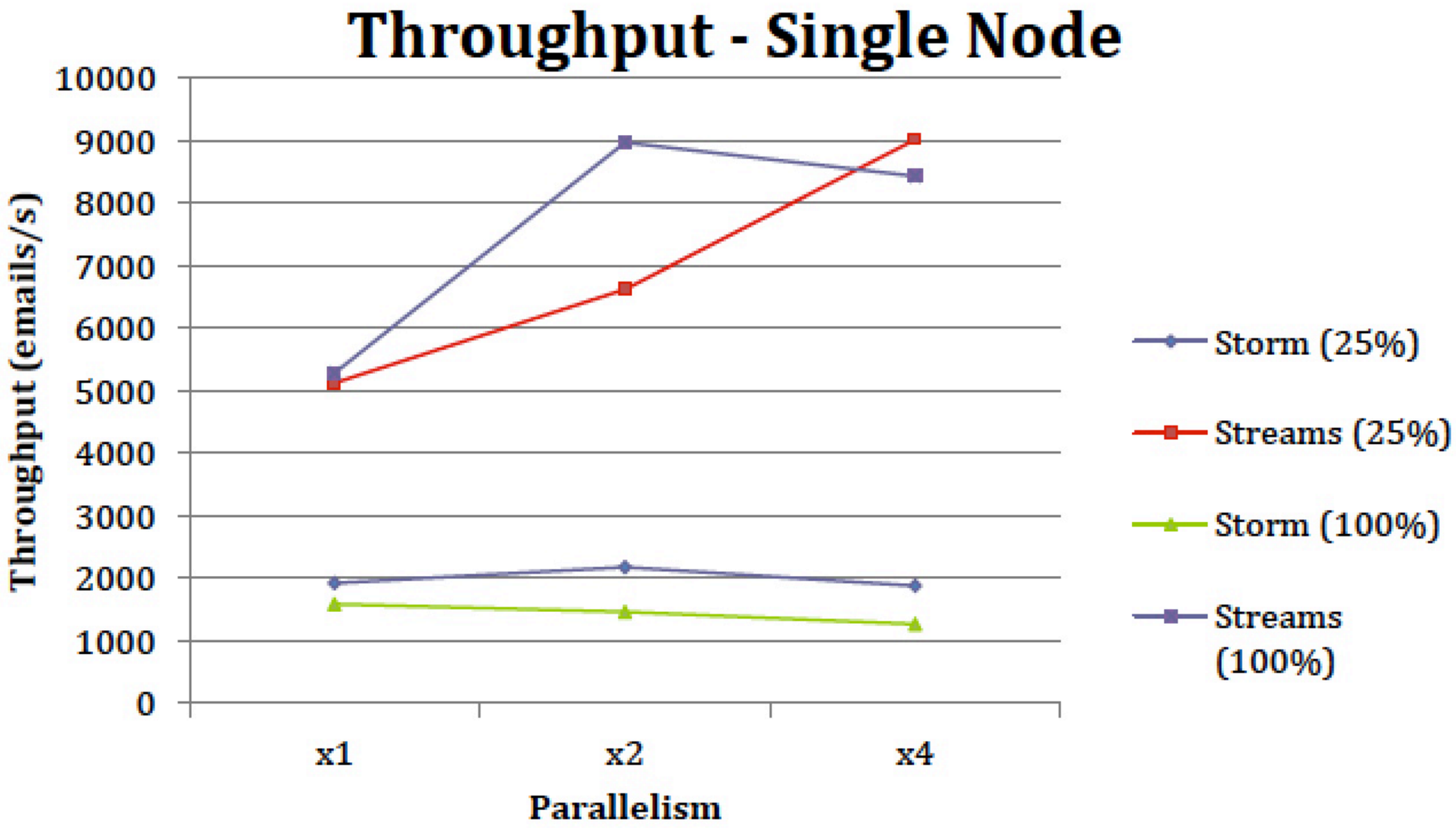
Source: Trivadis

Acknowledgments: Please refer to source, adaptation, and acknowledgments page:



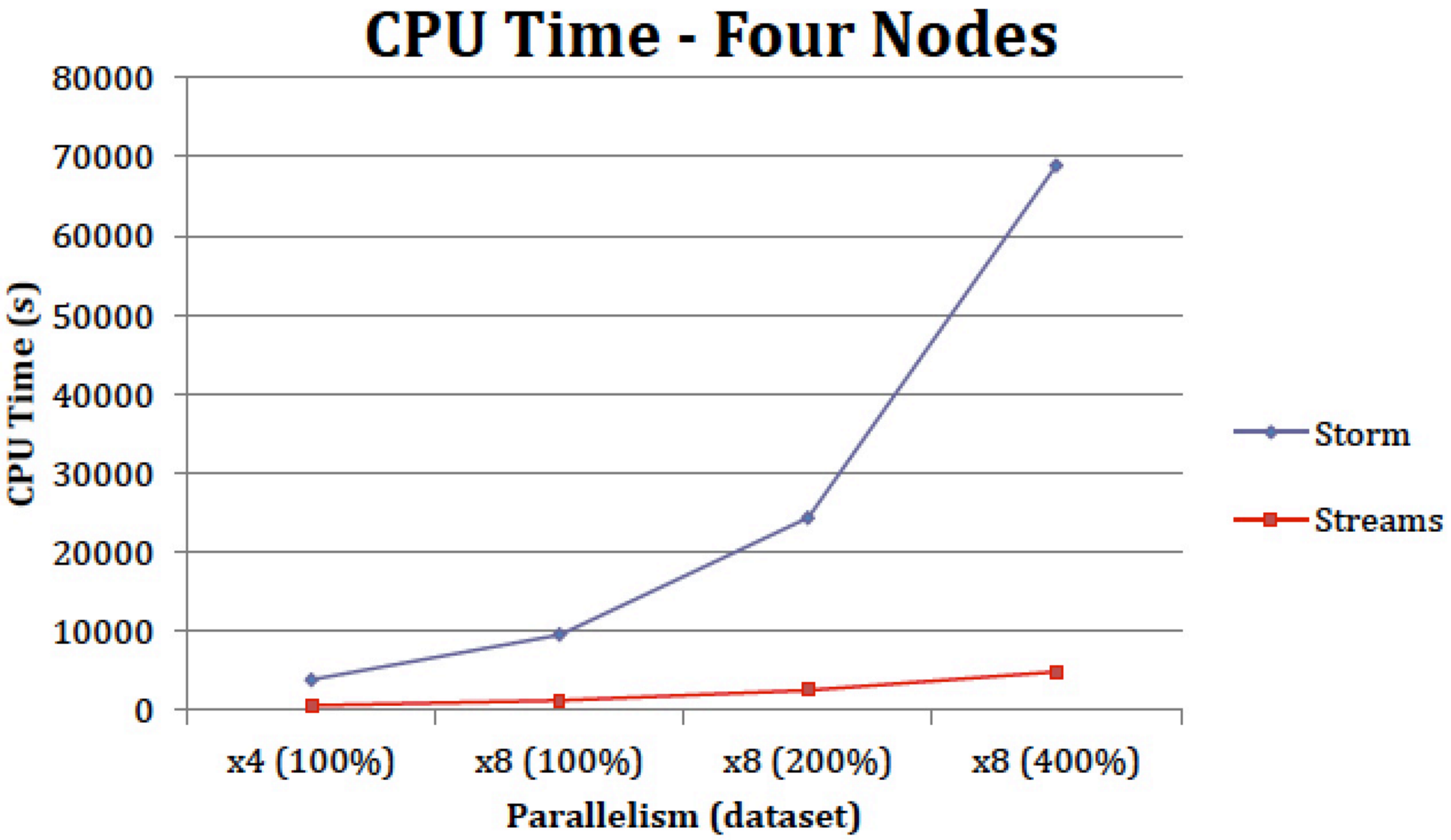
Source: IBM

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.



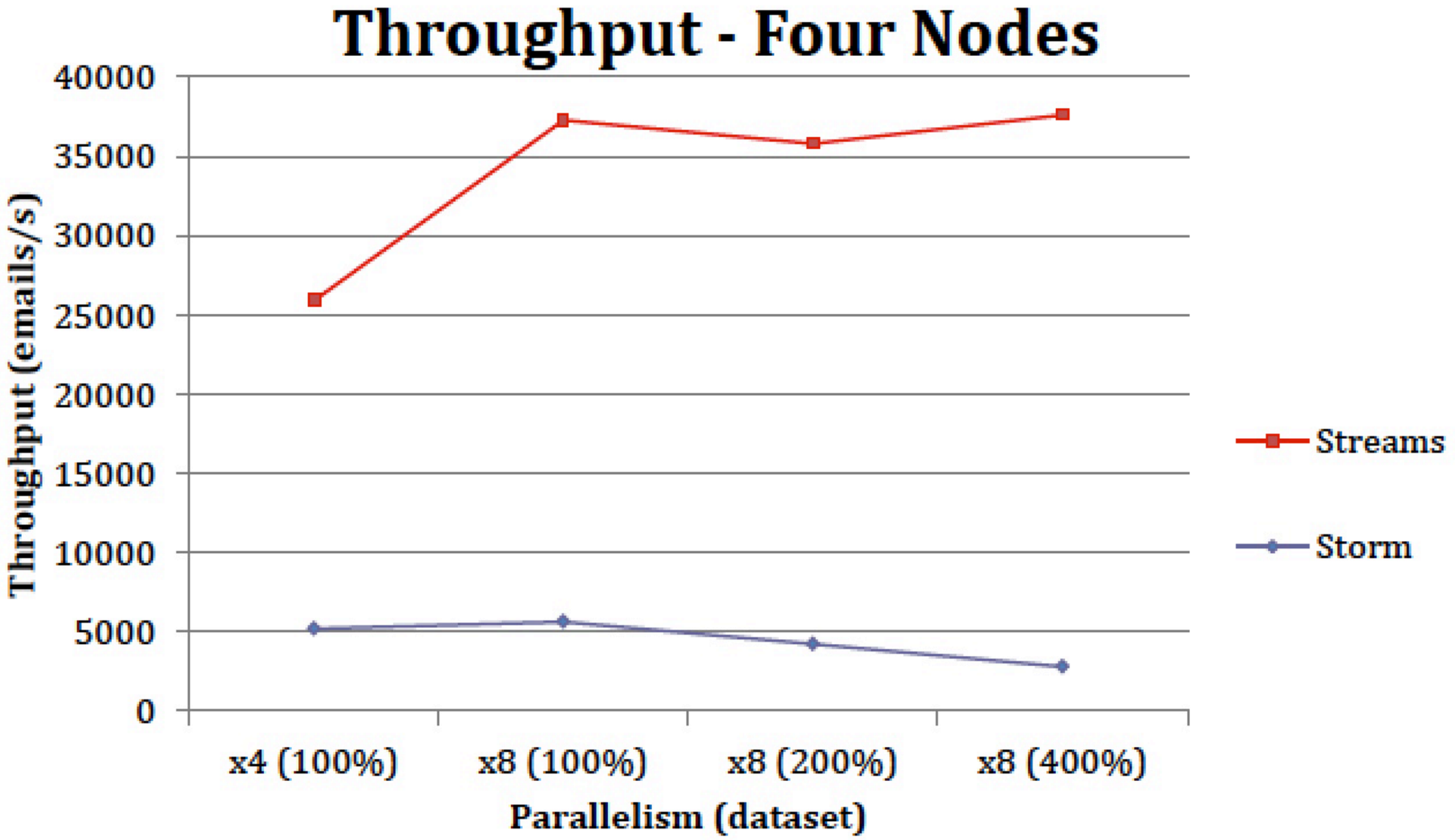
Source: IBM

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.



Source: IBM

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.



Source: IBM

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

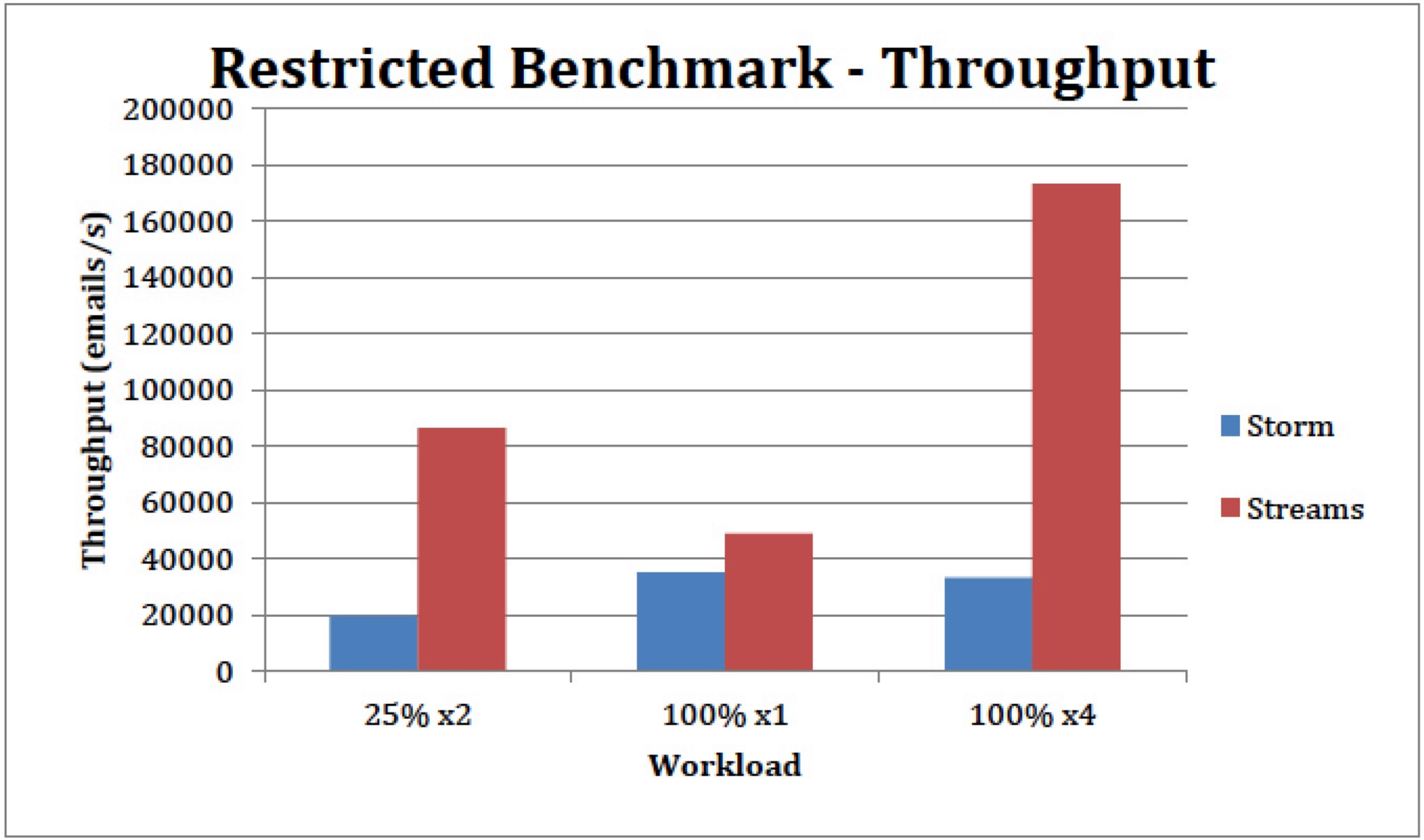


Figure 11: Restricted Benchmark Throughput

Source: IBM

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

Security

- What changes in the IoT:
  - Resource poverty: relatively low processing power and energy stores
  - Asynchrony: your devices are switched off most of the time
  - Clock sync is not a given and is important
  - Mobility, the importance of location
  - Poor access to the hardware
  - Byzantine is the norm – things fail, but frequently not cleanly.
  - Cascading failure is the norm
  - Boundaryless security
    - Self protection
    - Intrusion detection
    - Many more points for information leakage
  - New DoS attacks
    - e.g. sleep deprivation
  - Actuators

Source: Steve Hailes, UCL

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

Key Analytical Points from the Workshop on the Internet of Things (IOT)

Security processes 1

- If we want to secure a system, then we need to follow a number of principles:
  - Prevention is *never* 100% effective – so:
    - Need defence in depth – several different mechanisms
    - Mechanisms for detecting and responding to attacks, preferably in real time, are essential:
      - Detect – get to know you're being attacked.
      - Localise – determine what's being attacked.
      - Identify – determine who the attacker is.
      - Assess – why are they doing this?
      - Respond – depends on all of above.
      - Recover – Have a plan better than 'go find a new job'

Source: Steve Hailes, UCL

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

Key Analytical Points from the Workshop on the Internet of Things (IOT)

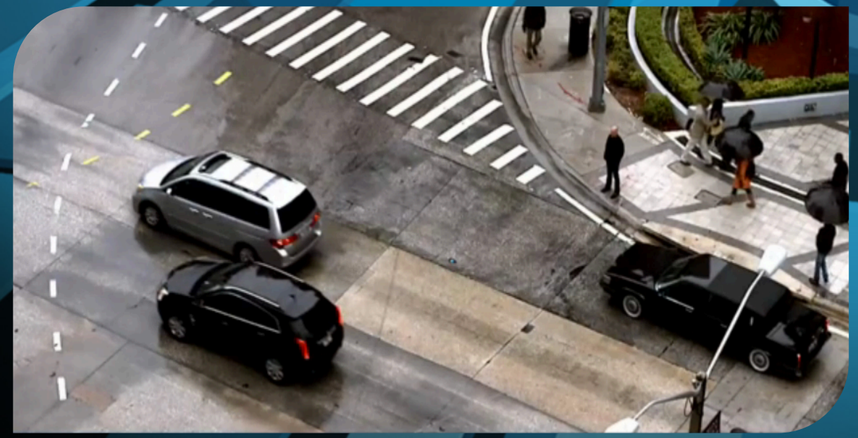
Edge Processing = Data Acquisition + Data Analytics

- The opportunity is in Sense-and Respond systems at the edge to optimize operations and avoid the need for black-start/quick-start.
- Success in Africa and for Smarter Cities/Smarter Planet necessitates integrating lessons from the Microgrid Stability Paradox so as to effectuate higher penetration of renewables while enhancing stability and resiliency.

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

1. Deficiencies of Event/SCADA Data (Big Data) -> Continuous Streaming Data (Bigger Data)

- Event and SCADA data are essentially too little and too late for effective operation of the modern Grid. Continuous streaming high quality data (Bigger Data) is required for a stable and resilient Grid.



Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

2. Deficiencies of an Arbitrary Bus Reference -> Calculated Center of Inertia

- (Base vector + Drift) ⇔ Context-Referenced Phase Angle Data
- Calculated Center of Inertia

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

3. High Penetration of Renewables -> From Transmission to Distribution

- The high penetration of renewables results in less stable operation of the distribution system. Acquisition of quality real-time data, enriched by analytics, will be used to enable operations with higher levels of renewables.

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

4. Consumer/PUC Reluctance to absorb cost of black-start/ quick-start -> Better Sense and Respond

- The costs of adding black-start/quick-start capability is prohibitively expensive. The providing of real-time monitoring, analytics, and controls for better “Sense-and-Respond” reduces the need for these very expensive facilities.

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

5. Desire for better Defense-in-Depth Methodology (Citizen Science/Crowd-Sourced Data)

- Augmenting real-time power system Data with Citizen Science/Crowd-Sourced Data facilitates the movement from Big Data to even Bigger Data.

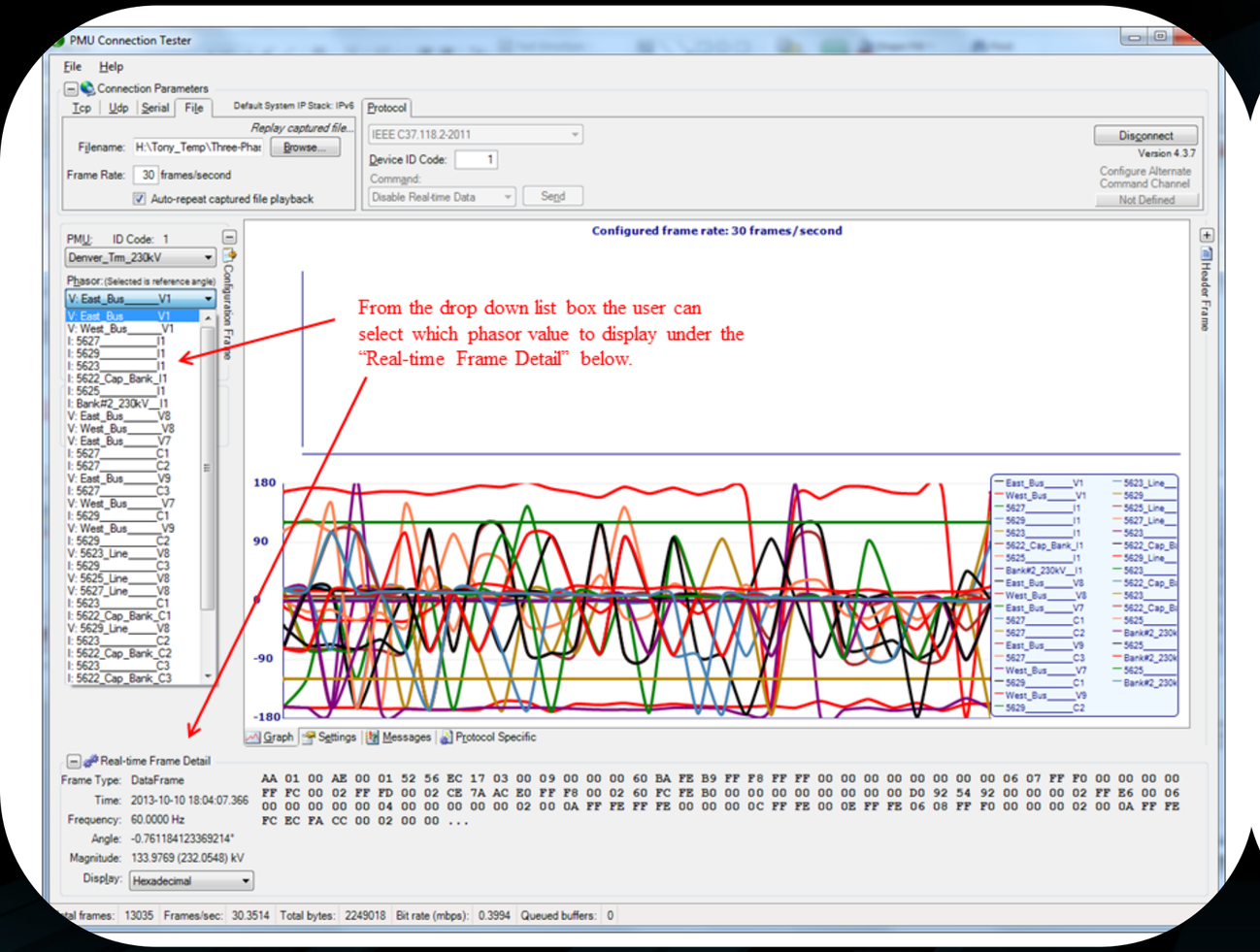
Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

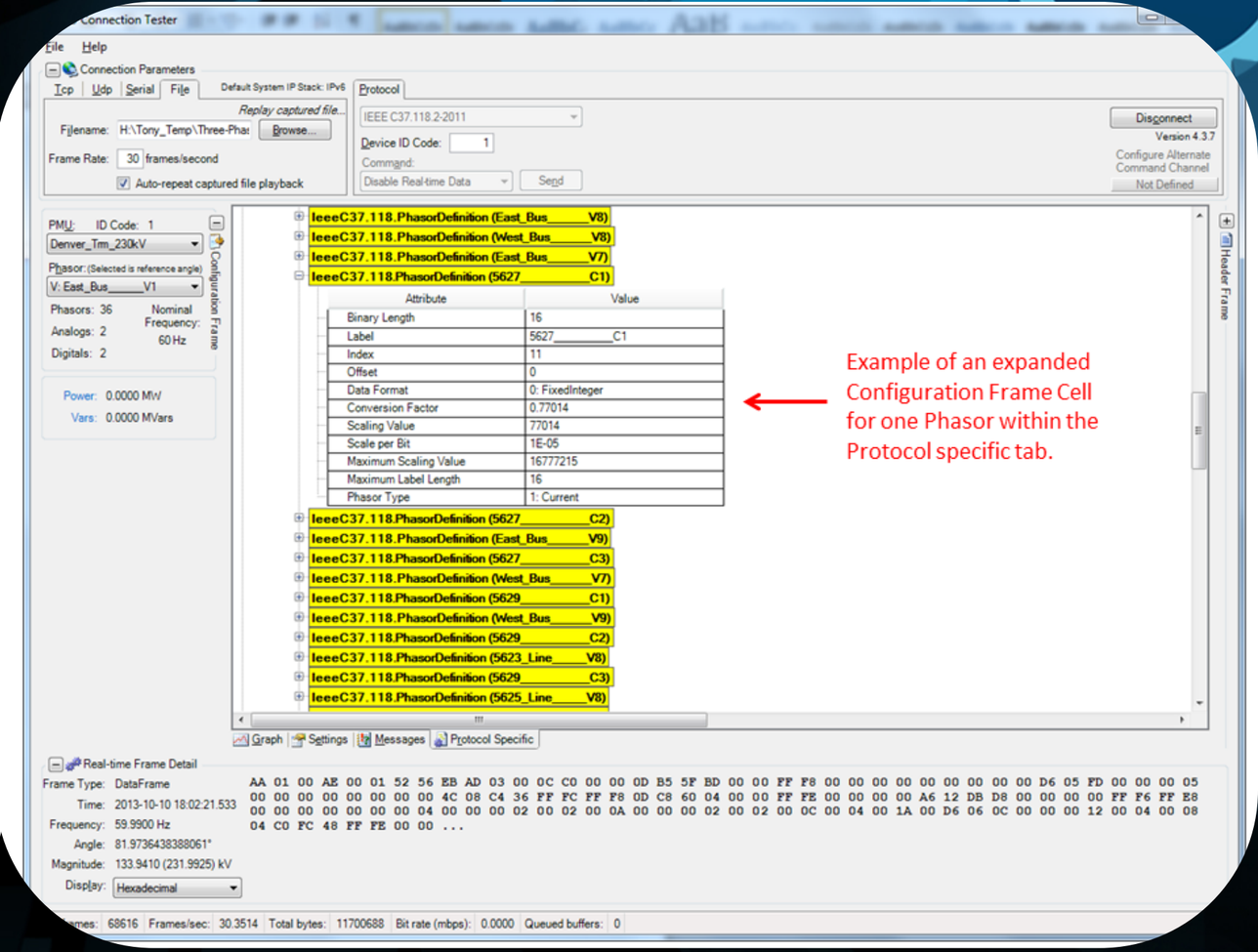
6. Microgrid (e.g. DOD, Data Centers)
-> High use of Renewables represents a Paradox

- Microgrids are expected to provide a higher level of availability that the Grid. Yet, the microgrids' high use of renewables introduces heightened instability. The effective operationalization of microgrids necessitates 1 to 5.

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

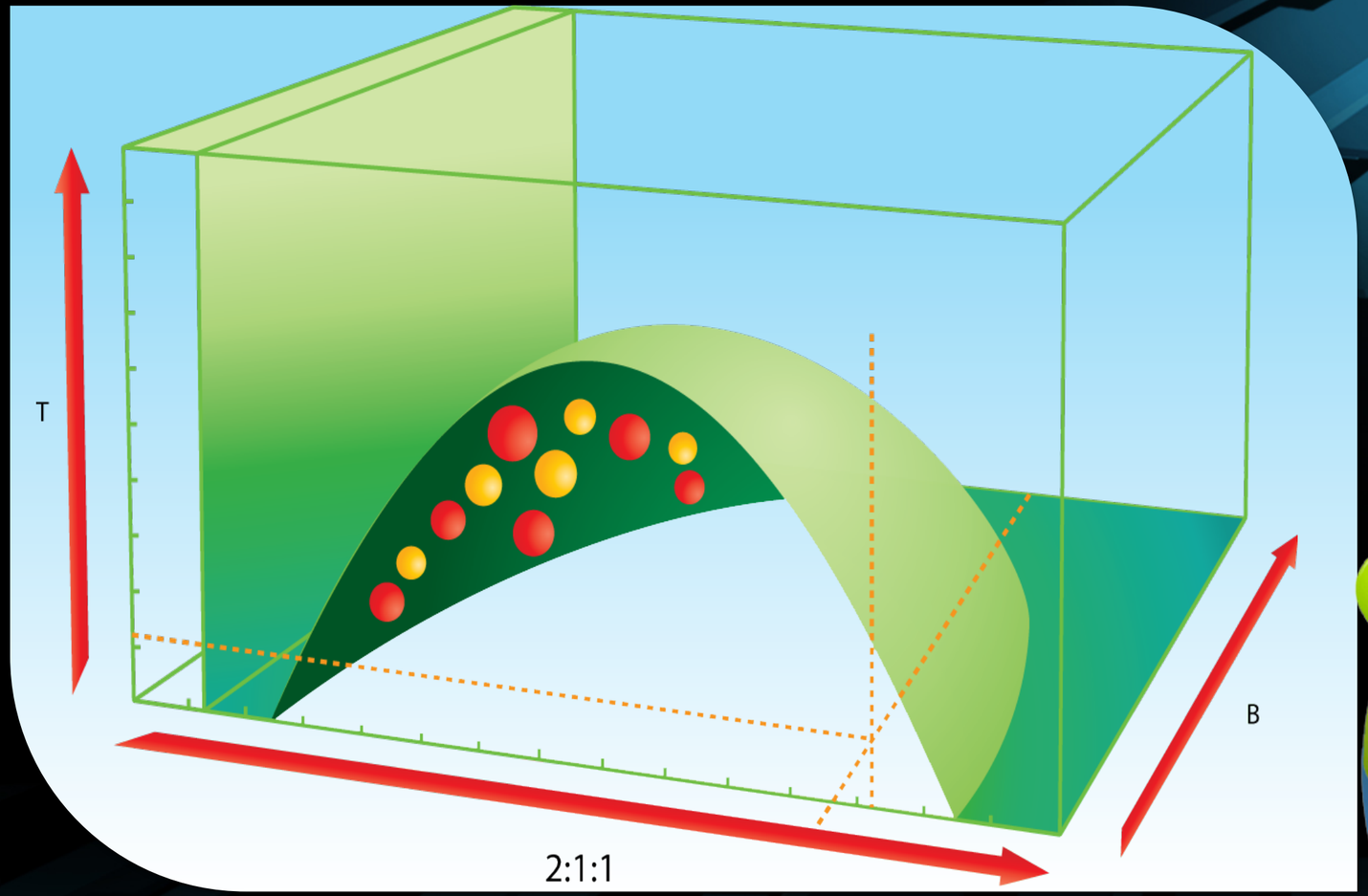
8. Isomorphic Experience -> Lower Ambiguity -> More Robust Decision Engineering



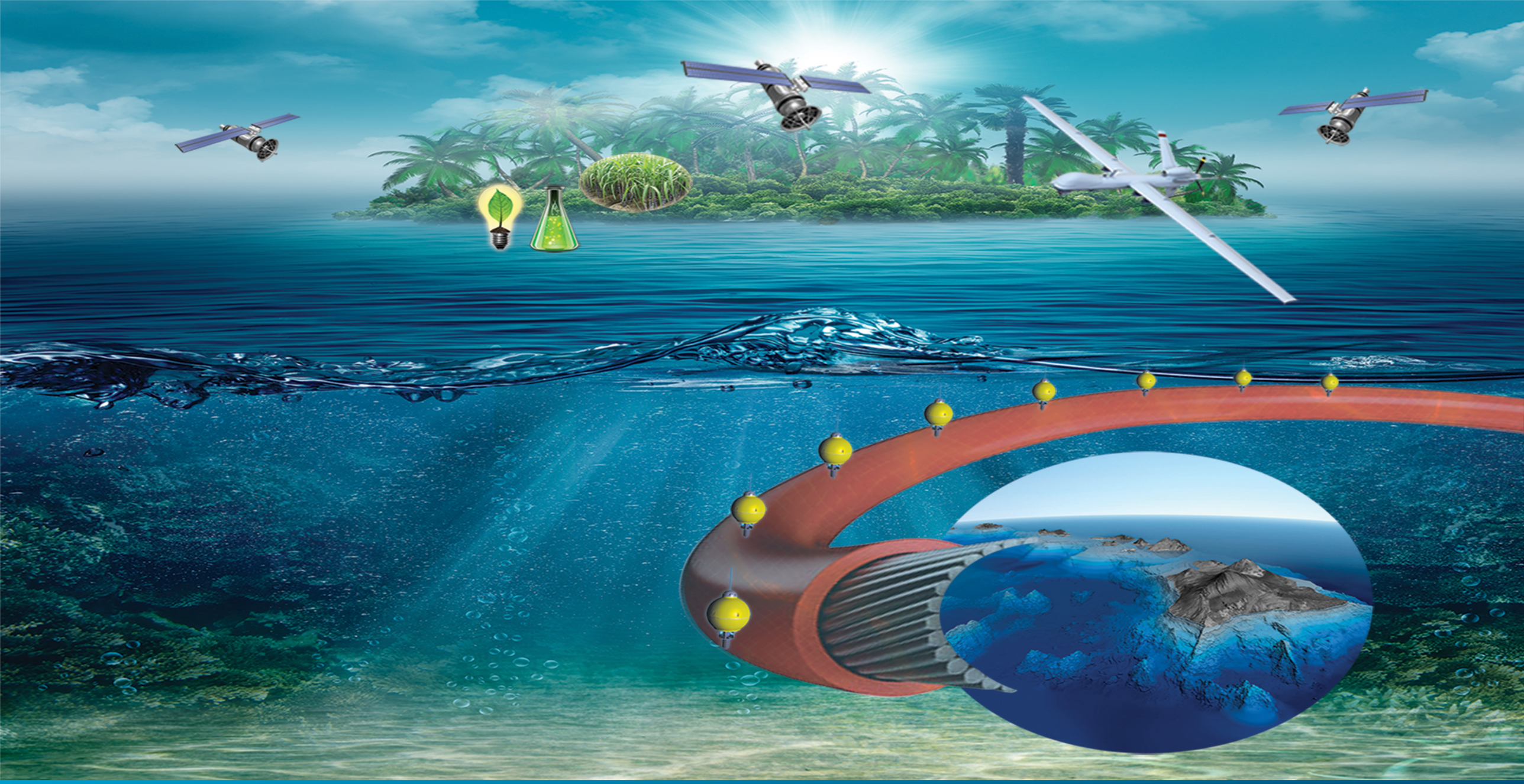


Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

8. Isomorphic Experience -> Lower Ambiguity -> More Robust Decision Engineering



Acknowledgments: Please refer to source, adaptation, and acknowledgments page.



Key Analytical Points from the Workshop on the Internet of Things (IOT)

A warning (1)….

If you believe that encryption is the answer to your security problem, then you probably asked the wrong question.

- What on earth does ‘security’ mean anyway?
  - It’s a state of being – everything is OK
- Security is about securing a **system**
- Security is a **process** NOT a product
- A sole focus on technology is blinkered and founded in ignorance

Source: Steve Hailes, UCL

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

Key Analytical Points from the Workshop on the Internet of Things (IOT)

Study Space: Haiti

A2O Finding: Commodities, such as Internet Access (for aid, weather, news), are more important to Tent City Refugees than water and medicines, amidst a paradigm of counterfeits (no electrolytes, sawdust). Context Matters.

Big Insight: Counterfeiters are the promulgators of – unexpectedly – 1/3 of the world's spam and malware.

NASA Resource Utilized: Uninhabited Aerial Vehicle Synthetic Aperture Radar (UAVSAR) data (e.g. backscatter) from NASA's C-20A Gulfstream III.

Takeaway: Wifi and they will come.

Key Analytical Points from the Workshop on the Internet of Things (IOT)

Study Space: Pacific Ocean

A2O Finding: HPC and High Order High Fidelity Modeling for robust Tsunami Warning (non-spoofing, via 5V Tests). Apropos Compute Matters.

Big Insight: Hybridizing near-shore and far-shore modeling provides fidelity lessons learned for texture, shape, and color histograms.

NASA Resource Utilized: NASA World Wind's Blue Marble for true colors and Landsat 7 for high resolution imagery.

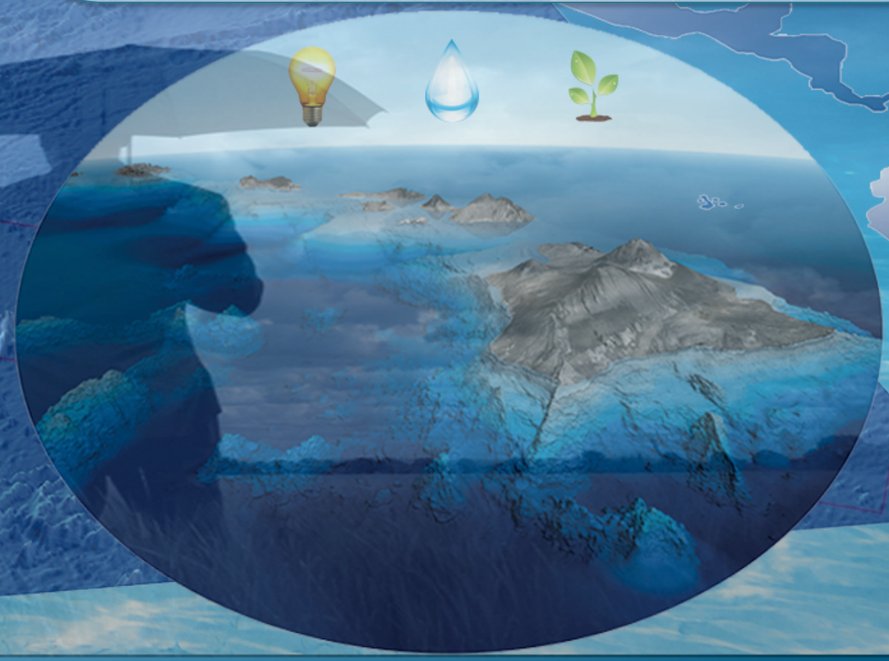
Takeaway: Slowly but surely.

Key Analytical Points from the Workshop on the Internet of Things (IOT)

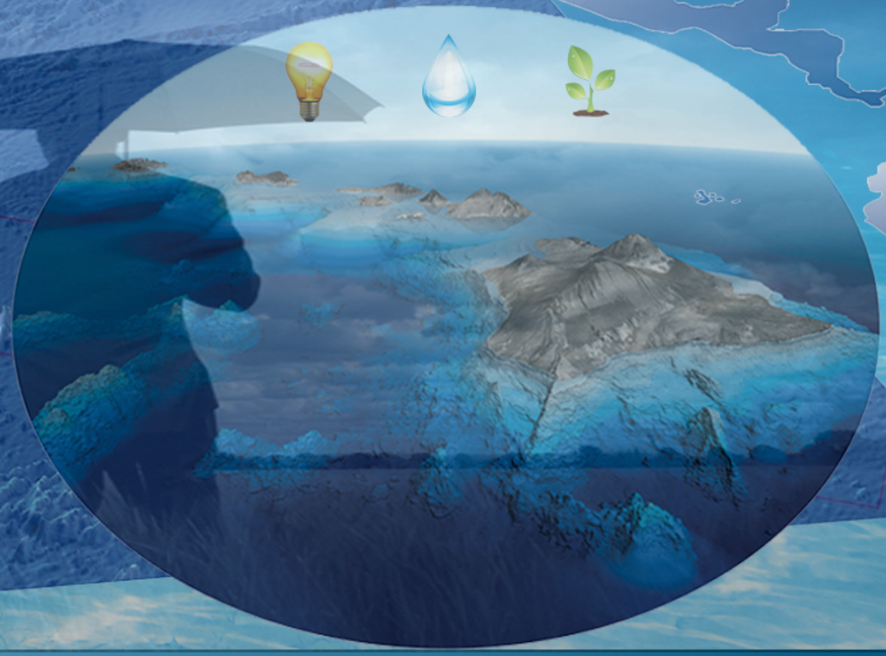
Alaskan Earthquakes:

- 1946 Alaska Earthquake (7.4) and Tsunami.
- 2014 Alaska Earthquake (7.9).

- 19 today.
- 463 this month.
- 5,313 this year, thus far.



Key Analytical Points from the Workshop on the Internet of Things (IOT)



Key Analytical Points from the Workshop on the Internet of Things (IOT)

Key Analytical Points from the Workshop on the Internet of Things (IOT)

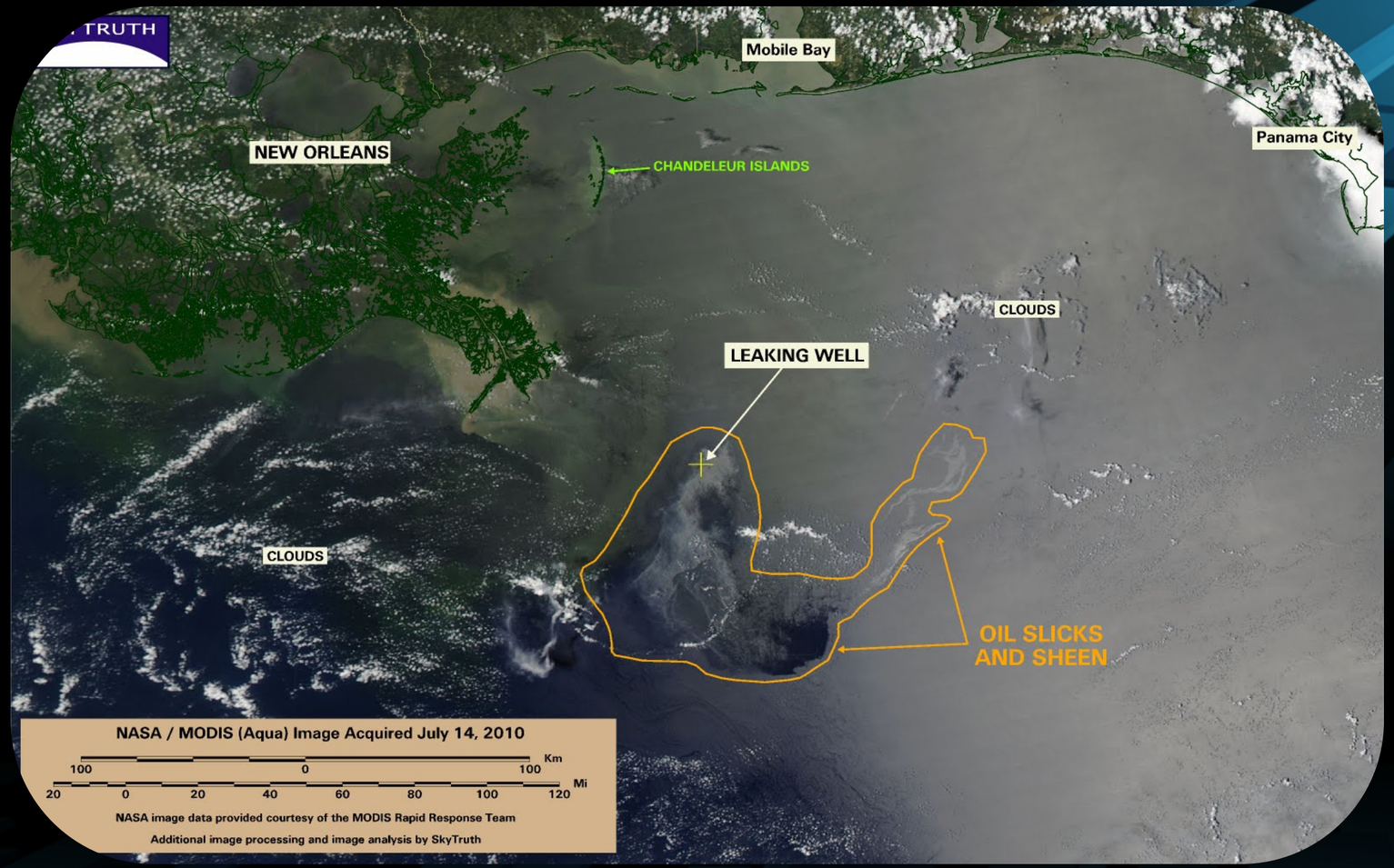
Study Space: Gulf of Mexico

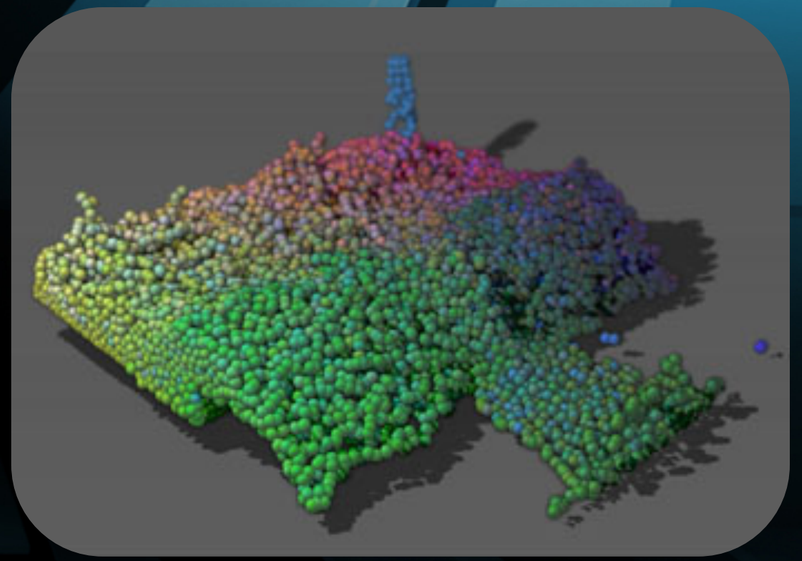
A2O Finding: HPC and High Order High Fidelity Modeling for the Oil Slick Spread (Deepwater Horizon Oil Spill). Apropos Compute Matters.

Big Insight: Smooth Particulate Hydrodynamic (SPH) Modeling for non-approximation.

NASA Resource Utilized: Advanced Spaceborne Thermal Emission and Reflection Radiometer (ASTER) imagery (e.g. light) from the Terra satellite.

Takeaway: Measure twice cut once.





Key Analytical Points from the Workshop on the Internet of Things (IOT)

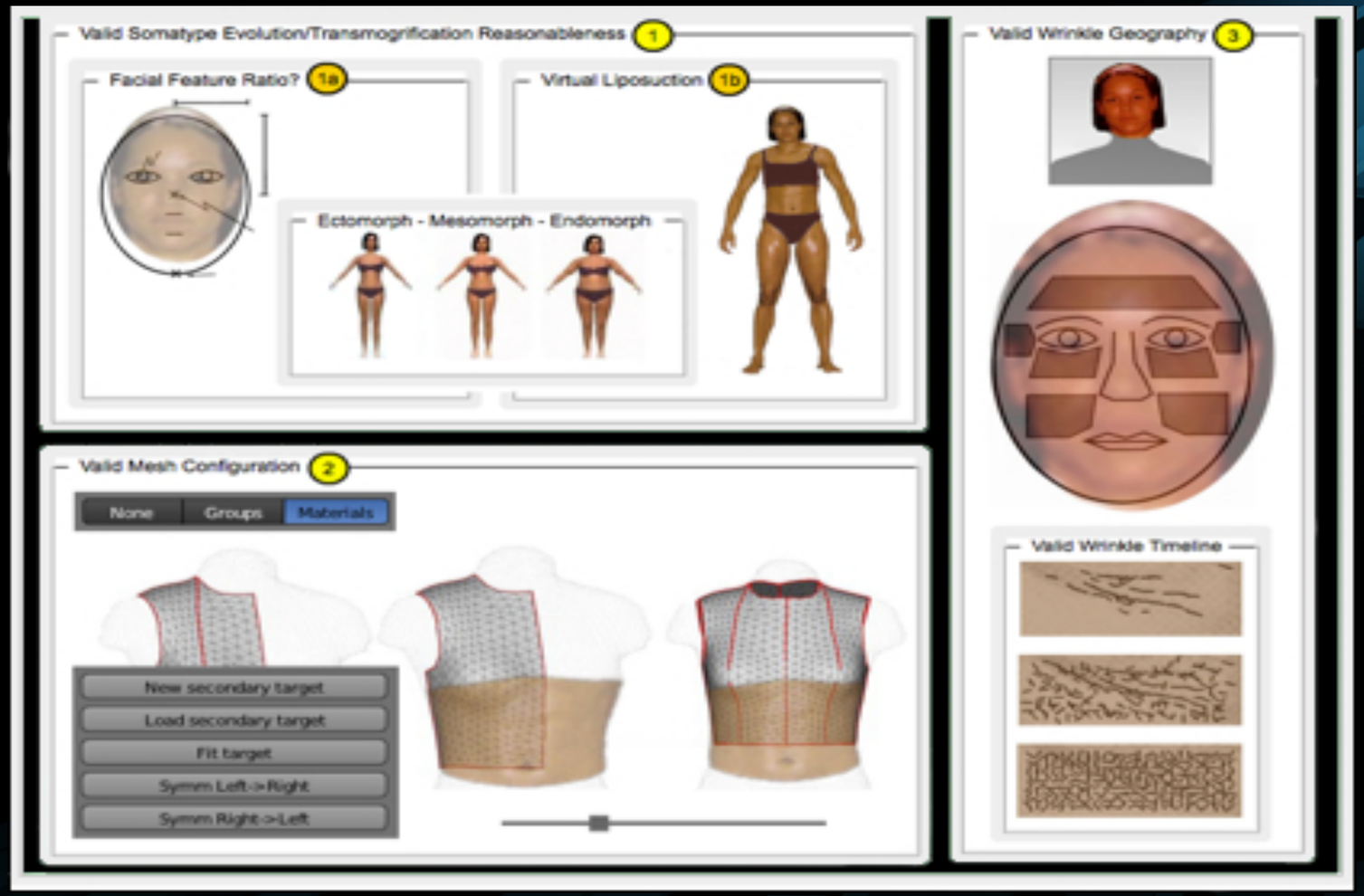
Study Space: Cyberspace

A2O Finding: Workflow process matters for removing hay from the haystack. Qualifying Sequence Neutrality.

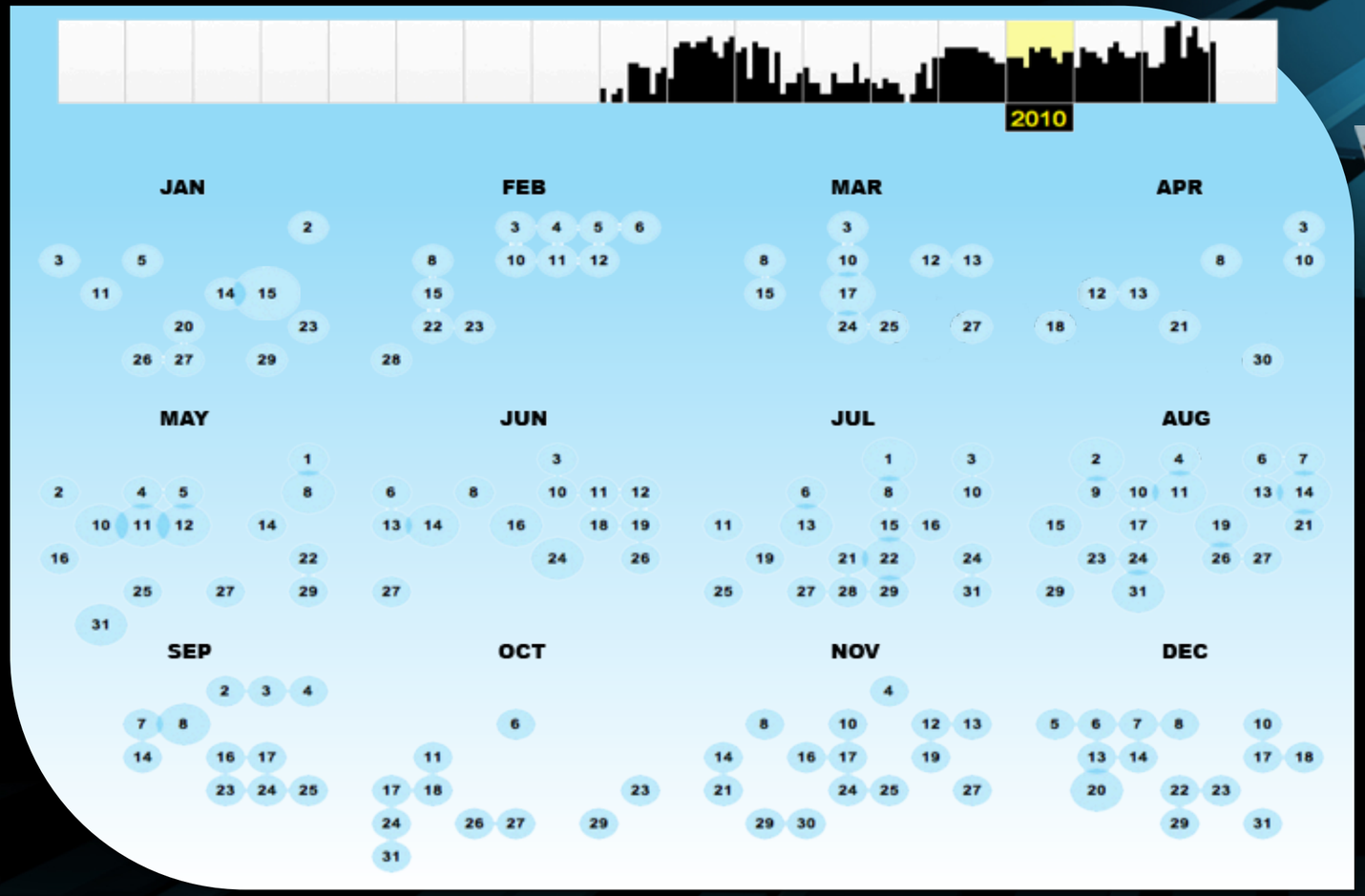
Big Insight: The analysis begins with detecting specular highlights, then mesh distortion, then wrinkle geography.

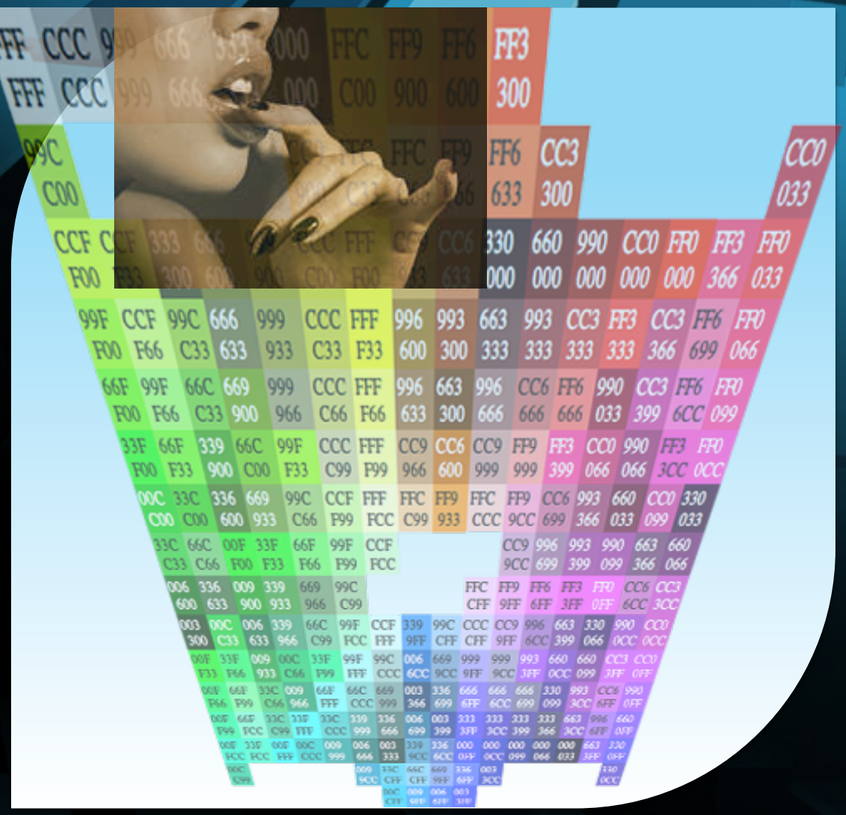
NASA Resource Utilized: Tool for Analysis of Surface Cracks (TASC) + Hyperspectral Recognition of processing tomato early blight based on Genetic Algorithms (GA) and Support Vector Machines (SVM)

Takeaway: Penny-wise, but pound foolish.

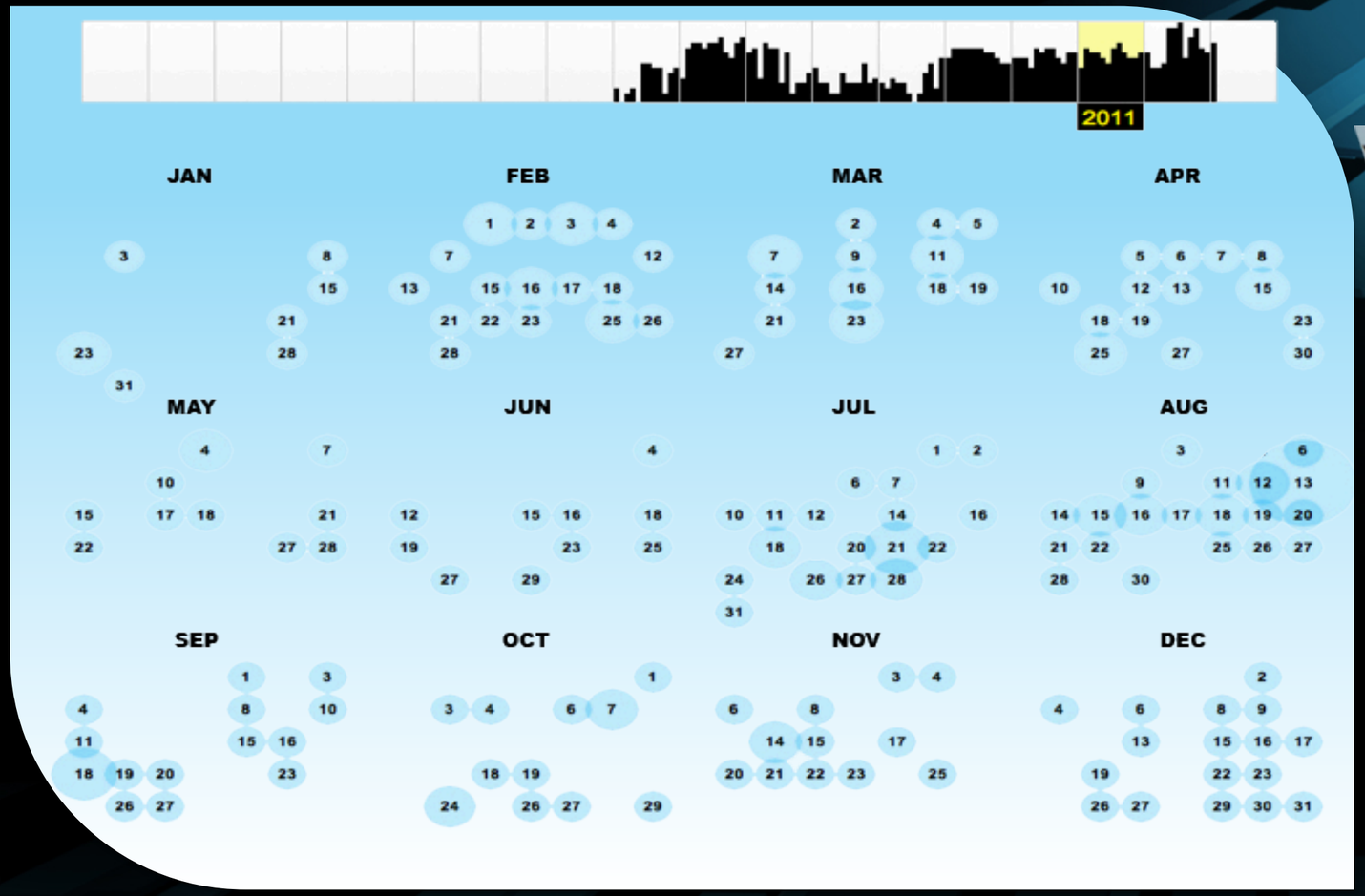


Key Analytical Points from the Workshop on the Internet of Things (IOT)

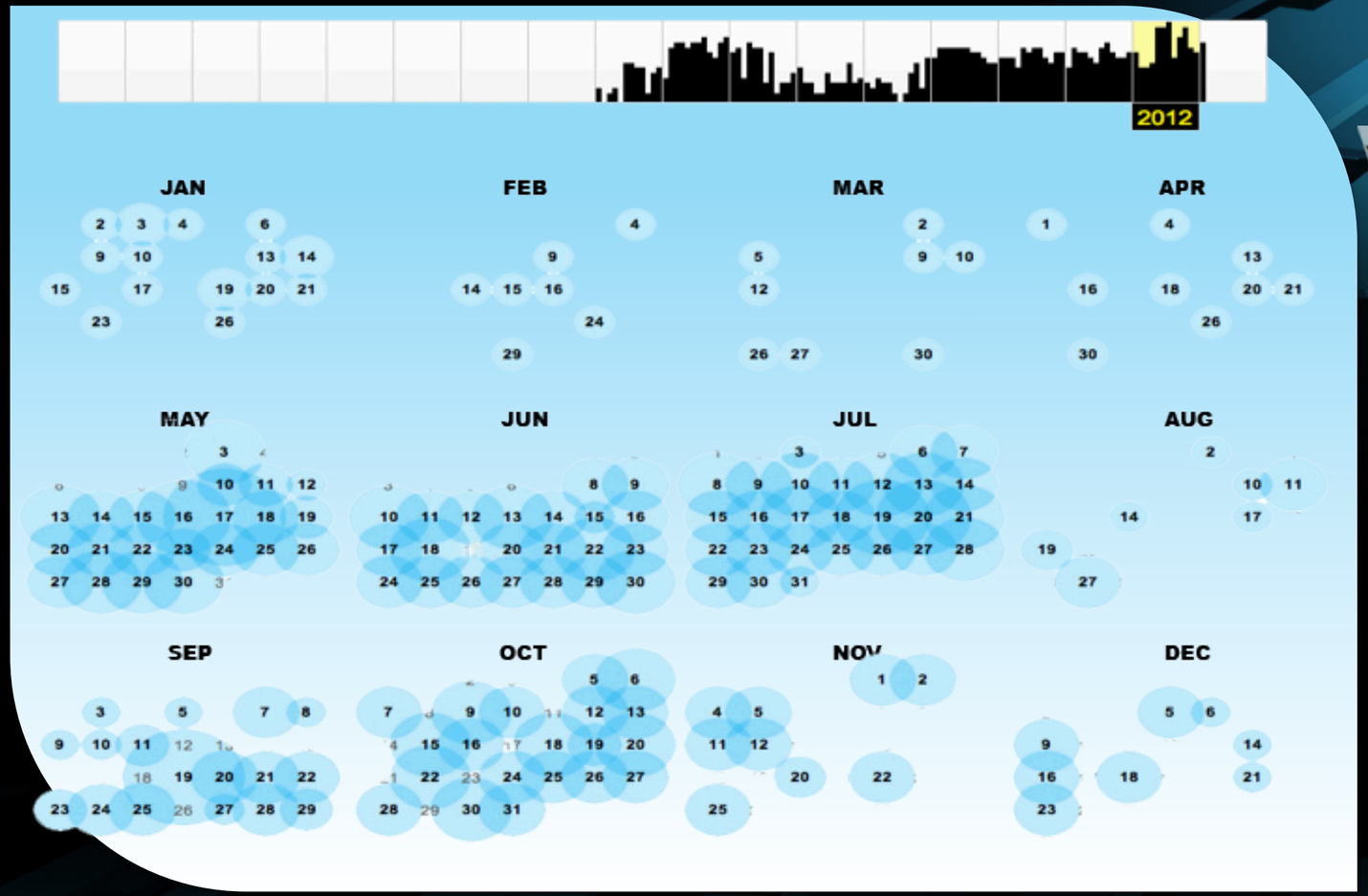


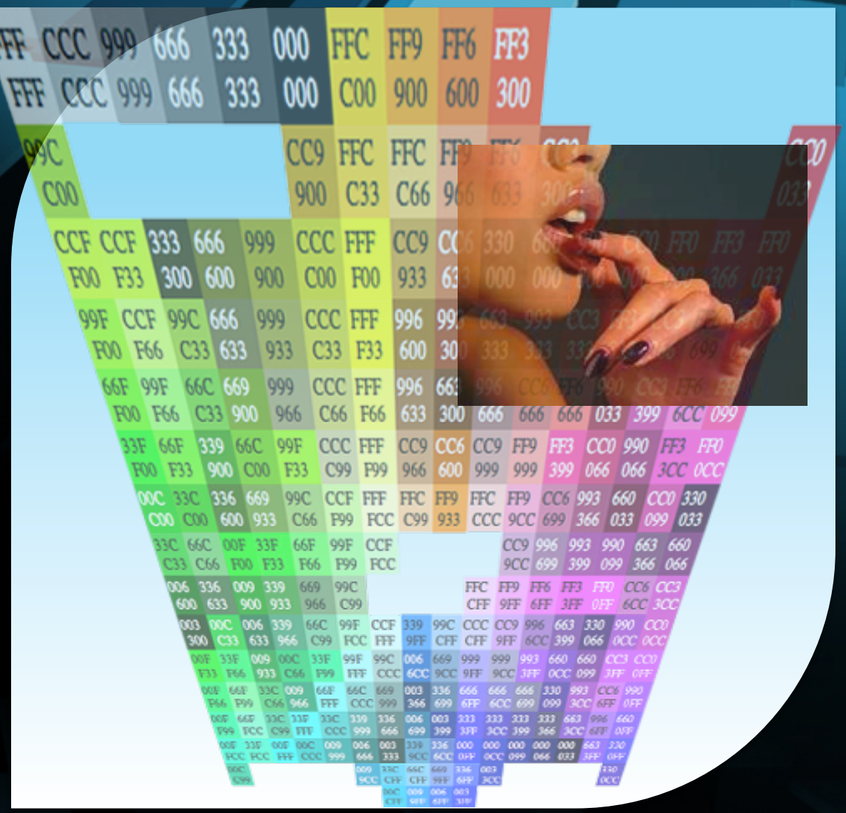


Key Analytical Points from the Workshop on the Internet of Things (IOT)



Key Analytical Points from the Workshop on the Internet of Things (IOT)





Key Analytical Points from the Workshop on the Internet of Things (IOT)

Security processes 1

- If we want to secure a system, then we need to follow a number of principles:
  - Prevention is *never* 100% effective – so:
    - Need defence in depth – several different mechanisms
    - Mechanisms for detecting and responding to attacks, preferably in real time, are essential:
      - Detect – get to know you're being attacked.
      - Localise – determine what's being attacked.
      - Identify – determine who the attacker is.
      - Assess – why are they doing this?
      - Respond – depends on all of above.
      - Recover – Have a plan better than 'go find a new job'

Source: Steve Hailes, UCL

Acknowledgments: Please refer to source, adaptation, and acknowledgments page.

Key Analytical Points from the Workshop on the Internet of Things (IOT)

Key Analytical Points from the Workshop on the Internet of Things (IOT)

Thank you!

Dr. Marco Zennaro,
Prof. Ermano Pietrosemoli,
The Guglielmo Marconi Laboratory,
and everyone at the
International Centre for Theoretical Physics (ICTP)

Key Analytical Points from the Workshop on Scientific Applications For the Internet of Things (IOT)

Colloquium in Trieste, Italy at:

The Abdus Salam
International Centre
for Theoretical Physics

Prof. Steve Chan, PhD
Chair, Swansea University's Cyber Analytics and Network/Relationship Science
Director, Asia-Pacific Institute for Resiliency and Sustainability (AIRS)
Director, IBM Center for Resiliency and Sustainability; Strategic Advisor, IBM Smarter Cities