Hair Raising Hazards from AI, ML & IoT:
Adaptive Response to Cyberphysical Risks

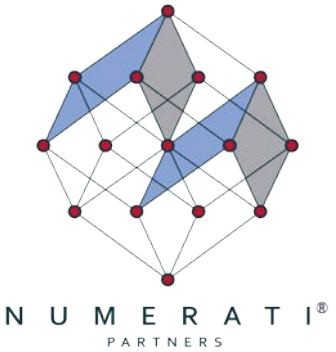
David K.A. Mordecai, PhD

RiskEcon® Lab@Courant Institute of Mathematical Sciences

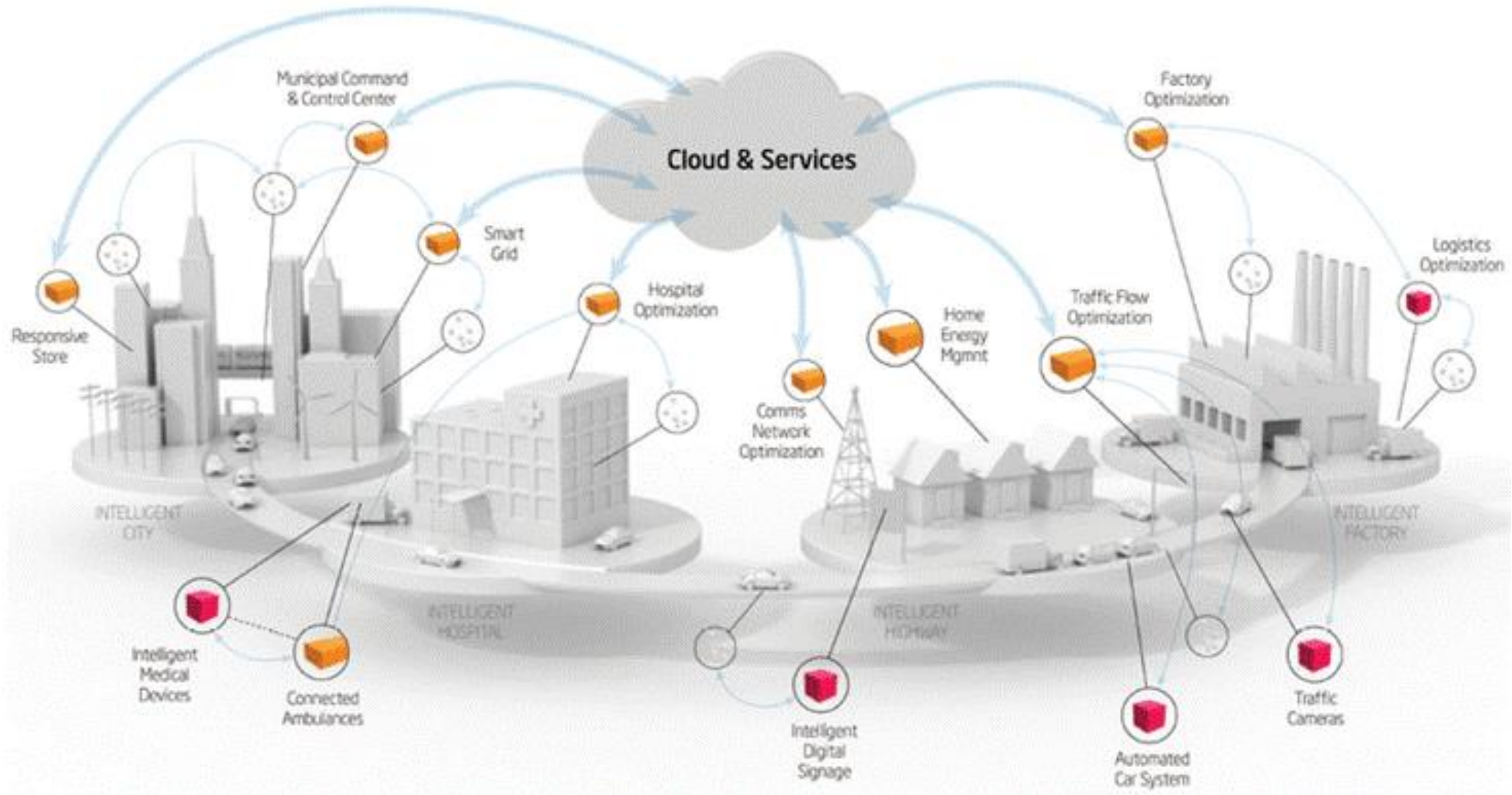
NYU Numerati Partners, LLC

NECPUC Symposium

May 22nd, 2018

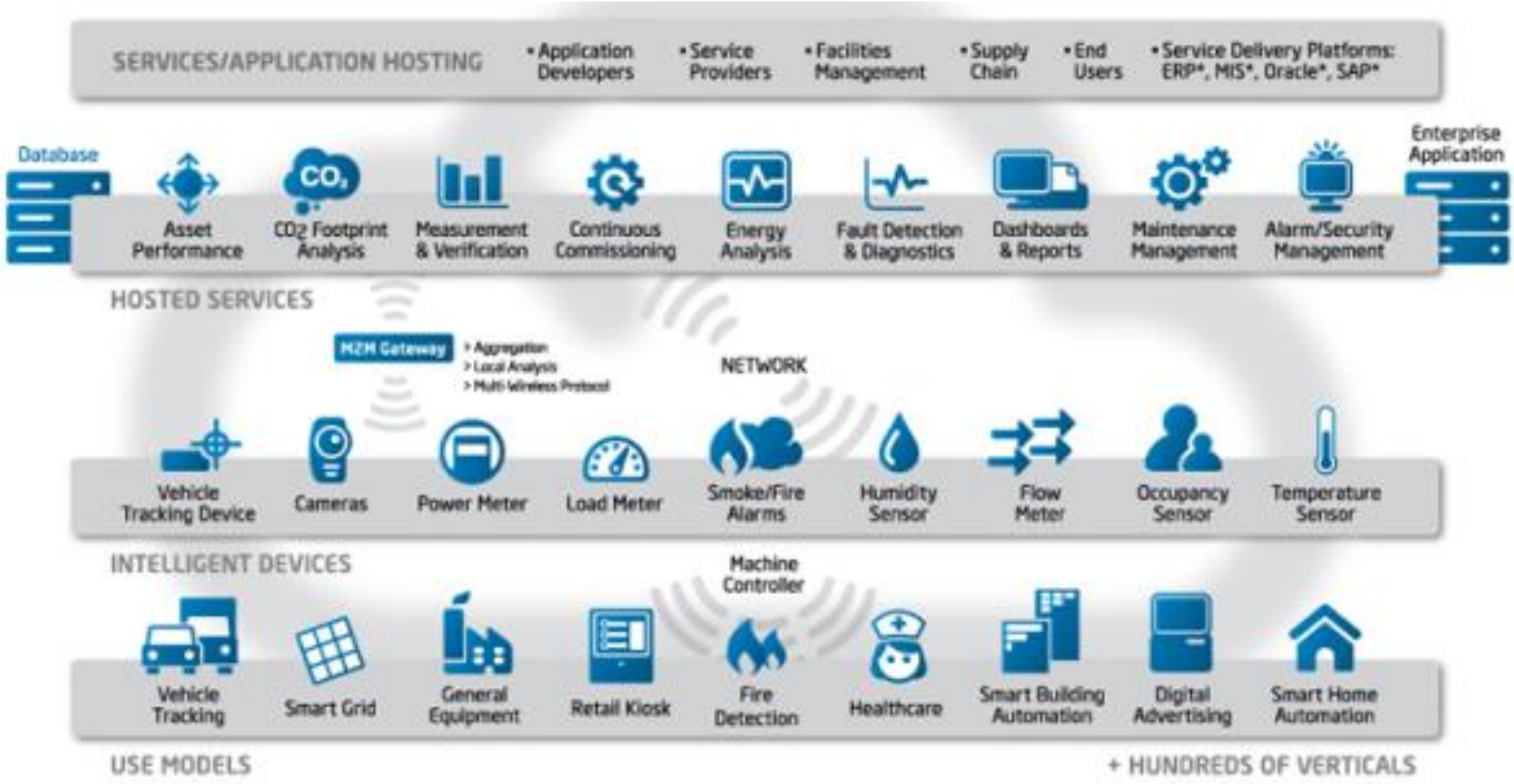


Proliferating Commercial Internet-of-Things (IoT)

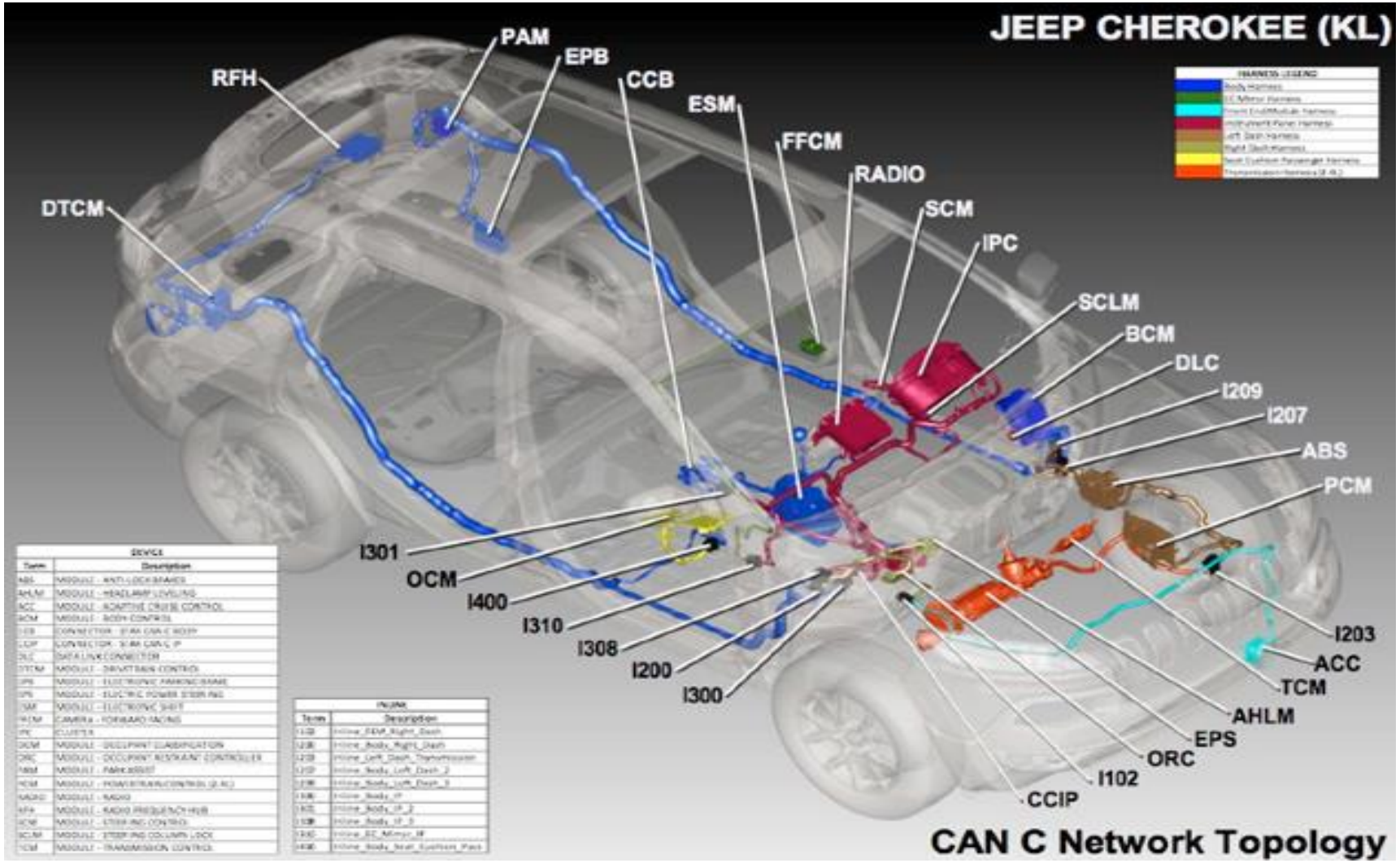


In 1984, the number of devices connected to the Internet: 1000. In 2012, number of connected devices: 17,000,000,000. By 2020, Gartner estimates anywhere from 26,000,000,000 to 50,000,000,000 devices

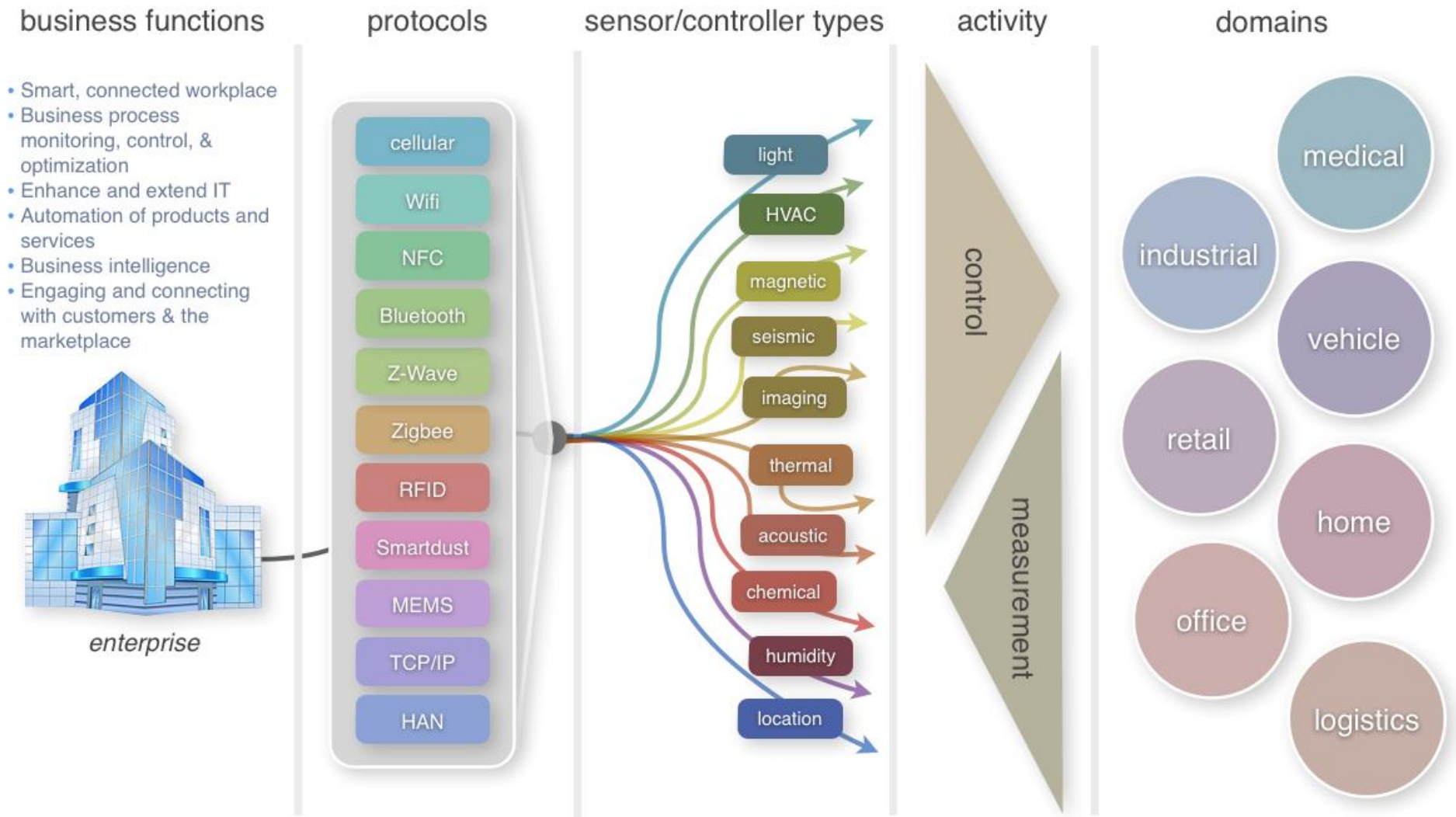
A Pervasive and Ubiquitous Network of Devices



Each ECU is a miniature computer with a specific set of tasks and vulnerabilities: More ECUs ==> more risk



Enterprise View of the Internet of Things



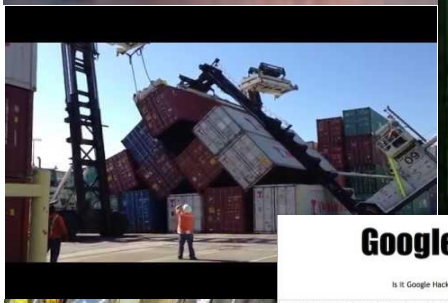
From http://zdnet.com/blog/hinchcliffe on ZDNet.

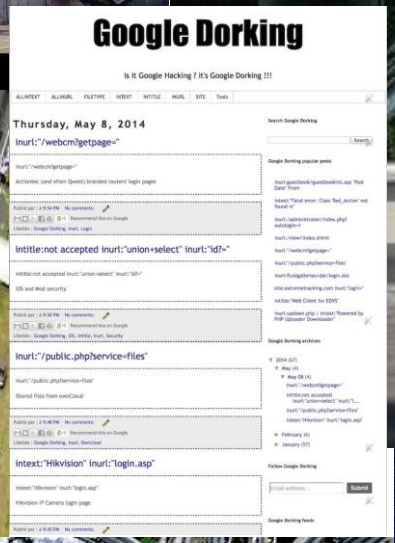
Feds issue bulletin warning about malicious 'Google dorking' cyber actors

Computerworld | Aug 26, 2014 8:20 AM PT

The bulletin referenced Search Diggity, another not-new project, which includes "free online tool suite that enables users to automate Google dork queries. It contains both offensive and defensive tools and over 1,600 pre-made dork queries that leverage advanced search operators."

June 2013 was the most recent update to SearchDiggity 3.1, "the primary attack tool of the Google Hacking Diggity Project. It is Bishop Fox's MS Windows GUI application that serves as a front-end to the most recent versions of our Diggity tools: GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, FlashDiggity, MalwareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMalwareSearch, and NotInMyBackYard Diggity."





```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitic
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<script type="text/javascript" language="javascript">
var areYouReallySure = false;
var internalLink = false;
function areYouSure() {
if (!areYouReallySure && !internalLink) {
areYouReallySure = true;
str = 'YOUR BROWSER HAS BEEN LOCKED.\n\nALL PC DATA WI
PAID.';
alert(str);
return str;
}
}
window.onbeforeunload = areYouSure;
```

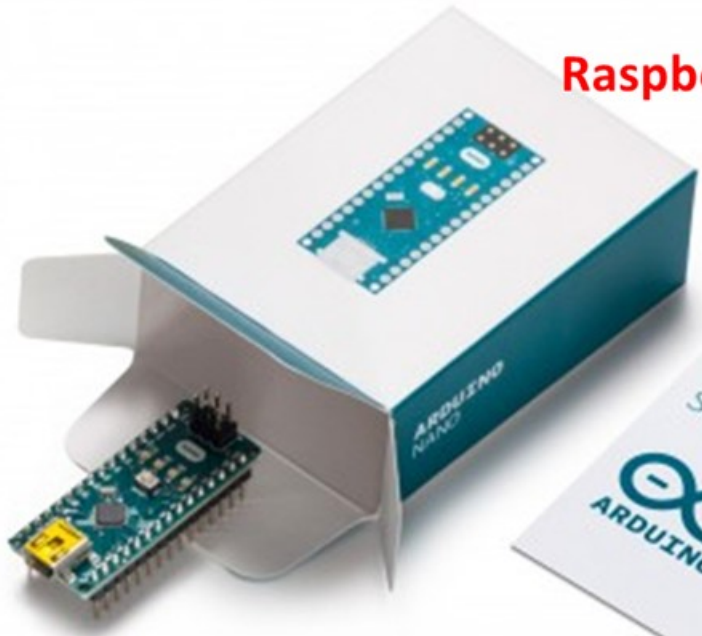
Tradeoffs of Adopting Distributed Cyber Networks

Redundancy + Resilience =>Reliability

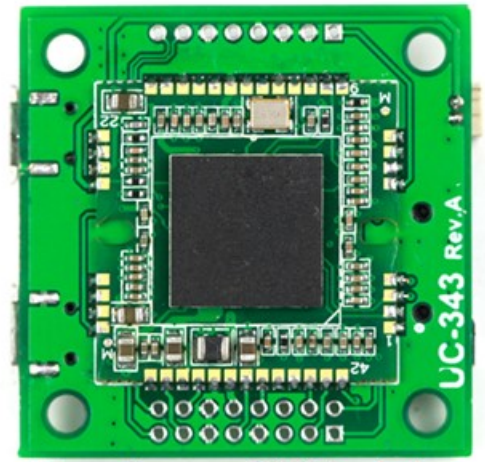
- Began during the 1950s with chemical processes, aviation, marine, telecommunications and electricity transmission (e.g. the grid is an adaptive distributed and networked supply chain)
- Efficiency gains to adoption of pervasive and adaptive process control networks
- Proliferating with as computing and remote sensing becomes another utility, i.e. "grid computing"

Proliferation of Attack Surfaces

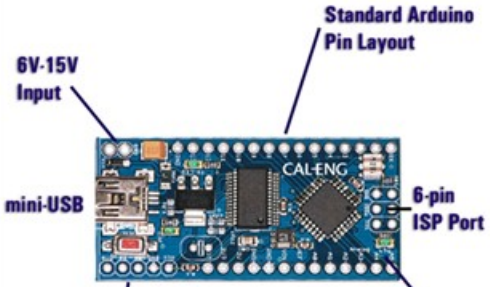
- Cybersecurity is effectively an "arms race"
  - Both ***Tactical*** and ***Strategic***
- Commercial *IoT* + *Just-in-Time* (Distributed) Supply-Chain => Amplified Knock-On Effects (i.e. Contagion)
- Risks are enormous, pervasive
- *Tort risk is nontrivial:*
  - *potential causation and damages might be deemed more foreseeable*



Raspberry Pi

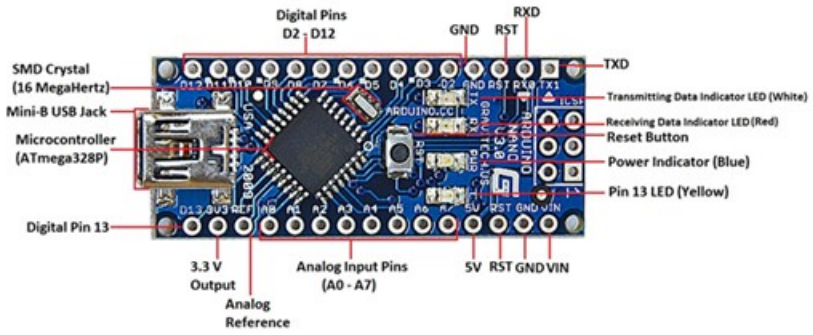


Raspberry Pi Module
(24mm x 24 mm)



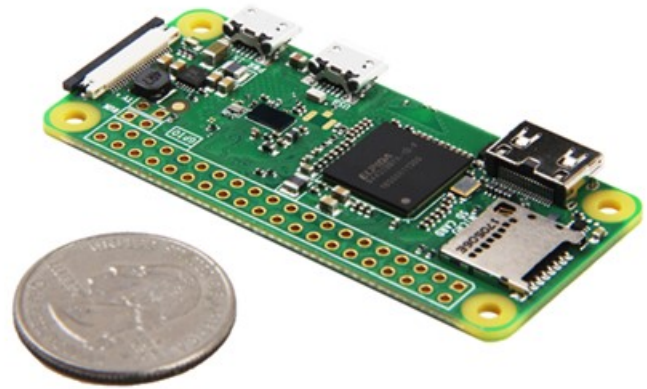
Arduino Nano

Lichee Pi Zero
The $6
Linux Computer



Arduino Nano V3.0 Pinout

www.CircuitsToday.com



UBS Adapters
(Bluetooth; Pins)

Rubber Ducky (Keystroke Injection Tool: $45)

Beagle Bone
($25-$55 Computer)

Lan Turtle (Covert Systems
Admin Penetration Tool: $55)

Malduino
(Bad USB
Firmware Hacking
Keystroke Injector)

WiFi Pineapple

Satellite Connectivity In the Palm of Your Hand

RockBLOCK 9603
Iridium SatComm
Module: $250.00

RockBLOCK Mk2
Iridium SatComm
Module: $250

Arduino Uno:
≤$5!!!

Stealing Creds From A Locked PC With the LAN Turtle

Introducing the Bash Bunny

The world's most advanced USB attack platform.

- Quad Core CPU
- Desktop-Class SSD
- Full Linux Distribution
- Payload Select Switch
- RGB LED Status Indicator
- Plug to Pwn in 7 Seconds

Bash Bunny Penetration Tool: $99.00

Advanced Attacks

- Driverless Multi-Gigabit Ethernet
- Fast USB 2.0 Storage
- Keystroke Injection
- Dedicated Serial Console

Simple Payloads

- Extendable Bunny Scripting Language
- Centralized Payload Library

BashBunny.com


GPS SPOOFER: $5
VGA
CE FC

Hack5 Field Kit: $579.00

RockBlock SatComm: $253.00

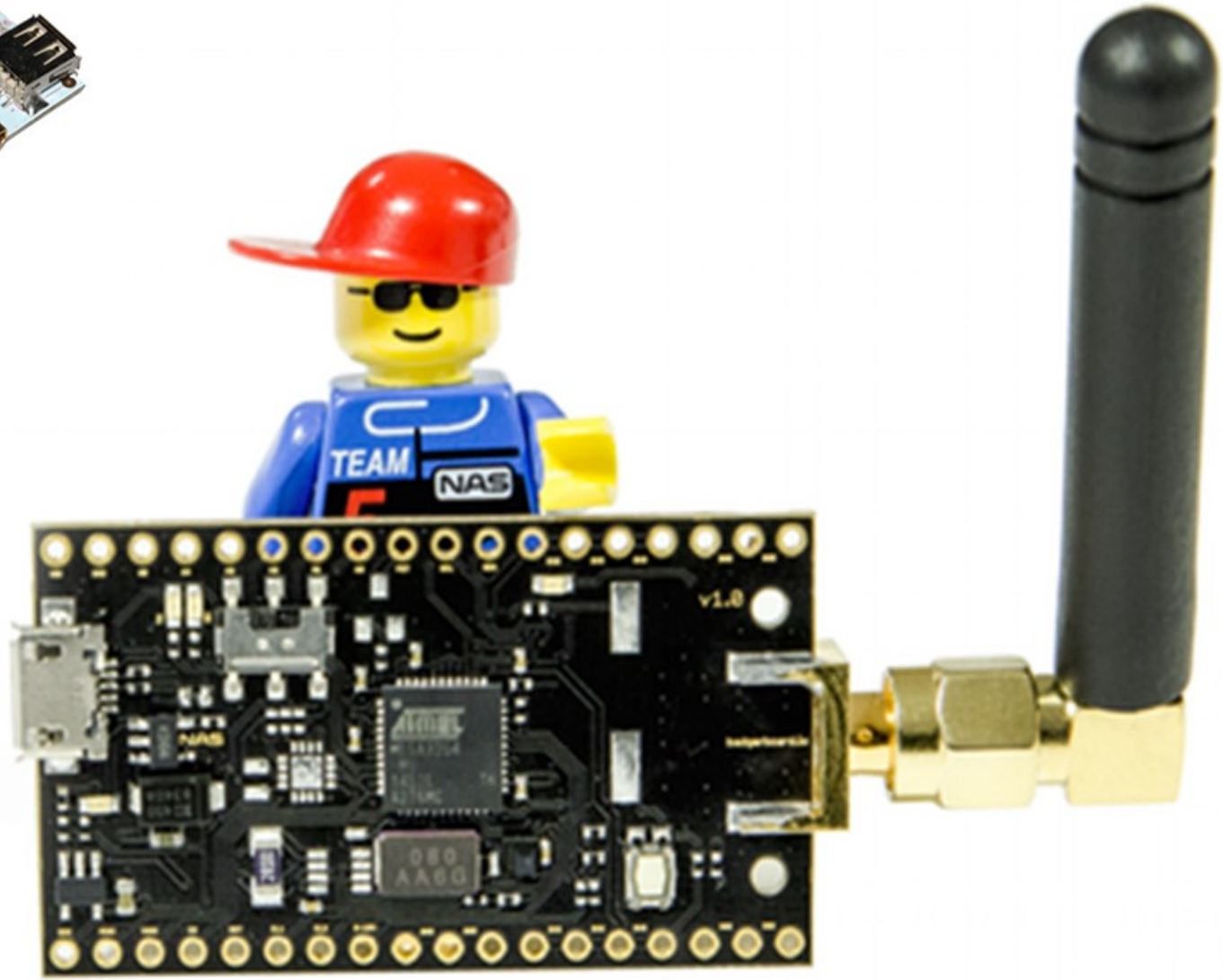
MalDuino Elite: $32.33

Hack5 Mr. Robot Toolkit

Wifi Pineapple/Bash Bunny/Rubber Ducky: $775.00

PCDuino: $59

Digispark Arduino USB Development Board ATTINY85: $1.58



BadUSB Beetle: $13.95

Adafruit Microcontroller: $6.95

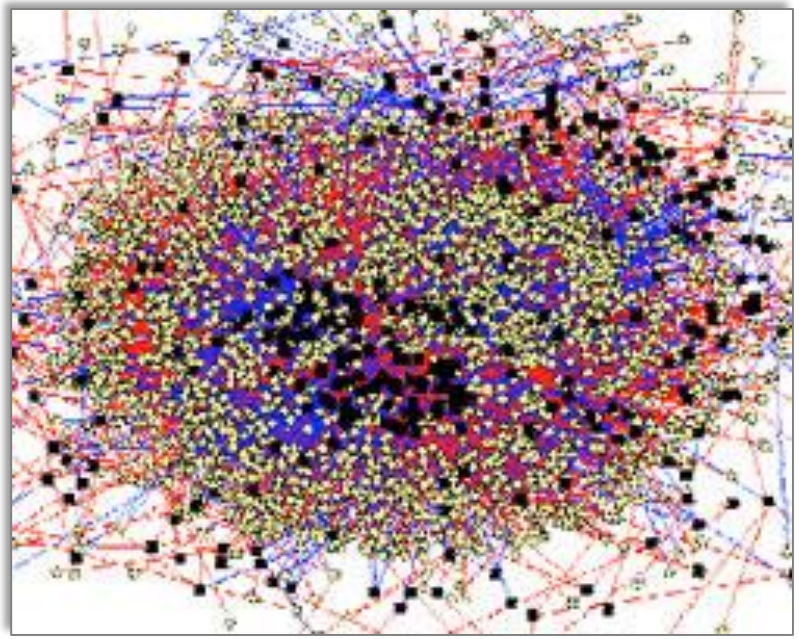
Pervasive Looming Threat of Cyberphysical Risk

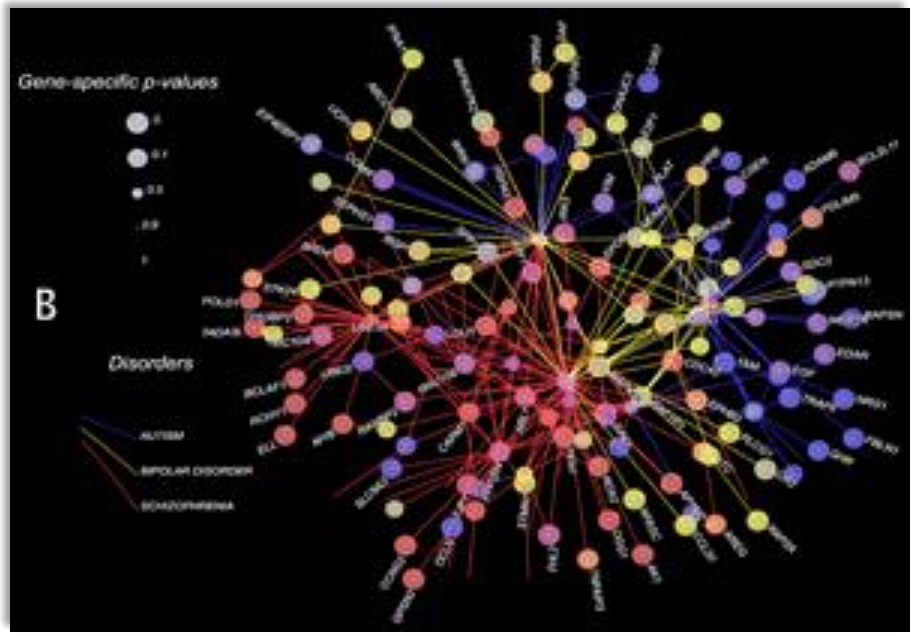
- All stakeholders and constituencies have direct and indirect physical loss exposure
  - Certain stakeholders and constituencies share more substantive and direct cyberphysical risk exposure
  - Others share cyberphysical risk exposure as a genuine threat to ongoing viability of business franchise (e.g. critical equipment failure, supply-chain and contingent business interruption)
- Where are these contingent risks currently overlooked? Everywhere!!!
- How cyberphysical risk differs from other cyber risks
  - How substantial is the threat of tort liability from customers and shareholders for failure to act
- Tactical and Strategic Cyberphysical Risk Governance is KEY!!!

Cyberphysical Risk Governance: Tech Strategy Considerations

- How should this risk exposure be measured, modeled, managed and governed?
  - The role of active ongoing system surveillance and red teams
  - Virtual scenario simulation and sensitivity analysis
  - Adaptive threat, fault, failure and conditional loss analytics
- Given the threat to ongoing viability and franchise value of firms as going concerns, who should participate in oversight and support of Risk Managers
  - What is the appropriate role and levelof engagement for the C-Suite and the board (e.g. a cyberphysical risk governance committee)?
- Are there common pitfalls to be avoided, e.g. Google Dorking?
  - When is enough security and investment enough? No Silver Bullet!!!
- What about the role of forensic surveillance of tertiary meta-data to enable active monitoring and simulation for early warning, preparedness, rapid response and recovery? Adapting and adopting well-established precedents!

Socio-Informatics: Network Analysis, Data-Mining and Text-Mining





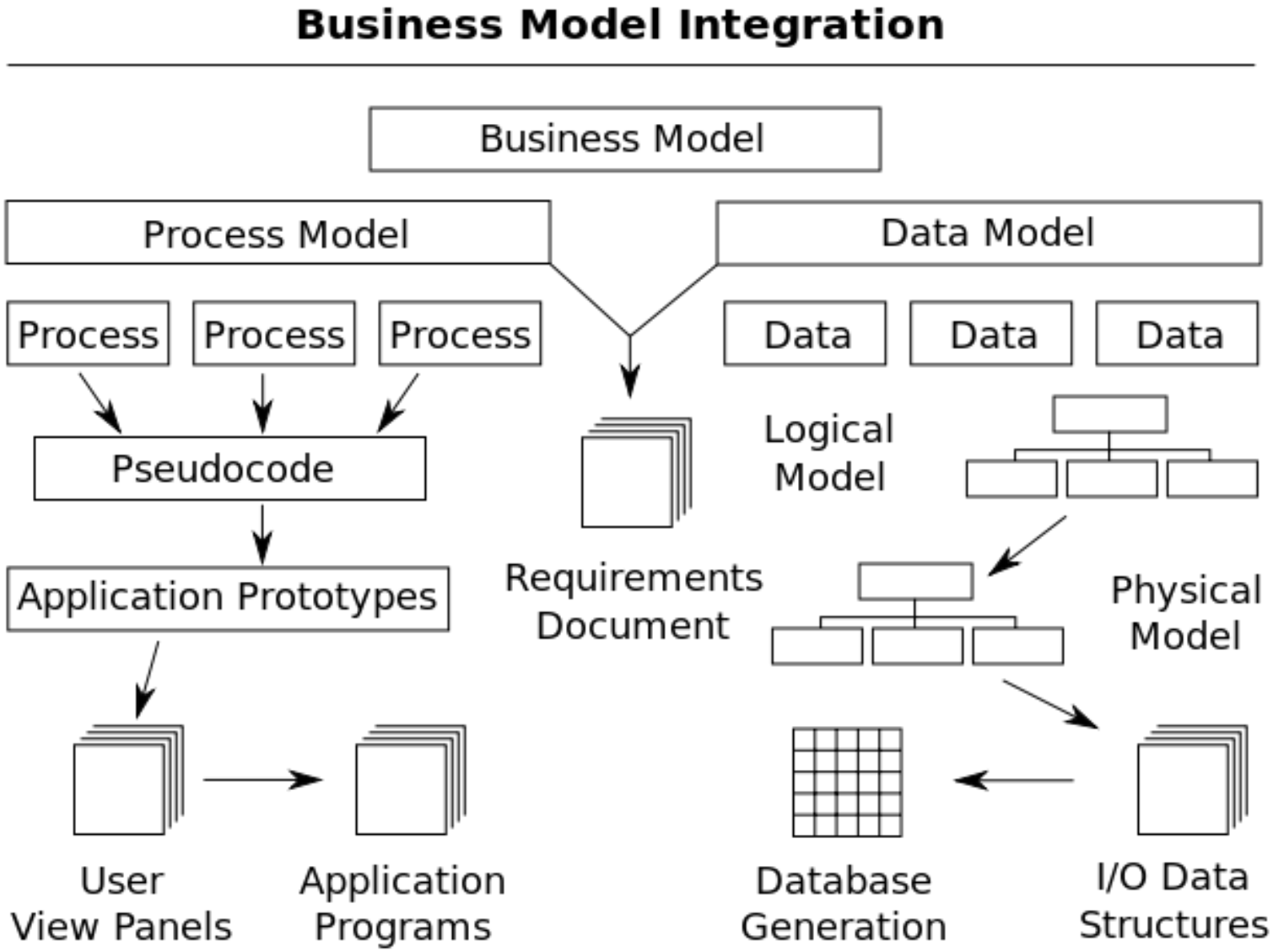
Source: CI Chicago

These analytic methods are applicable to many risks: Energy and power and **natural resource markets**; **Social systems and integrated modeling of interactions between natural and social processes**; **national security topics**, e.g. distributed adaptive network control and terrorist networks; **supply chain dynamics**; **biological systems, including pandemics**; **industrial and macroeconomic structures (trade and capital flows)**; **other geopolitical, socioeconomic**, legislative, **regulatory, commercial**, financial market and **policy issues**.

Navigating Emergent Risks in Real-Time with Scalable Data Analytics

- Harnessing massive and dynamic datasets for underwriting, pricing, loss mitigation and claims management
- The need to navigate the *Deep Web* in order to respond to the evolving risk landscape
- New ***data forensics*** i.e. metrics/analytics to explore deep structure and collective behavior, and hence reflect future dynamics
- Spatio-temporal Mapping of Metadata
  - In 2012, 2.5 exabytes (2.5 billion gigabytes) created daily; that number doubles every month)
  - In 2013, mobile data traffic = 1.4 million terabytes per month (Source: iGR); forecasted for 2014 is 2.6 million terabytes/m
  - 2018 Projections: 15.9 million terabytes per month
    - Mostly *unstructured data* (i.e. text, audio, video, usage) which requires special tools (e.g. *machine learning*)

Cyber-Physical



https://en.wikipedia.org/wiki/Business_process_modeling#/media/File:Process_and_data_modeling.svg

RiskEcon® Lab for Decision Metrics @ Courant

- The focus of RiskEcon® Lab @ Courant Institute of Mathematical Sciences, New York University (https://cims.nyu.edu/riskeconlab/), is to facilitate the development of software, analytics tools, and semantic libraries that employ high-dimensional datasets to integrate conventional data with web-enabled demographic, biometric, psychometric and sociometric data from innovative sources, by applying a range of computational and analytical methods to commercial, consumer and population-related societal trends, focusing primarily on research and development (R&D).
- Our goal is to integrate web-enabled crowdsourcing with machine learning, data-mining, and text-mining, in order to promote research fundamental to large-scale, real world questions, employing applied computational statistics, and robust and scalable data analytic solutions.
- RiskEcon® Lab for Decision Metrics was established in 2011 at Courant Institute of Mathematical Sciences, an independent division of New York University (NYU). Courant is considered to be one of the world's leading mathematics educational and scientific research centers, and has been ranked first in research in applied mathematics. RiskEcon® Lab is the cornerstone of the Computational Economics and Algorithmic Data Analytics (CEcADA) cooperative at New York University, established concurrently in 2011.

Numerati Partners LLC

The mission of Numerati® Partners LLC is to manage privately-held data analytics investment and development consortia in order to curate the next generation of scalable data-intensive risk and liability management enterprises, by providing resources critical to accelerating the development of nascent leading-edge inferential surveillance, monitoring, and cyberphysical distributed network analytics technologies for deployment in forensic domains of *RiskTech*, *LitTech* and *FinTech* (i.e. risk technology, litigation technology and financial technology).

Numerati-affiliated consortia curate and commercialize domain-specific use-case applications via systems integration and managed service provider platforms, by employing fully-integrated, risk technology-oriented domain-specific and customized data analytics-driven enterprise solutions, i.e. *Solutions-as-a-Service* (SolaaS) that implement and maintain use-case applications via proprietary value-added reseller arrangements of *Software-as-a-Service* (SaaS), *Infrastructure-as-a-Service* (IaaS), *Platform-as-a-Service* (PaaS) functionality.

RiskEcon® & Numerati® Eco-System

- RiskEcon® Lab for Decision Metrics @ New York University
- Courant Institute of Mathematical Sciences
- General descriptions of other participants:
  - Cyberphysical risk engineering (telematics) spinoff (CEO formerly engaged with Batelle, DARPA and other programs)
  - Global leader in economic regulatory analysis, liability, litigation-risk, causation and damages analysis
  - Social media surveillance and monitoring development teams
  - Wearable tech (telemetrics) monitoring development team
  - Remote-sensing platforms (cellular, satellite, etc.)
  - Leading global Technology Infrastructure-as-a-Service providers
  - AFL-CIO leadership
  - Governmental agencies (e.g. NOAA, NTSB, DOT, etc)
  - NGOs (agriculture, environmental and conservation science, etc.)
  - Other Academic Research Institutions, Financial and Technology Industry Participants …

David K.A. Mordecai
Samantha Kappagoda

RiskEcon® Lab for Decision Metrics @ NYU Courant
Numerati® Partners LLC
Risk Economics®, Inc.