SYSTEMS ENGINEERING RESEARCH CENTER

SERC TALKS

WELCOME

How Can We Systems Engineer Trust into Increasingly Autonomous Cyber-Physical Systems?

February 5, 2020 | 2:00 PM ET

Dr. Joseph Mitola III, Chief Technologist, Aerospace Sciences and Engineering (ASE) Division, ENSCO, Inc

Mitola.Joe@ensco.com

- Today's session will be recorded.
- An archive of today's talk will be available at: www.sercuarc.org/serc-talks/ as well as on the SERC YouTube channel.
- Use the Q&A box to queue questions, reserving the chat box for comments, and questions will be answered during the last 5-10 minutes of the session.
- If you are connected via the dial-in information only, please email questions or comments to SERCtalks@stevens.edu.
- Any issues? Use the chat feature for any technical difficulties or other comments, or email SERCtalks@stevens.edu.

How Can We Systems Engineer Trust into Increasingly Autonomous Cyber-Physical Systems?

5 February 2020

Dr. Joseph Mitola III, Chief Technologist
Aerospace Sciences and Engineering (ASE) Division
ENSCO, Inc., Cocoa Beach, Florida

Agenda

- Motivation: Autonomous Cyberphysical Systems
- Hardware-software Foundations of Trust
- Counter-cultural COTS Dataflow Computing Zeroizes Network Attack Surfaces
- Systems Engineering
  - Challenges
  - Enhancing SE processes
  - Opportunities

ENSCO®

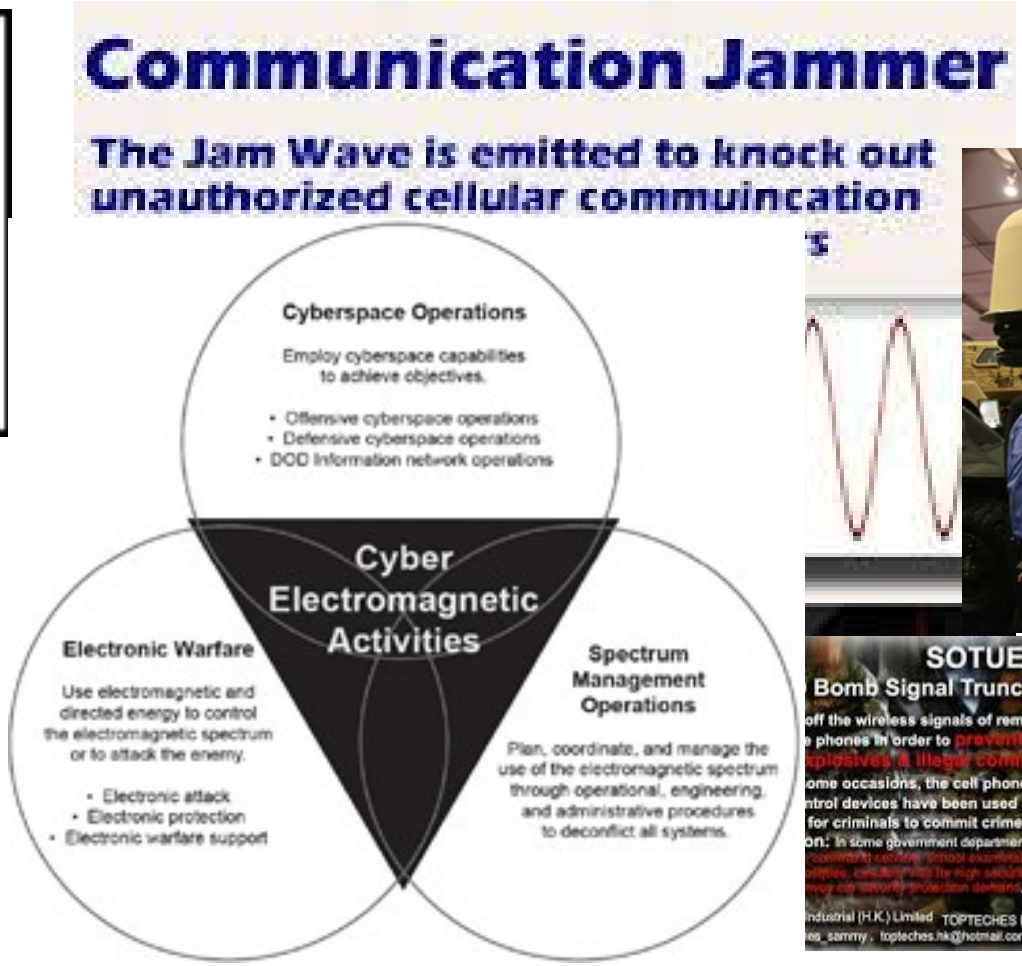
ANGEL Has Fallen?

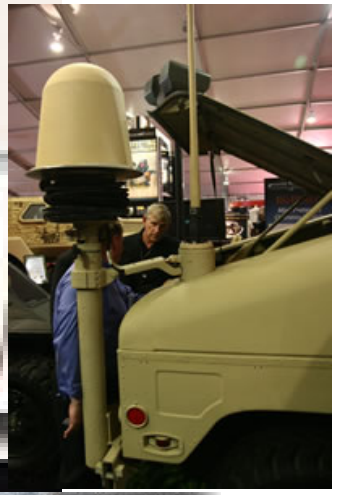
Self-Driving Tanks, Machine Guns and Spacecraft (Theirs and Ours)

The Adversaries that are selling these weapons on-line are bringing *Autonomy to Weapons in EW-Cyber Contested Environments*

Autonomy in EW-Cyber (CEMA)

US Army Field Manual 3-38 ***Cyber Electromagnetic Activities (CEMA)*** 2014

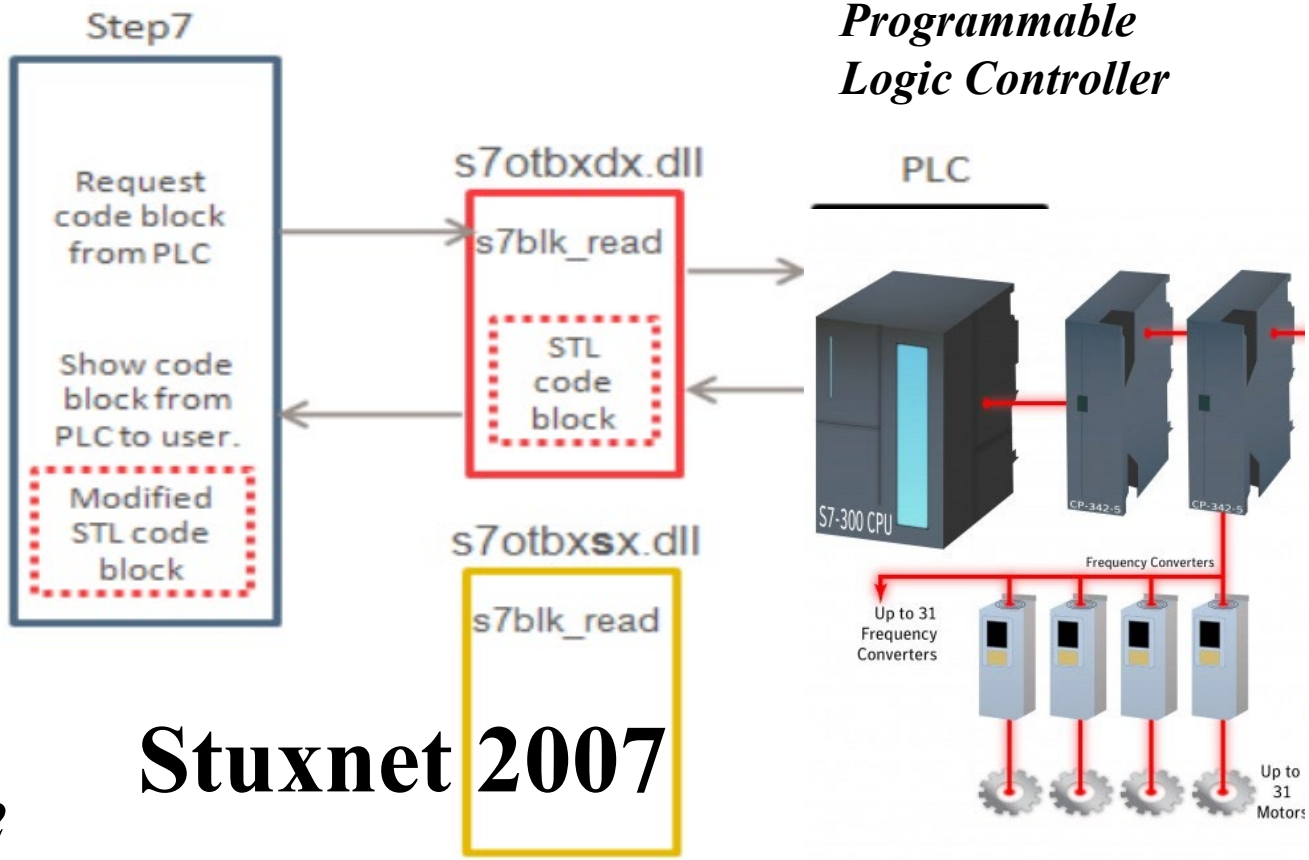




Land-Sea-Air-Space-Cyberspace

Advanced Persistent Threat (APT)

Operators in front of the Cascade Protection System

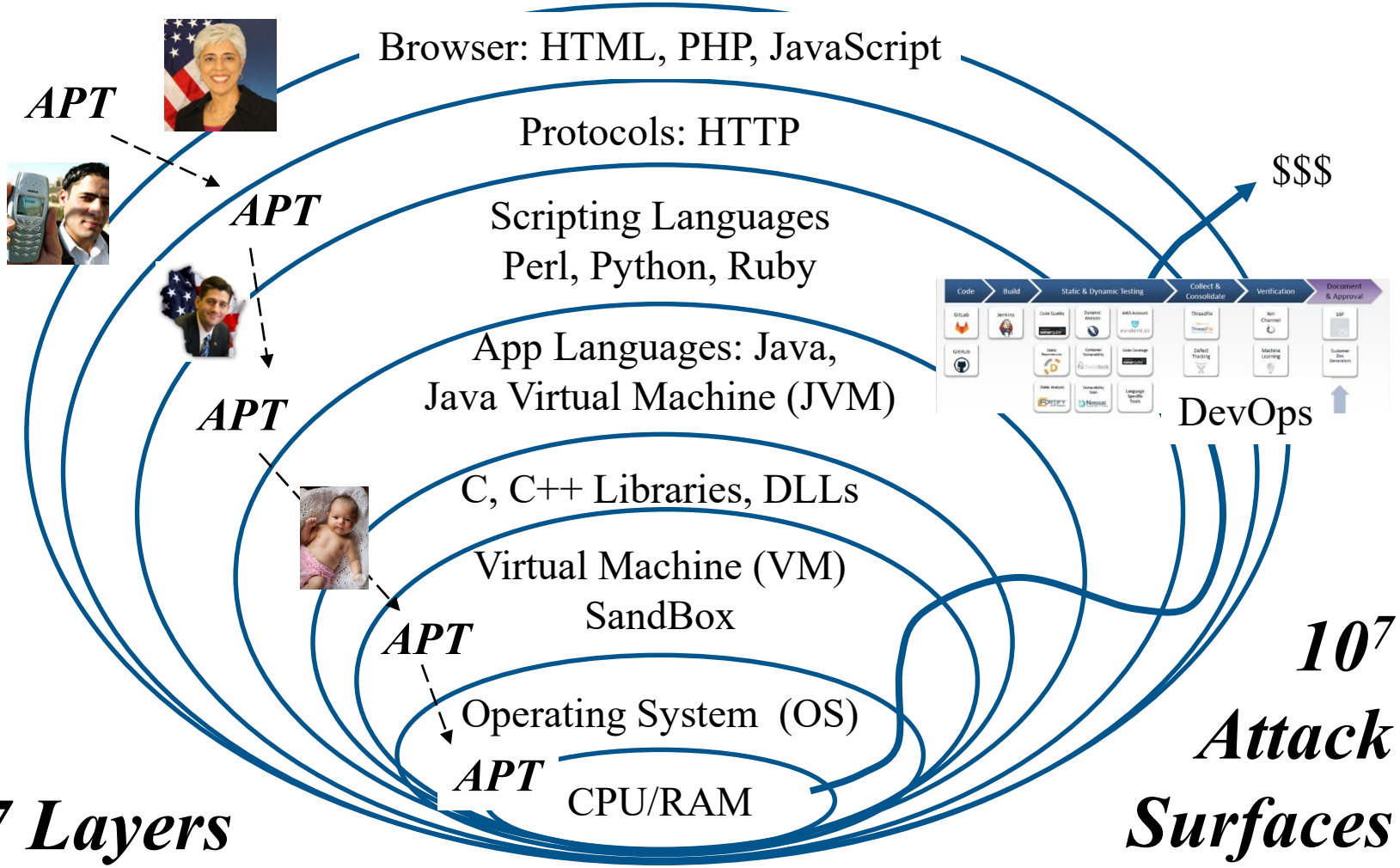


Programmable Logic Controller

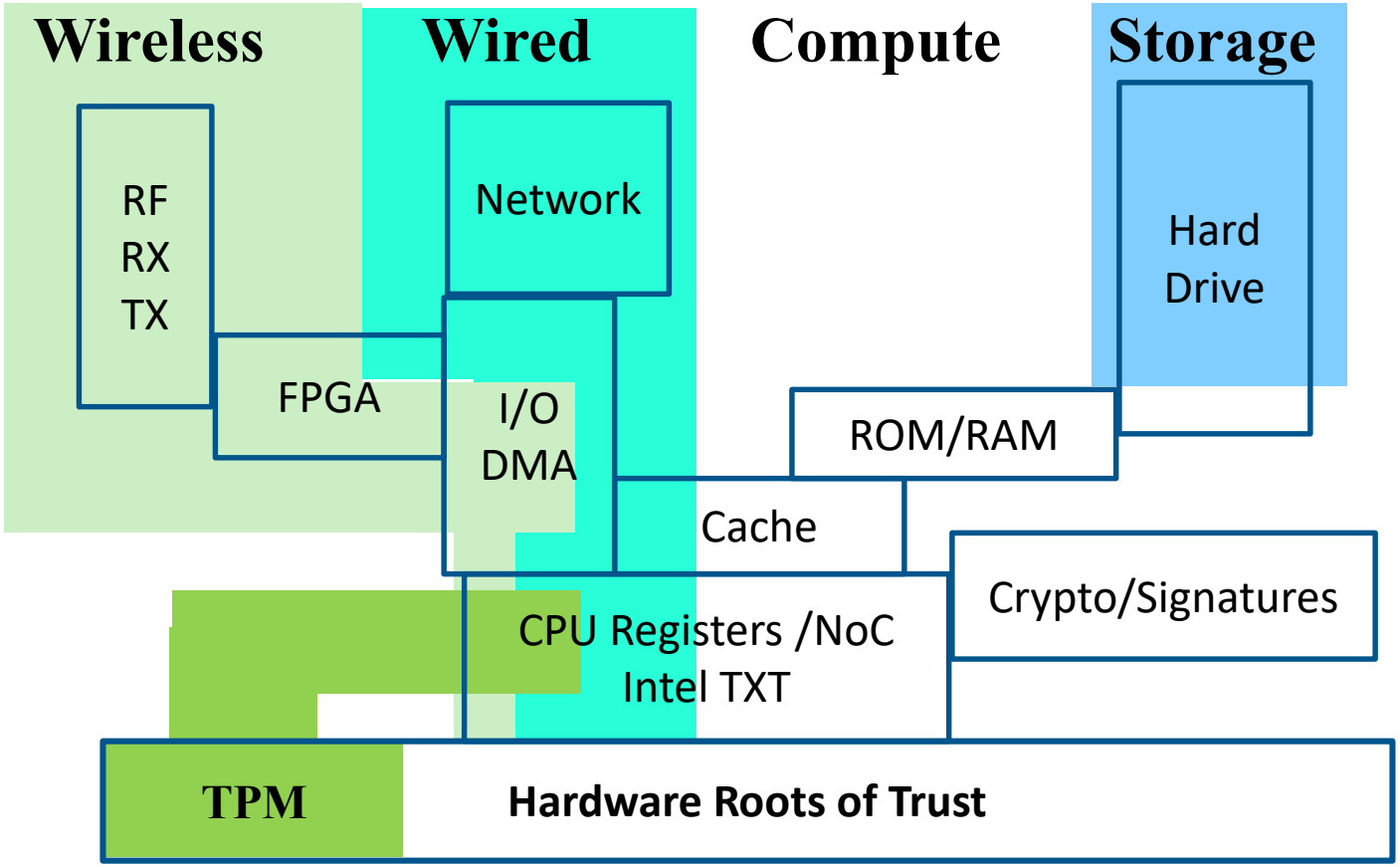
Fire Eye APTs
Symantec, IBM
Palo Alto Code 42
Threat Intelligence

Stuxnet 2007

Software Layering Exponentiates Cyber Attack Surfaces

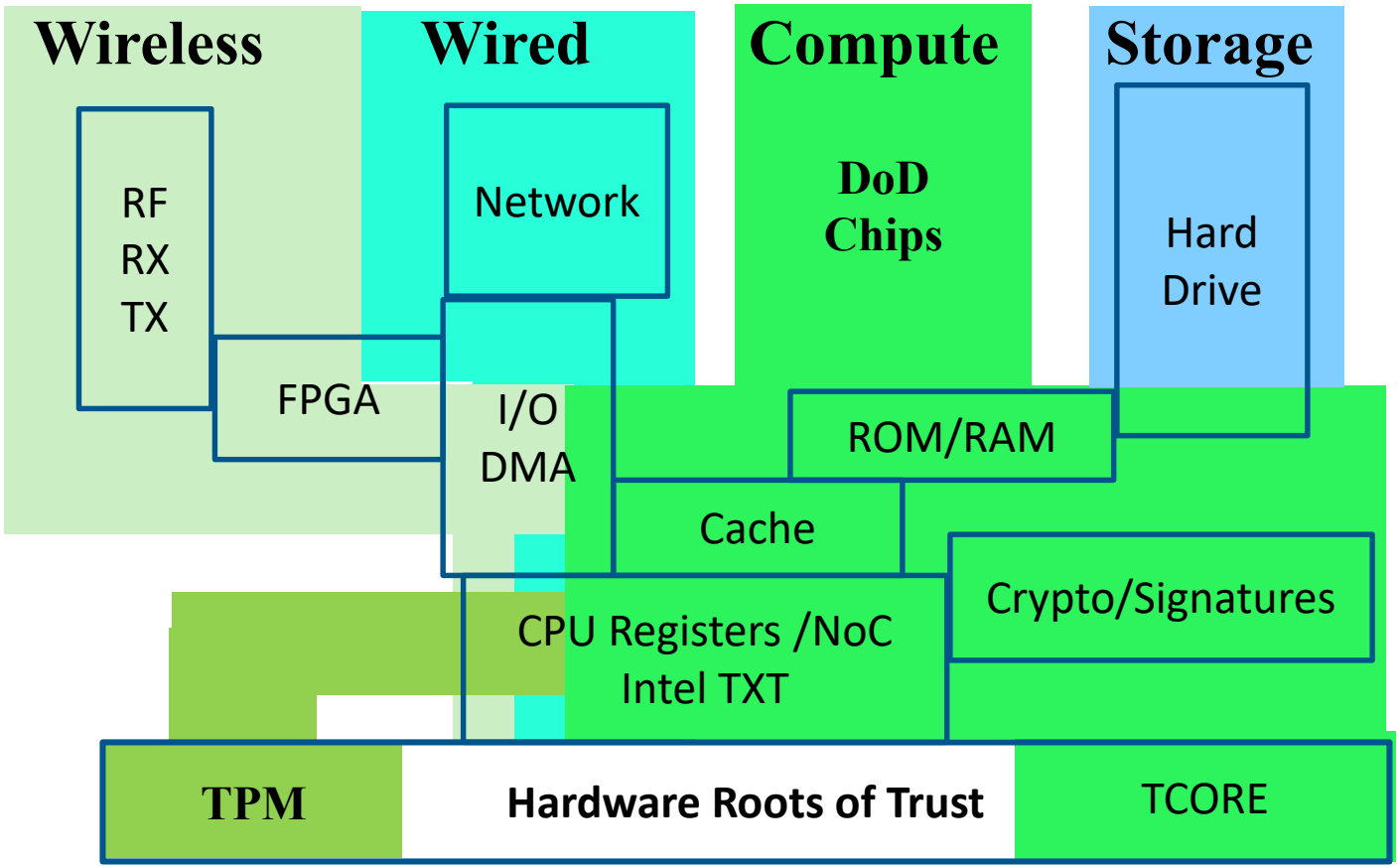


Hardware Cyber Hardening



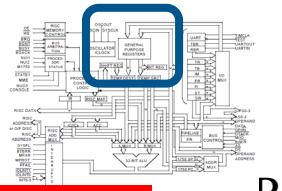
Trusted Platform Module (TPM)

Hardware Cyber Hardening



Protecting COTS CPUs is Impossible

COTS von Neumann Stored-program CPU Architecture Cannot Be Guaranteed Safe()



Unsafe({R})

Monitor Functions

Mon(1)
Mon (2)
…
Mon (j)
Mon (j+1)

Safe({R})

$\{R\}_0$ $\{R\}_1$ $\{R\}_2$ *Recursively Enumerable Sequence* $\{R\}_i$ → i

0	0	0	….	1	1	1	0	…
0	1	0	….	1	1	0	1	…
0	1	1	…	1	1	0	0	…

Proof by Cantor Diagonalization (1839)

Diagonal(Ex4(j, i=j)) = (0,1,1, …)

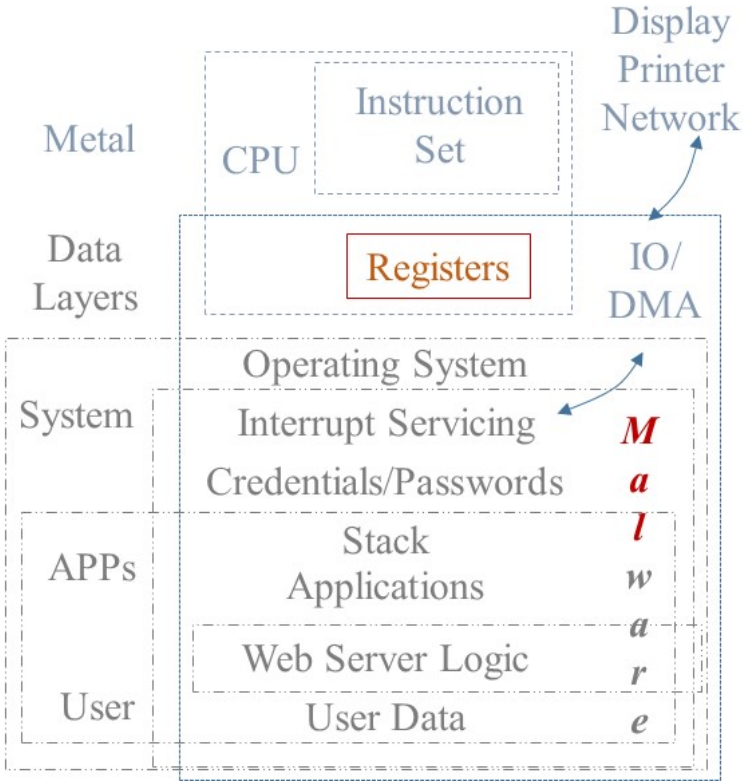
Not(Diagonal(Ex4(j, i=j))) = **(1,0,0, …)** $\notin$ Mon*

*Power Set of Safe($\{R\}_i$) **is not decidable** $\Rightarrow$ Monitor(Rj) can **never** be complete*

Hackers [Erickson] "Bits are bits"

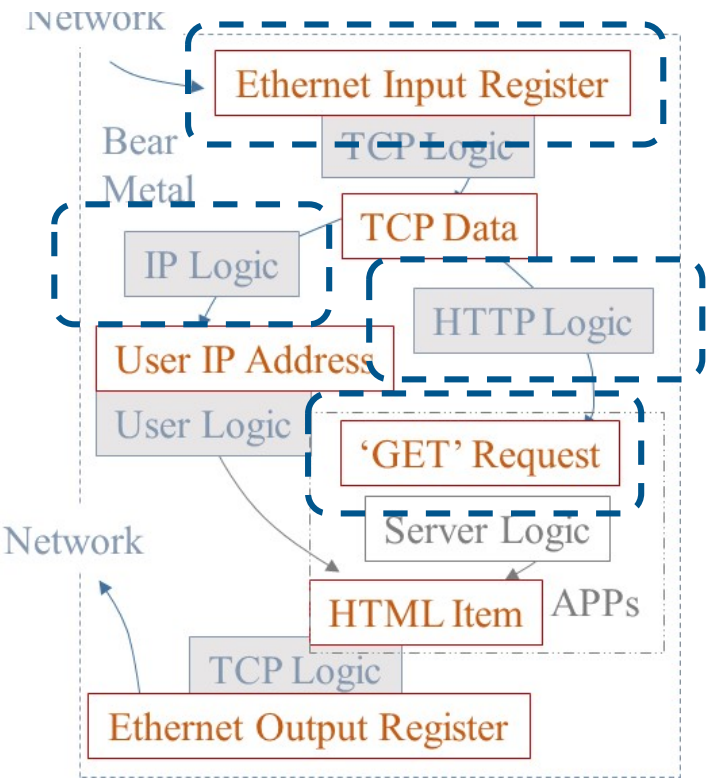
Pure Dataflow Pipeline Safe Alternative

COTS/GOTS



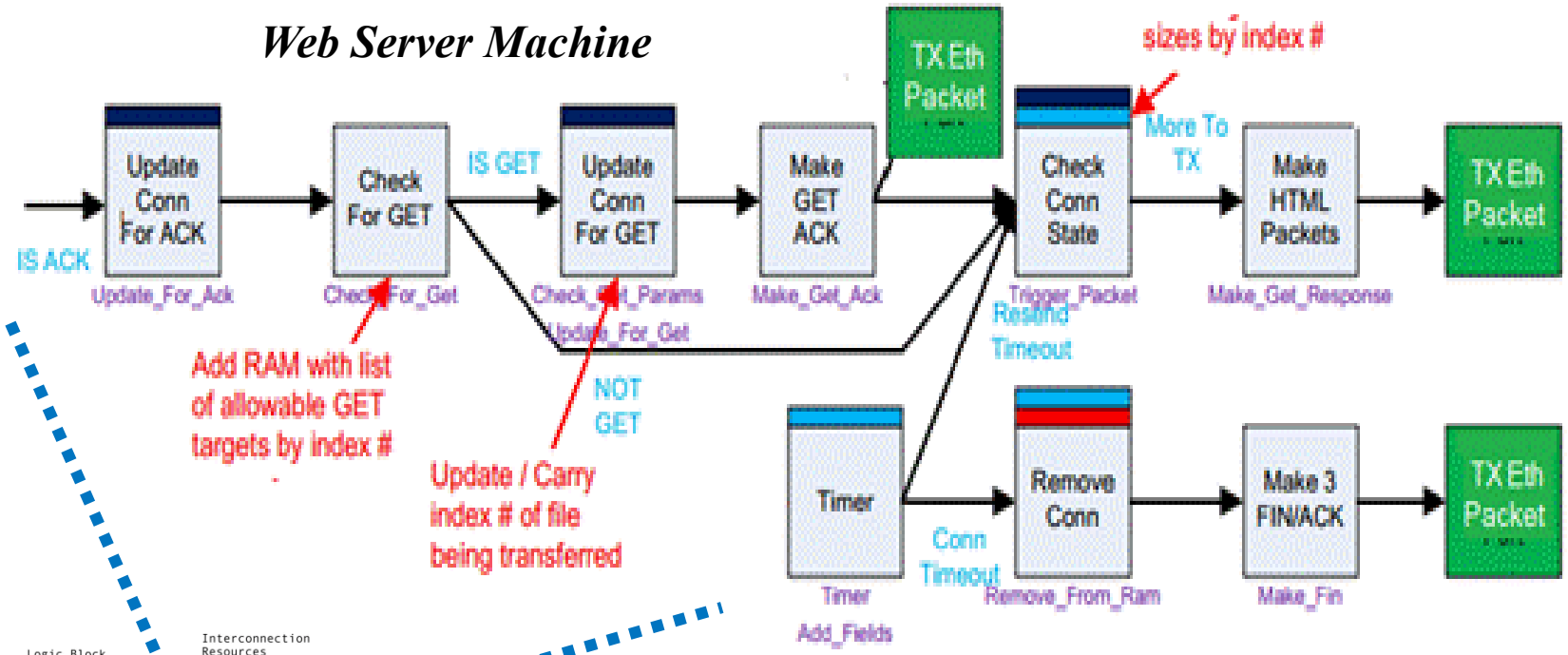
150 Watts, 100k CVE

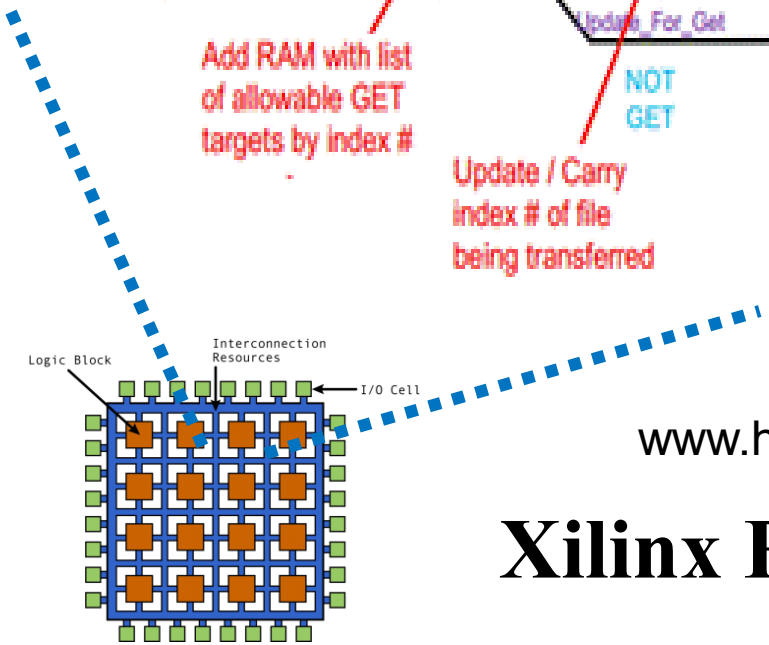
"Pure" Dataflow



40 Watts, 0 CVE

Pure Dataflow Web Server 2014-2020



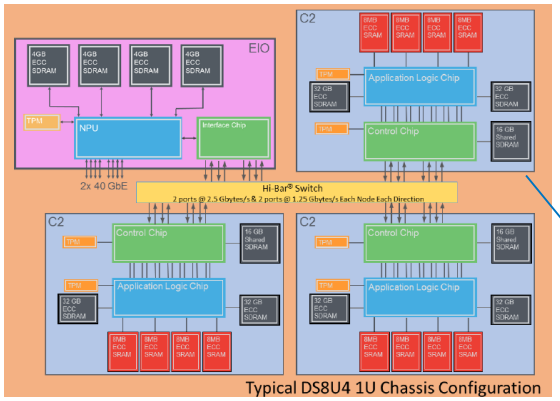


www.hackprooftechnologies.com

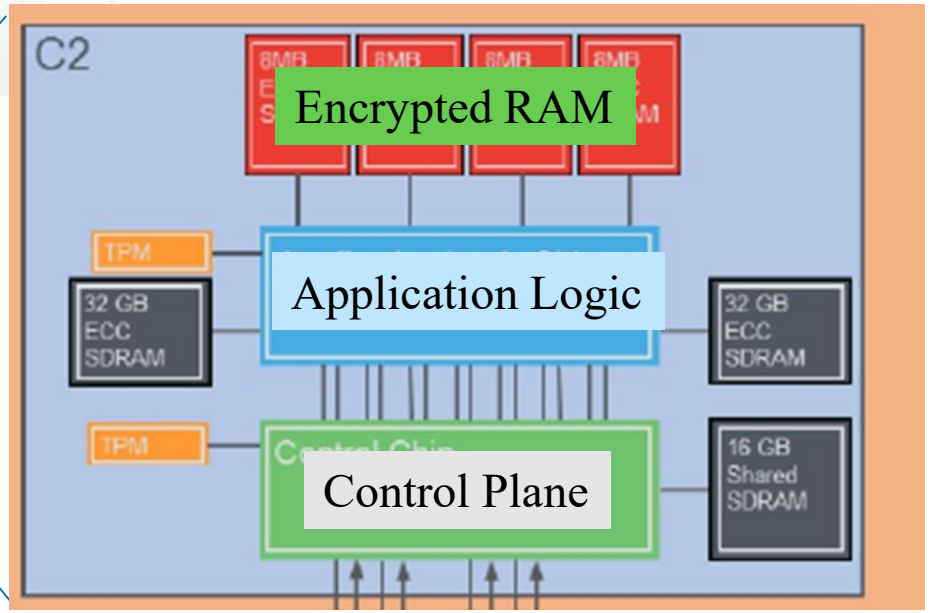
Xilinx FPGA (1/4 of chip)

Pure Dataflow COTS

DirectStream DS8U4

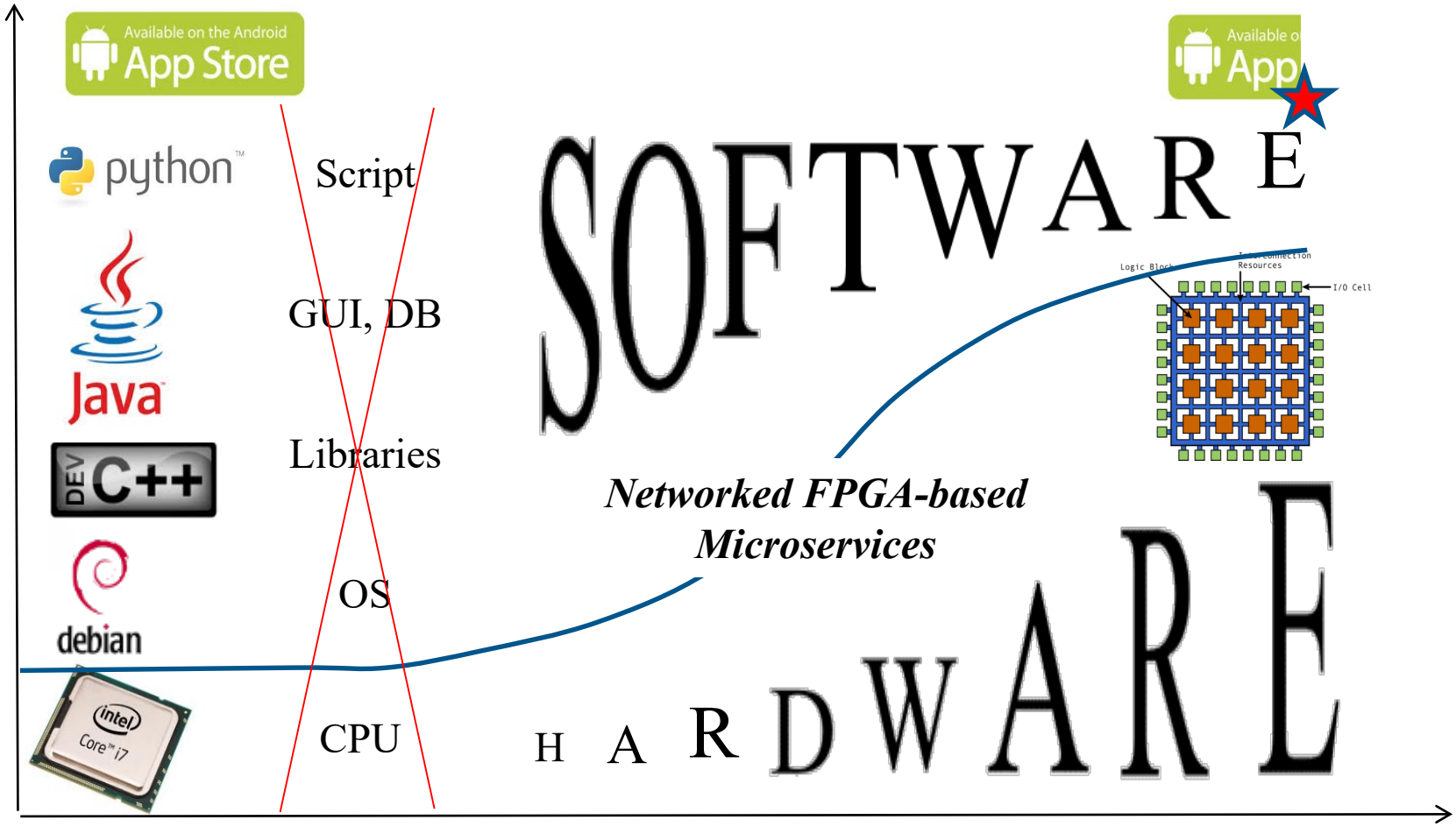


Typical DS8U4 1U Chassis Configuration

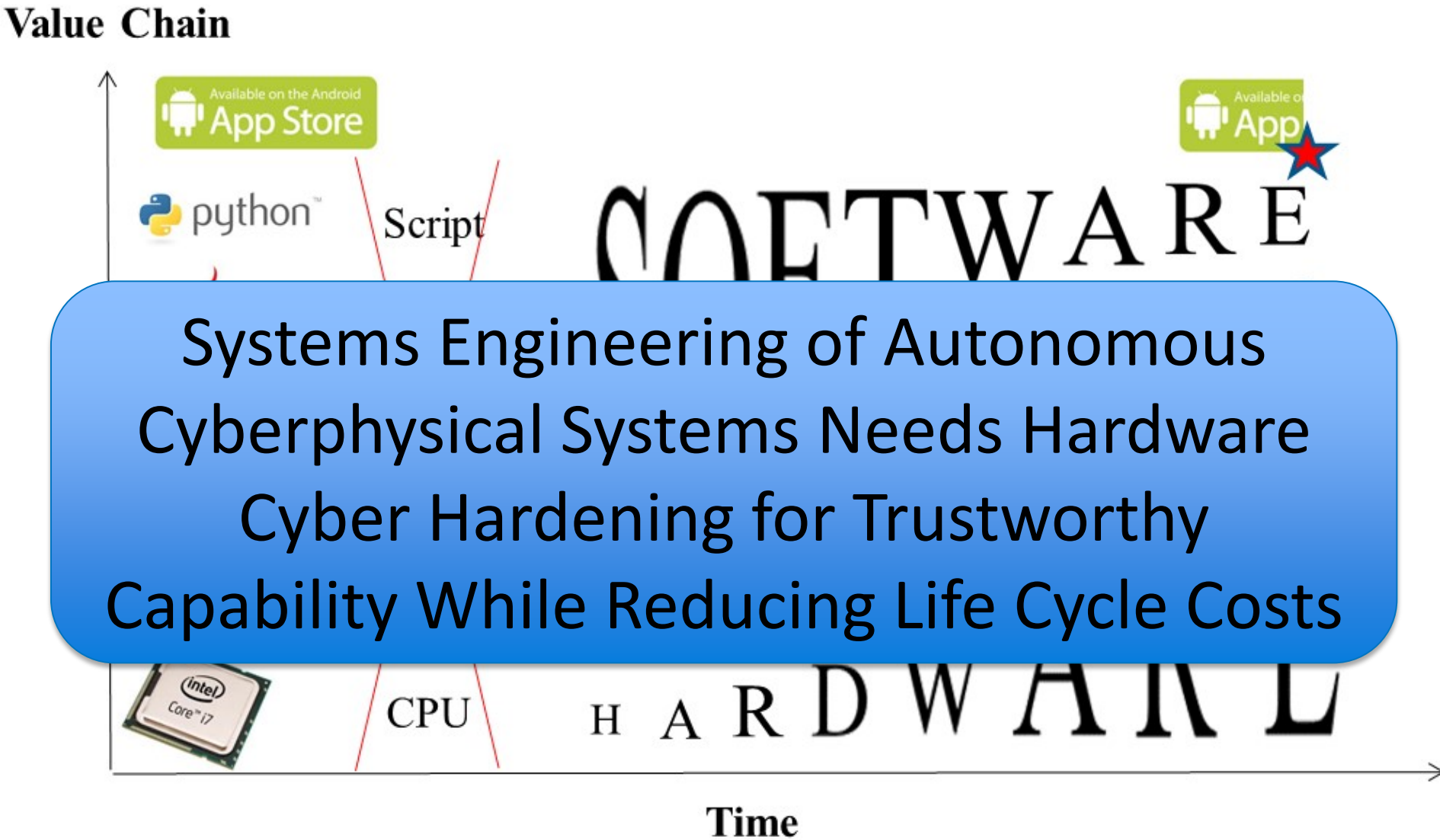


Trustworthy Autonomous Systems

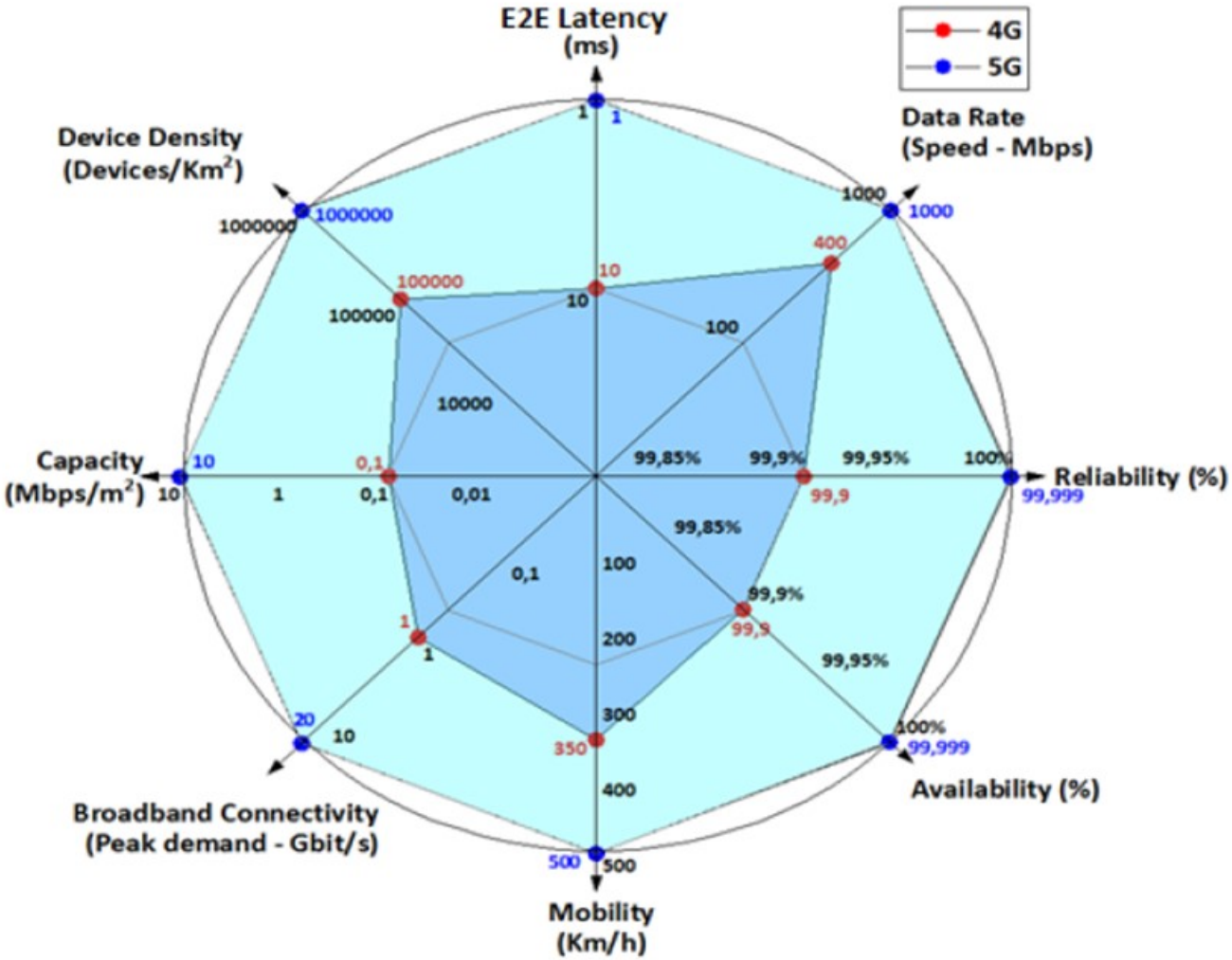
Value Chain



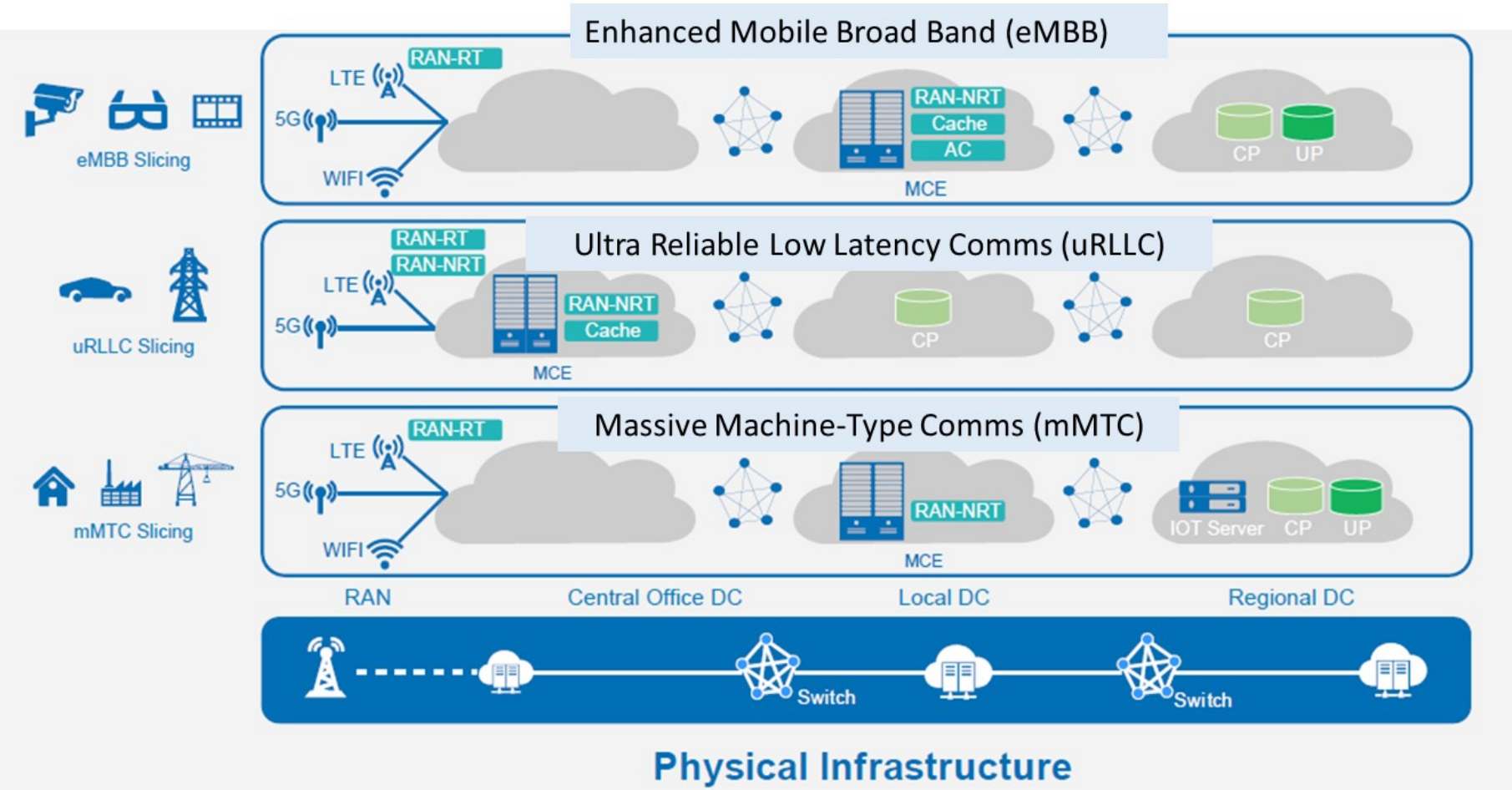
Trustworthy Autonomous Systems



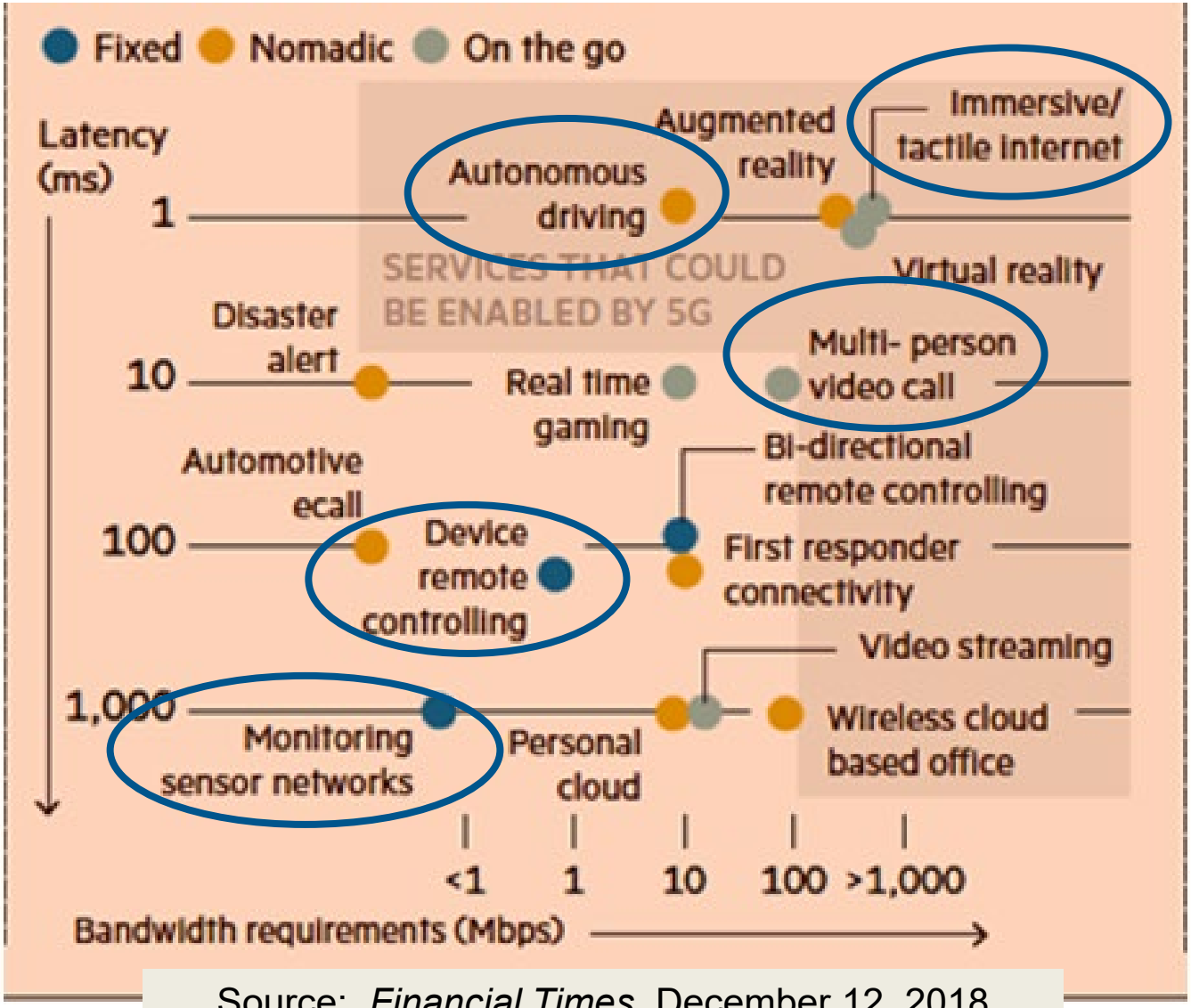
Networking Autonomous Swarms
5G vs. 4G



5G Network Slicing

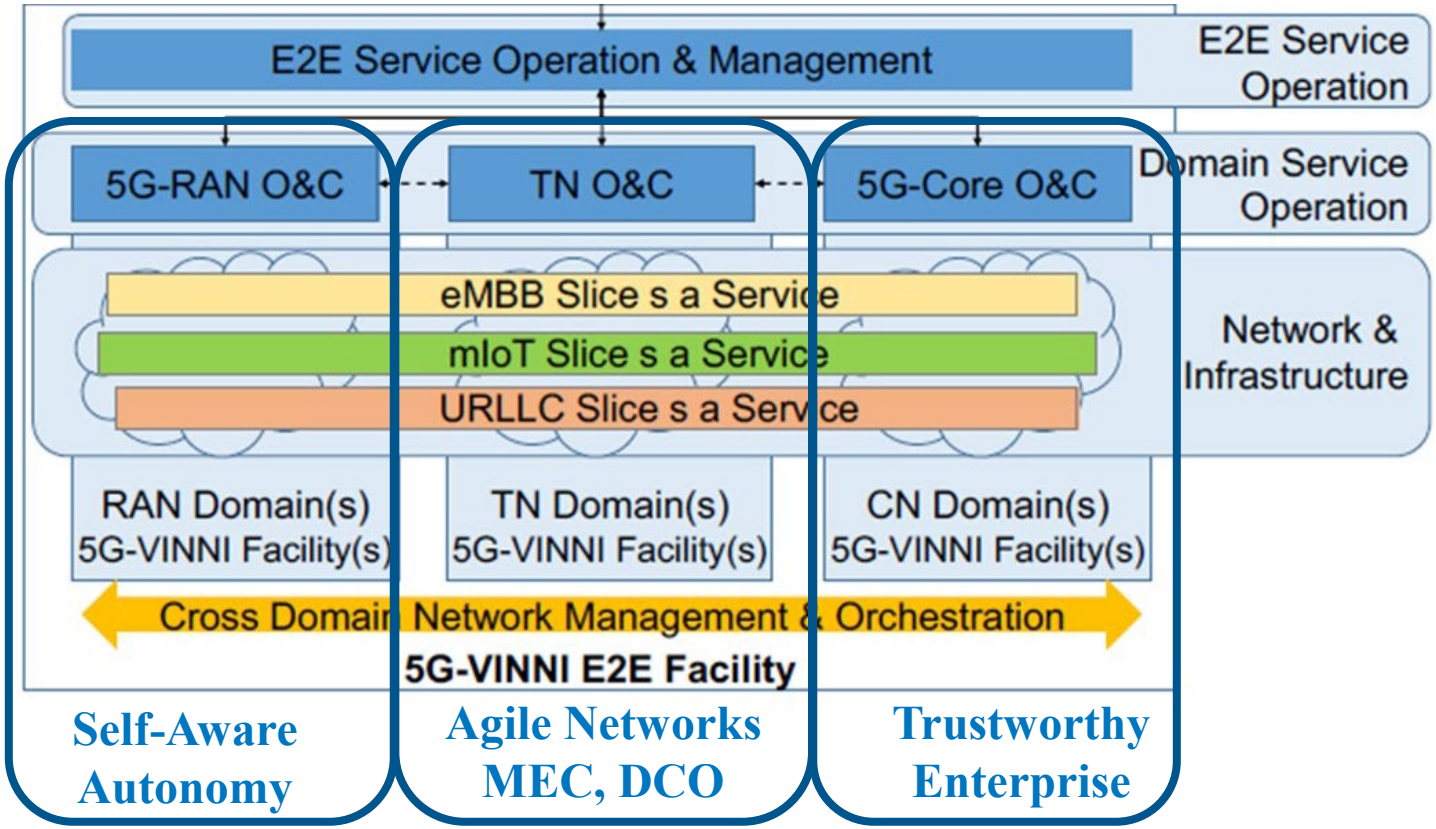


Autonomy Enablers from 5G



Source: *Financial Times*, December 12, 2018

Orchestrating 5G for Trustworthy Autonomous System of Systems



TN – Transport Networks CN-Core Network; VINNI – Virtual Network
DCO Defensive Cyber Operations; MEC – Mobile Edge Computing

ENSCO®

Systems Engineering Challenges

- Pure Dataflow (No CPU/OS) is Counter-cultural
  - CPUs are OK at design time, but not at runtime
  - DirectStream data plane / control plane / antitamper
  - DoD could support the nascent dataflow ecosystem
- Systems Engineers Should “Require”
  - Entity Self-awareness
  - Domain specifications for domain-based
  - Hardware-based Machine DNA
  - Hardware self-checking
- Systems Engineer Multisensory Awareness
  - Dead reckoning, visual awareness, GPS
    - Makes GPS spoofing much more difficult
  - Apply to mission-critical requirements

ENSCO®

Systems Engineering for Trustworthy Autonomy

- Functions
  - Enduring (“requirements”)
  - Self-aware, user-aware, social animal
- Component Specifications
  - Hardware: sub-Turing, self sensing & limiting
  - Software: dataflow cross-compilers
- Design Rules
  - Allocate functions to components
  - Require clarity (IETF)
  - Require practical modularity
    - “Structured Design” ⇔ Microservices

ENSCO®

Systems Engineering Opportunities

- Demonstrate Trustworthy Autonomous Systems
  - Autonomous cell phone would
    - Know who you are and what you do
    - Assist you with mobility, banking, fitness, health
    - ***Would NOT tell the network*** or anybody else
- Define OODA-loop architectures for Σ AI/ML
- Global collaboration?
- SERC Research Directions?
  - Discussion

ENSCO®

Supplementary Material

SERC Research Review 2020: Save-the-Date

NEW LOCATION:
NATIONAL PRESS CLUB
529 14TH ST. NW, 13TH FLOOR
WASHINGTON, DC 20045

SAVE THE DATE
17-18 NOVEMBER

SERC 2020
SPONSOR
RESEARCH
REVIEW

For more information, contact Monica Brito: mbrito@stevens.edu

Visit our website for more information: https://sercuarc.org/research-reviews/

SERC TALKS

UPCOMING TALKS:

"Autonomy and Trust for Cyber-Physical Systems" Series

April 1, 2020 | 2:00 PM ET

Dr. Jeff Voas, Computer Scientist, US National Institute of Standards and Technology (NIST); co-founder of Cigital, now part of Synopsys

June 3, 2020 | 2:00 PM ET

Dr. Martin Törngren, Professor, Department of Machine Design (MMK), KTH Royal Institute of Technology

CONTACT

Editor-in-Chief: Dr. Barry Boehm, University of Southern California – boehm@usc.edu

Webinar Coordinator: Ms. Mimi Marcus, Stevens Institute of Technology – mmarcus@stevens.edu

Please visit the SERC Talks page to register and for more information and updates.

SERC TALKS

Thank you for joining us!

Please check back on the SERC website for today's recording and future SERC Talks information.

Subscribe and follow SERC on our social channels: