NIST IoT-AB Meeting (18-19 April)

Cyber-SCRM perspectives

Don Davidson, Director Cyber-SCRM
Synopsys, Inc. don.davidson@synopsys.com

18 April 2023

Don Davidson, Synopsys Director for C-SCRM since 2019

- 44+years US Government Federal Service (Military & USG/DoD civilian)
- Masters Degree in National Security Strategy, concentrated in Information Resource Management from US National Defense University
- Co-Author “Knowledge Enabled Logistics” on DoD classic SCRM (2004)
- Led US Dept of Defense ICT/Cyber-SCRM program, 2009-2019 under CNCI-SCRM
- “Quoted” in the 2019 National Security Telecommunications Advisory Committee (NSTAC) Report to the President on “Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem”. *“With respect to ensuring we have the ability to assess whether ICT products are trustworthy…We need to evolve the science and the standard.”* Don Davidson, Synopsys
- Selected as a Cyber-SCRM Fellow at the Institute for Critical Infrastructure Technology https://icitech.org/ .

  https://www.linkedin.com/posts/parhamtech_he-helped-write-the-book-on-how-to-improve-activity-7036106572107763712-ZA3O/?originalSubdomain=lk
- Selected to the DOC/BIS- ISTAC in Dec 2021.
- Selected to co-lead NDIA Cybersecurity Division’s Cyber-SCRM Committee.

Comprehensive National Cybersecurity Initiative (CNCI)

Focus Area 1

- Trusted Internet Connections
- Deploy Passive Sensors Across Federal Systems
- Pursue Deployment of Intrusion Prevention System

  (Dynamic Defense)
- Coordinate and Redirect R&D Efforts

Establish a front line of defense

Focus Area 2

- Connect Current Centers to Enhance Cyber Situational Awareness
- Develop a Government Wide Cyber Counterintelligence Plan
- Increase the Security of the Classified Networks
- Expand Education

Demonstrate resolve to secure U.S. cyberspace & set conditions for long-term success

Focus Area 3

- Define and Develop Enduring Leap Ahead Technology, Strategies & Programs
- Define and Develop Enduring Deterrence Strategies & Programs
- Develop Multi-Pronged Approach for Global Supply Chain Risk Management
- Define the Federal Role for Extending Cybersecurity into Critical Infrastructure Domains

Shape the future environment to demonstrate resolve to secure U.S. technological advantage and address new attack and defend vectors

Ensuring Confidence in Defense Systems

- *Threat*: Nation-state, terrorist, criminal, or rogue developer who:
  - Gain control of systems through supply chain opportunities
  - Exploit vulnerabilities remotely
- *Vulnerabilities*
  - All systems, networks, and applications
  - Intentionally implanted logic
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- *Traditional Consequences*: Loss of critical data and technology
- *Emerging Consequences*: Exploitation of manufacturing and supply chain
- Either can result in corruption; loss of confidence in critical warfighting capability

Today's acquisition environment drives the increased emphasis:

Then		Now
Stand-alone systems	>>>	Networked systems, IT / OT
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers
CPI (technologies)	>>>	CPI and critical components

DoD Strategy for Trusted Systems and Networks/SCRM

1. Understand system criticality and prioritize limited resources
   - Focus on National Security Systems: Mission Critical Systems -and classified networks
2. Within priority systems, strengthen systems security engineering practices to identify and protect mission critical functions and their critical components
3. For critical components, utilize all-source supply chain threat assessments from DIA SCRM Threat Assessment Center to inform risk management strategies
4. Manage risk to critical components throughout the acquisition lifecycle through acquisition *program protection* and SCRM by:
   - Proactive SCRM key practices to strengthen acquisition operations security
   - Trusted supply chain for DoD unique Application Specific Integrated Circuits (ASICs)
   - Employ technical mitigations and enhanced vulnerability detection
5. Partner with industry to drive security (manufacturing, engineering, test and evaluation, etc.)

Existing and Emerging SCRM Research, Policy, Standards and Practices

Government

CNCI Stood Up

Software & Supply Chain Assurance (SSCA) Forum (Public-Private Partnership)

DoD ICT SCRM Key Practices

UMD Research

NIST IR 7622

GAO Report

Sec 515/516 for CJS

EO13636 Report

PMOs developed in DOJ, DOE and DOC

Cybersecurity Framework And Roadmap

Industry Best Practices

NIST SP 800-161

NIST SP 800-171

CNSSD 505 Update

OMB Circular A-130

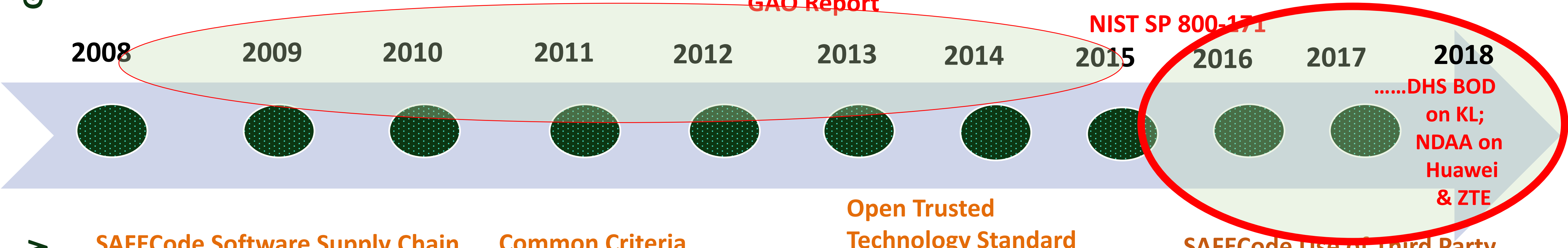
Risk Analytics

Metrics White Paper

Draft CSF v1.1

China TC260: GB C-SCRM Standard

NIST IR 8179 Criticality Analysis



……DHS BOD on KL; NDAA on Huawei & ZTE

Industry

SAFECode Software Supply Chain Integrity papers

Common Criteria Supply Chain Security Assurance

ISO/IEC 27036 – Information Security in Supplier Relationships

IEC 62443-2-4 – Industrial-process measurement, control and automation

Open Trusted Technology Standard ISO/IEC 20243

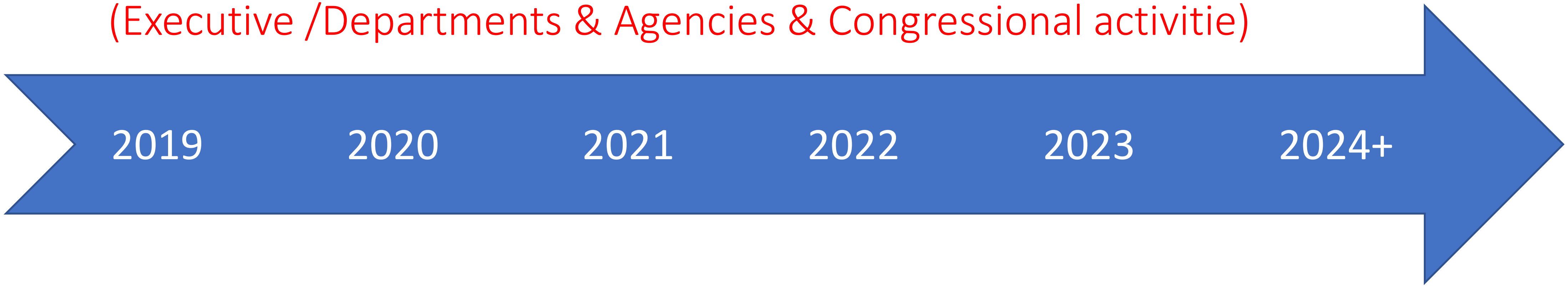
SAFECode Use of Third Party Components

ABA Vendor Checklist In Contracts

USG continues SUPPLY CHAIN RISK MANAGEMENT activities

https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats

Series of Executive Orders (next page)
& updates to NIST SP 800-161 rev1 etc. (also NIST SP 800-171 & CMMC)
Davidson / Synopsys / Industry is actively engaged with USG
(Executive /Departments & Agencies & Congressional activitie)



2019 2020 2021 2022 2023 2024+

Industry (and Academia) continues SCRM activities (see next pages for examples)

Synopsys / Davidson is actively engaged with Public-Private Programs / efforts,
Trade Associations, Non-Profit Organizations
& Standards Development Organizations.

SUPPLY CHAIN RISK MANAGEMENT https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats

Executive Orders

EO 13636 Improving Critical Infrastructure Cybersecurity

EO 13806 Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States

Executive Order **13806 Report**

EO 13873 Securing the Information and Communications Technology and Services Supply Chain

EO 13913 Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector

EO 13984 Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities

EO 14005 Ensuring the Future Is Made in All of America by All of America's Workers

EO 14017 America's Supply Chains

EO 14024 Blocking Property with Respect to Specified Foreign Activities of the Government of the Russian Federation

EO 14028 Improving the Nation's Cybersecurity

NIST: Security Measures for "EO-Critical Software" Use

NIST: Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order (EO) 14028

EO 14034 Protecting Americans' Sensitive Data from Foreign Adversaries

Synopsys is engaged in several Public-Private Microelectronics & Cyber-SCRM Initiatives

- Synopsys is member of **NDIA** (CSO on NDIA Board of Directors)
  - **NDIA Electronics Division / Trusted & Assured Microelectronics (TAME) Committee** (and other Divisions / WGs)
  - **NDIA Cyber-Division ICT/Cyber-SCRM Committee co-lead** (interface with TAME above & Manufacturing Division)
  - provides NDIA focal-point / lead on **NDIA input** to **DoD 5200.44 on Trusted Systems & Networks** and **NDAA 2019 Section 224 on Microelectronics Security Standard(s)--- New MQA / MAF construct**
- Synopsys is an active participant in **DHS/CISA's public-private ICT-SCRM Task Force--- leads SBOM WG**
- We provide a **Cyber-SCRM Fellow at Institute for Critical Infrastructure Technology** (ICITech)
- We are an active member of **Semiconductor Industry Association** (SIA)
- Synopsys co-leads **Accellera.org** with mission ***"to provide a platform in which the electronics industry can collaborate to innovate and deliver global standards that improve design and verification productivity for electronics products."***
- Synopsys briefs on **Microelectronics & Cyber-SCRM** at DoD sponsored Conferences
  - **TAME**
  - **GOMAC**
  - "**Diminishing Manufacturing Sources and Material Shortages (DMSMS) Conference & Parts Obsolescence Symposium and Defense Manufacturing Conference (DMC)**"
- We served on the IDA-led Core WG on **Hardware Assurance Body-of-Knowledge (HwA BoK)**
- We participate in **SAE/G32- Cyber Physical Systems Security** WG (HwA, SwA, SSE, Risk Mgt) er-SCRM ad-hoc WG shaping US National Positions on SCRM-related standards.-
- Active in **GSA-TIES** initiative (Global Semiconductor Alliance Trusted IoT Ecosystem Security)
- Authored C-SCRM Chapter in new ICITech.org book on "***Securing US Critical Infrastructure"***
- ***Provides SME to DOC CHIPS-ACT Industrial Advisory Committee.***
- ***Provides SME to DOC/BIS Information Systems Technical Advisory Committee (ISTAC).***

- **NDIA** efforts to secure DIB in several Divisions https://www.ndia.org/about
- OUSD R&E's "**Zero Trust / Quantifiable Assurance**" efforts https://rt.cto.mil/ddre-rt/dd-rtl/tam/
- **DARPA & IARPA** efforts in Microelectronics Security https://www.darpa.mil/ https://www.iarpa.gov/index.php/contact
- **JFAC** (HwA & SwA) https://rt.cto.mil/stpe/rs/jfac/
- OUSD R&E funded **HwA BoK**, in support of Systems Engineering Wiki https://www.sebokwiki.org/wiki/Systems_Engineering_Overview
- OUSD R&E efforts on **NDAA 2019's Section 224 "Microelectronics Security Standard**(s)": " (I) manufacturing location; (II) Company ownership; (III) Workforce composition; (IV) Access during manufacturing, suppliers' design, sourcing, manufacturing, packaging, and distribution processes; (V) Reliability of the supply chain; and (VI) Other matters germane to supply chain and operational security;" and 2022 ANSI workshops on Section 224 / MQA, Microelectronics Quantifiable Assurance.
- **CISA's public-private ICT-SCRM TF** efforts https://www.cisa.gov/ict-scrm-task-force
- **Institute for Critical Infrastructure Technologies** efforts https://icitech.org/
- **Cyberspace Solarium Commission & Supply Chain Paper** https://www.solarium.gov/
- **Industrial Internet Consortium** efforts https://www.iiconsortium.org/about-us.htm
- **SAE / G32 work on Cyber-Physical Systems Security (CPSS)** https://www.sae.org/works/committeeHome.do?comtID=TEAG32
- **ISO 15026: Software & Systems Assurance Case** https://webstore.ansi.org/Standards/ISO/ISOIEC150261998?gclid=EAIaIQobChMI0aDZrbLQ7AIVhq_ICh2wcgPAEAAYASAAEgIEcPD_BwE
- **ISO 27036: Information technology & Security techniques for supplier relationships** https://webstore.ansi.org/standards/iso/isoiec27036information?gclid=EAIaIQobChMI6ZfE1bLQ7AIViI3ICh1YeQICEAAYASAAEgJdIPD_BwE
- Many **DevSecOps** (SwA) efforts in lots of places https://tech.gsa.gov/guides/understanding_differences_agile_devsecops/
- **Accellera** collaborates, innovates and delivers global standards to improve design and verification productivity for electronics products. https://www.accellera.org/about
- *…and Lots of Others…*

SYNOPSYS®
Silicon to Software™

Supply Chain:
PERSPECTIVES

Supply Chain RESILIENCY (mostly availability)
is important but we also need focus on

Product INTEGRITY (NIST-800-161)
&
Information System CONFIDENTIALITY (NIST-800-171 / CMMC)

How do we improve our trust & confidence
in HW, SW & Services we source from a
global supply chain?

ISO/IEC 27002

Confidentiality=
Ensuring that information is accessible only to those authorized to have access.

Integrity=
Safeguarding the accuracy and completeness of information and processing methods.

Availability=
Ensuring that authorized users have access to information and associated assets when required.

Product/Part & Data
AVAILABILITY

March 2023 US National Cybersecurity Strategy raises challenges for Product Security/Integrity linkage to Information Systems Enterprise Risk Management
--NIST CSF 2.0 may need more specification on ICT/Cyber-SCRM (HwA & SwA)

NDAA 2023 Section 5949

NDAA 2023 /// Section 5949------PROHIBITION ON CERTAIN SEMICONDUCTOR PRODUCTS AND SERVICES (*w/ TRACEABILITY Tasking*)

https://www.congress.gov/bill/117th-congress/house-bill/7776/text

- "…(f) Governmentwide Traceability and Diversification Initiative.--

(1) In general.--Not later than two years after the date of the enactment of this Act, the Secretary of Commerce, in coordination with the Secretary of Homeland Security, the Secretary of Defense, the Director of National Intelligence, the Director of the Office of Management and Budget, and the Director of the Office of Science and Technology Policy, and in consultation with industry, shall establish a microelectronics traceability and diversification initiative to coordinate analysis of and response to the Federal Government microelectronics supply chain vulnerabilities."

Cyber Supply Chain Risk

U.S. National Institute of Standards and Technology (NIST) definition of *Cyber Supply Chain Risk Management* (C-SCRM):

- C-SCRM is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of Information Technology and Operational Technology (IT/OT) product and service supply chains.
- C-SCRM covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.

https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management

Software Supply Chain Risk Management: managing risk in the software that your business builds, buys, deploys, and maintains.

*Everything is being **connected**, **software enabled**, sped by **5G**, distributed through **Cloud.***

Cyber Supply Chain Perspectives

Cyber Supply Chain Risk Management (C-SCRM):

- C-SCRM is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains.

- C-SCRM covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.

https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management

*Everything is being **connected (IoT)**, **software-enabled**, sped by **5G**, & distributed through **Cloud.***

Cyber Supply Chain Perspectives

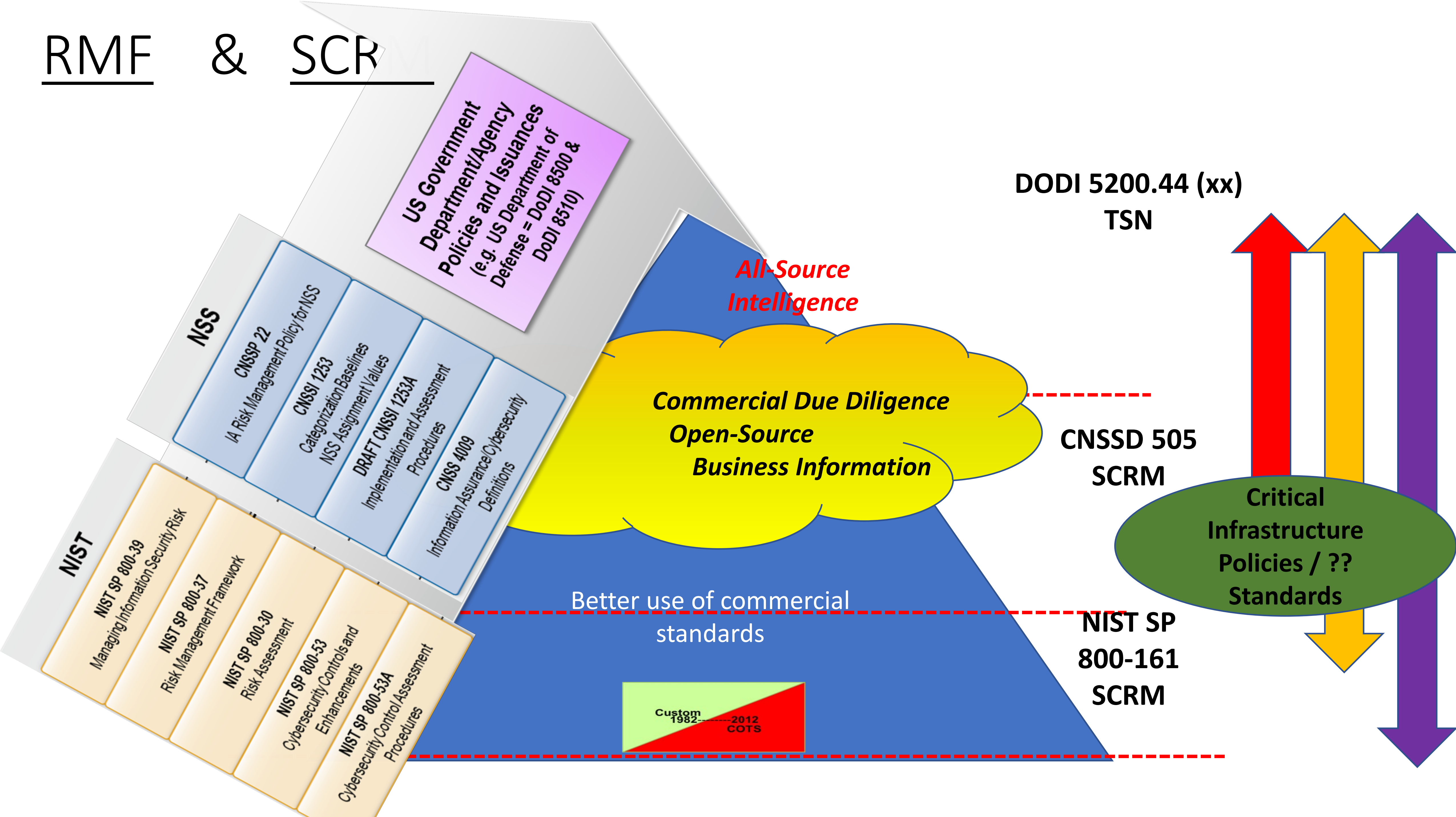
Scope of IT/OT definition – Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Subchap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018)

IT/OT (“Covered Articles”) means:

- Information technology, including cloud computing services of all types (41 USC 4713(k)(2)(A));
- Telecommunications equipment or telecommunications service (41 USC 4713(k)(2)(B));
- The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (41 USC 4713(k)(2)(C));
- All Internet of Things/Operational Technology (IoT/OT) – (hardware, systems, devices, software, or services that include embedded or incidental information technology). (41 USC 4713(k)(2)(D)).

Bottom line – IT/OT/ICT/IoT interpreted by US government as everything that is (or may be) connected to a network. C-SCRM addresses both information systems and the IoT ecosystem.

RMF & SCRM



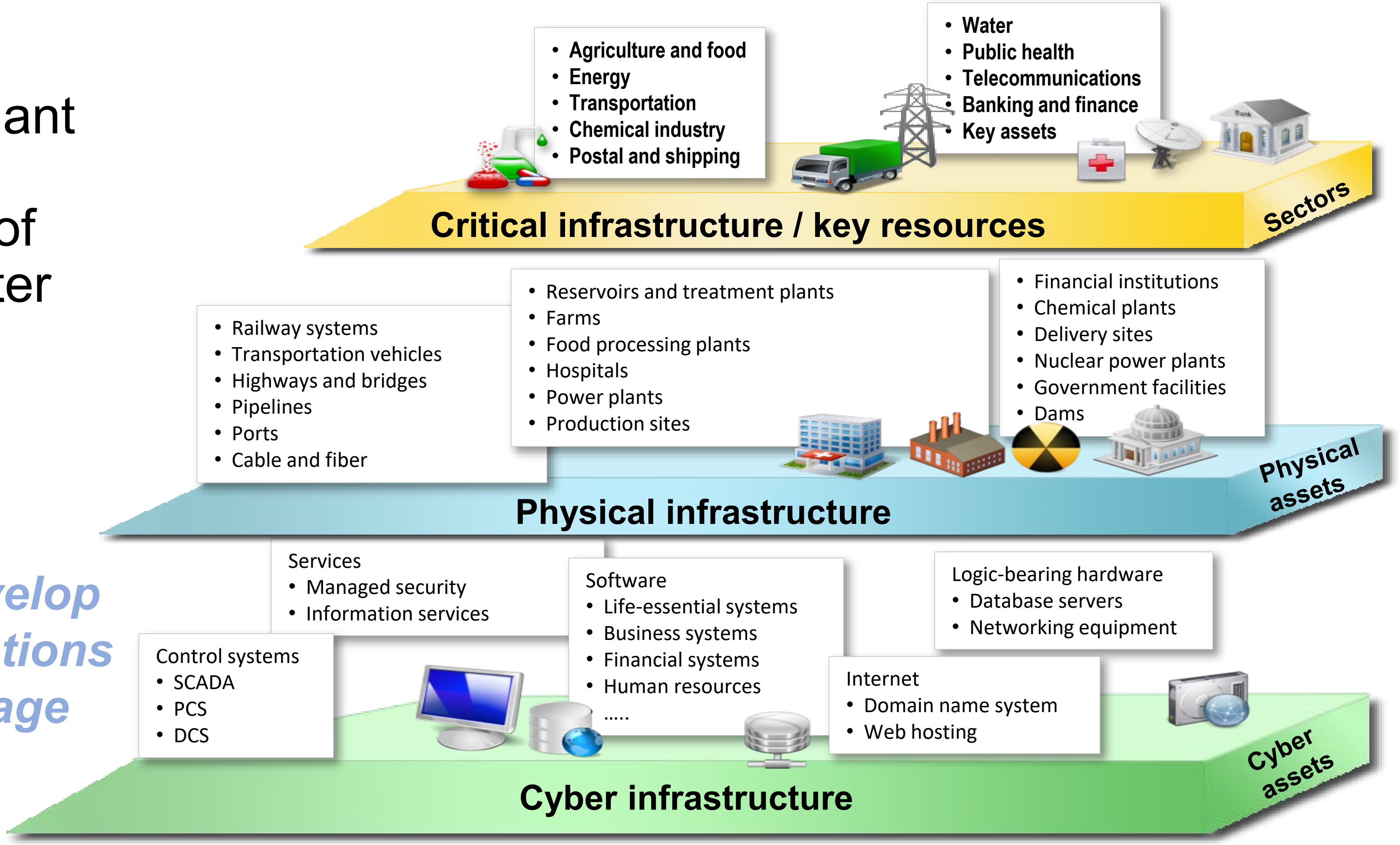
US Government Department/Agency Policies and Issuances (e.g. US Department of Defense = DoDI 8500 & DoDI 8510)
NSS
CNSSP 22 IA Risk Management Policy for NSS
CNSSI 1253 Categorization Baselines NSS Assignment Values
DRAFT CNSSI 1253A Implementation and Assessment Procedures
CNSS 4009 Information Assurance/Cybersecurity Definitions
NIST
NIST SP 800-39 Managing Information Security Risk
NIST SP 800-37 Risk Management Framework
NIST SP 800-30 Risk Assessment
NIST SP 800-53 Cybersecurity Controls and Enhancements
NIST SP 800-53A Cybersecurity Control Assessment Procedures
All-Source Intelligence
Commercial Due Diligence
Open-Source
Business Information
Better use of commercial standards
Custom
1982---------2012
COTS
DODI 5200.44 (xx)
TSN
CNSSD 505
SCRM
NIST SP 800-161
SCRM
Critical Infrastructure Policies / ?? Standards

Securing Critical Infrastructure

Reliance on ICT/IoT & SW-based technologies

Dependencies on software-reliant information communications technology (ICT) and Internet of Things' (IoT) devices are greater than ever

Individual Enterprises must develop "overlays" of controls/specifications and standards to measure/manage risk to their respective critical infrastructure.



- Agriculture and food
- Energy
- Transportation
- Chemical industry
- Postal and shipping

- Water
- Public health
- Telecommunications
- Banking and finance
- Key assets

Critical infrastructure / key resources

Sectors

- Railway systems
- Transportation vehicles
- Highways and bridges
- Pipelines
- Ports
- Cable and fiber

- Reservoirs and treatment plants
- Farms
- Food processing plants
- Hospitals
- Power plants
- Production sites

- Financial institutions
- Chemical plants
- Delivery sites
- Nuclear power plants
- Government facilities
- Dams

Physical infrastructure

Physical assets

Services
- Managed security
- Information services

Software
- Life-essential systems
- Business systems
- Financial systems
- Human resources
- .....

Logic-bearing hardware
- Database servers
- Networking equipment

Control systems
- SCADA
- PCS
- DCS

Internet
- Domain name system
- Web hosting

Cyber infrastructure

Cyber assets

Cyber infrastructure is enabled and controlled by software

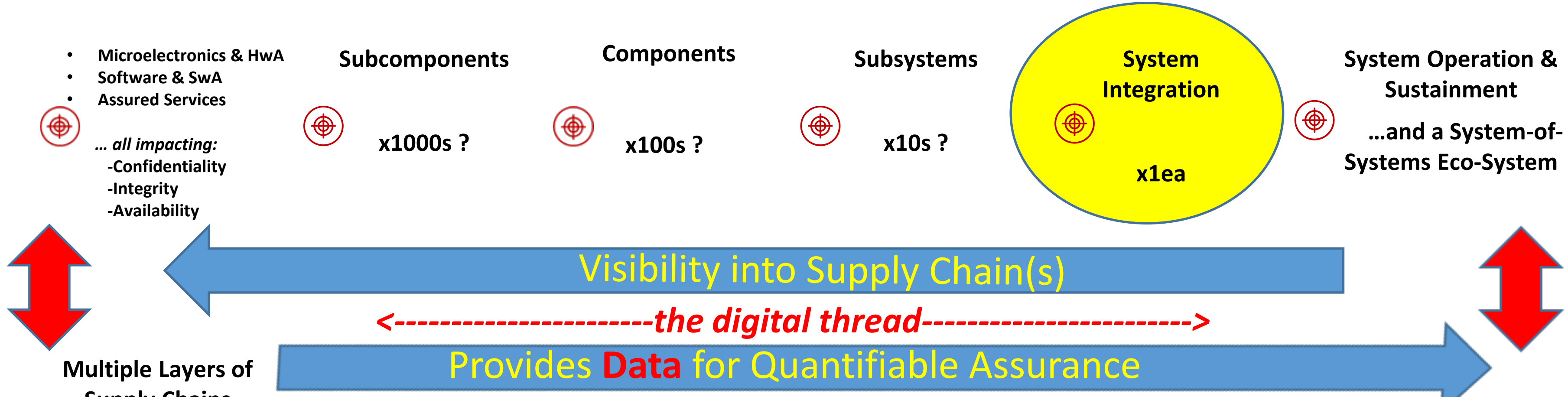
Visibility into Supply Chains can deliver Data to improve ICT/Cyber-Supply Chain Risk Management

Vulnerabilities exist in the System Lifecycle - Research, Development, and Acquisition phases, as well as during Operations and Sustainment.

Organizations need both centralized and decentralized capabilities to: Strengthen supply chain security & Reduce the attack surface

Need some "agreed" Traceability & Provenance metrics.

Need some "agreed" Levels of Assurance (LOAs).



- Microelectronics & HwA
- Software & SwA
- Assured Services

… all impacting:
-Confidentiality
-Integrity
-Availability

Subcomponents

x1000s ?

Components

x100s ?

Subsystems

x10s ?

System Integration

x1ea

System Operation & Sustainment

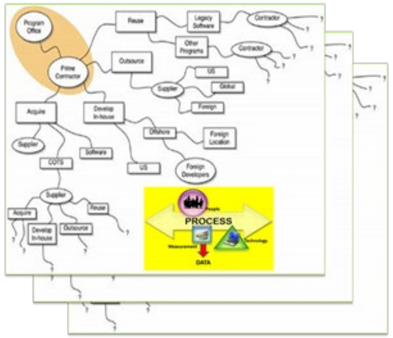
…and a System-of-Systems Eco-System

Visibility into Supply Chain(s)

<----------------------the digital thread----------------------->

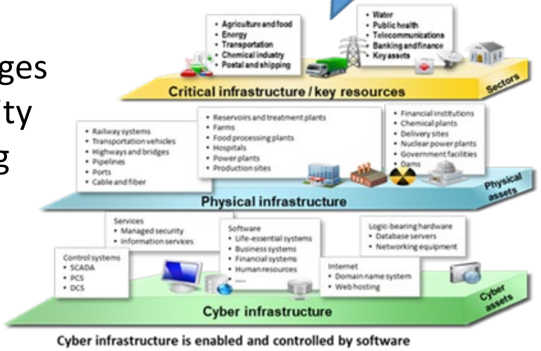
Provides **Data** for Quantifiable Assurance

Multiple Layers of Supply Chains



"The U.S. manufacturing industry… (has both challenges and opportunities due to) …advanced interconnectivity fueled by the Internet of Things (IoT) and the growing value of data, *'the digital thread'*, that traverses a manufacturing network. "

https://www.ndia.org/-/media/sites/ndia/divisions/working-groups/cfam/ndia-cfam-2017-white-paper-20171023.ashx?la=en



Cyber infrastructure is enabled and controlled by software

How can Blockchain (DLT) Technologies & ML / AI help?

Q&A

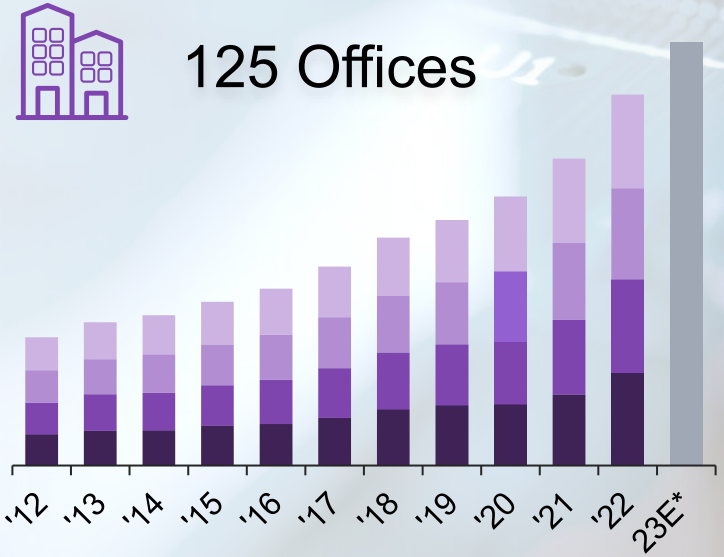
BACK-UP SLIDES

$5.08B Revenue (TTM)

19,008 Employees

3,386 Patents

125 Offices



synopsys®

#1 Electronic Design Automation Tools and Services

Broadest IP Portfolio and **#1** Interface, Foundation & Physical IP

'Leader' In Gartner's Magic Quadrant for Application Security Testing

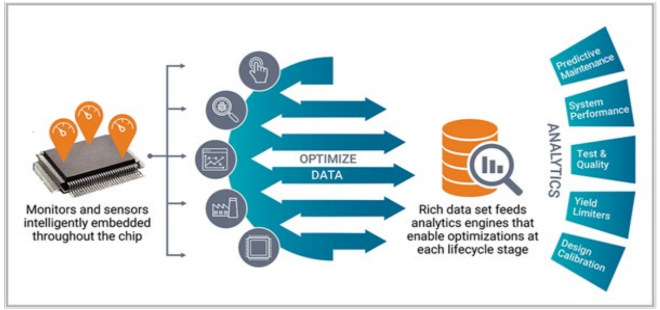
Smart- Safe-Secure Everything !

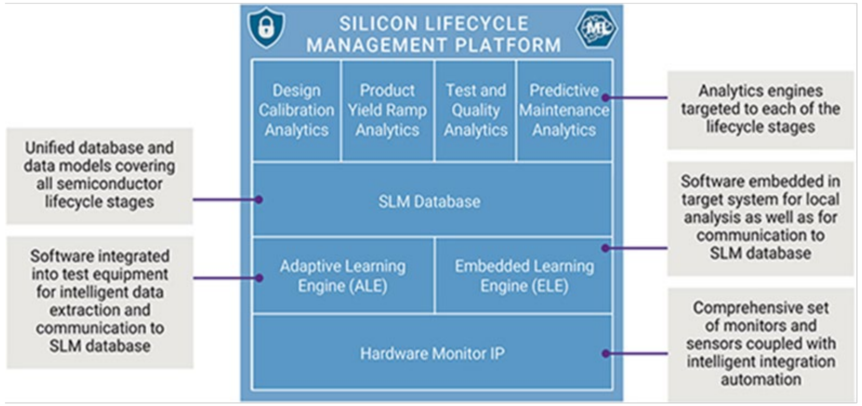
Hardware (EDA & IP)

Smart, Safe, Secure Everything

- **October 20, 2020** -

Synopsys unveils Industry's first Silicon Lifecycle Management Platform to Optimize Entire IC Life Span


Monitors and sensors intelligently embedded throughout the chip
OPTIMIZE DATA
Rich data set feeds analytics engines that enable optimizations at each lifecycle stage
ANALYTICS
Predictive Maintenance
System Performance
Test & Quality
Yield Limiters
Design Calibration



SILICON LIFECYCLE MANAGEMENT PLATFORM

Design Calibration Analytics | Product Yield Ramp Analytics | Test and Quality Analytics | Predictive Maintenance Analytics

SLM Database

Adaptive Learning Engine (ALE) | Embedded Learning Engine (ELE)

Hardware Monitor IP

Unified database and data models covering all semiconductor lifecycle stages

Software integrated into test equipment for intelligent data extraction and communication to SLM database

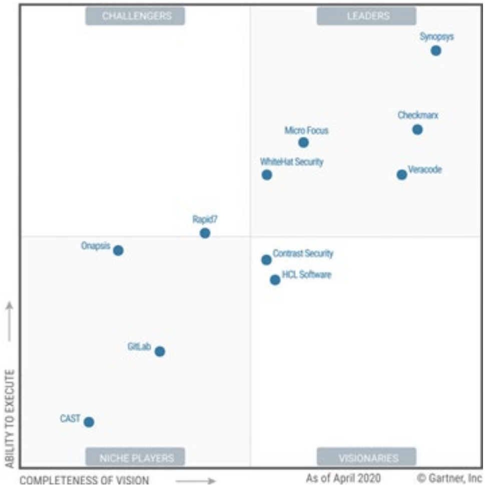
Analytics engines targeted to each of the lifecycle stages

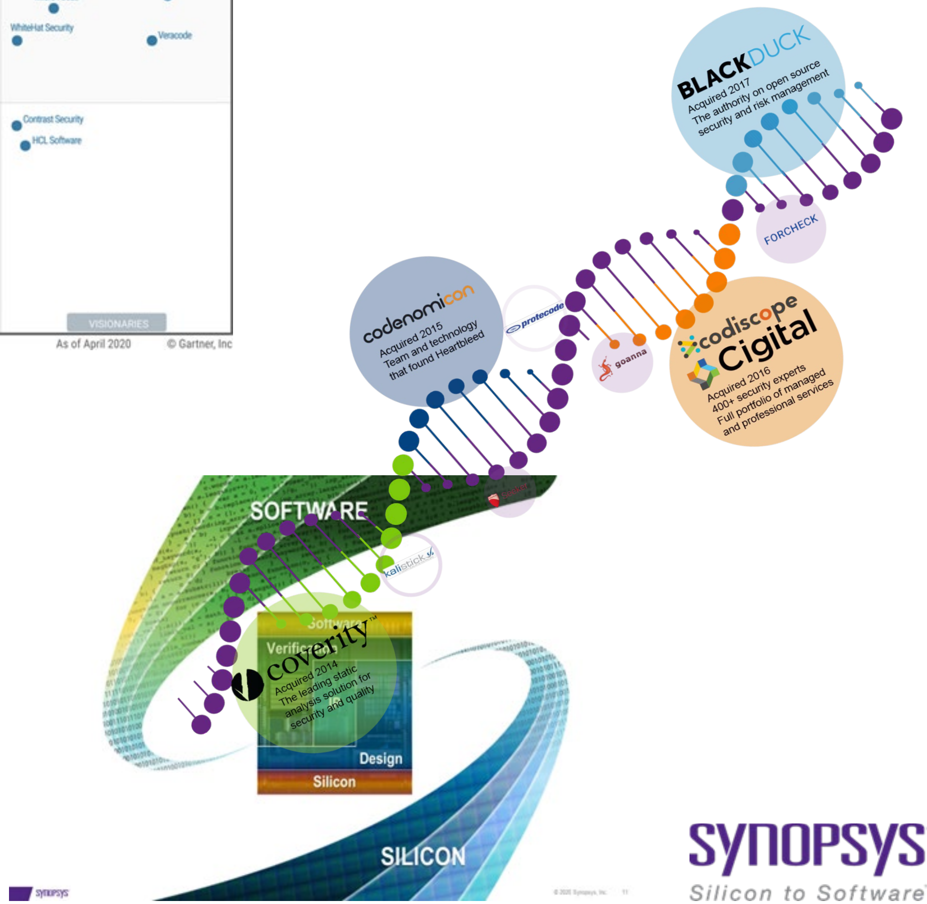
Software embedded in target system for local analysis as well as for communication to SLM database

Comprehensive set of monitors and sensors coupled with intelligent integration automation

https://www.synopsys.com/solutions/silicon-lifecycle-management.html

2022 Gartner Magic Quadrant for Application Security Testing:
Synopsys is a Leader for the Sixth Year in a Row





SYNOPSYS®
Silicon to Software™