Enabling Delivery Uncompromised Digital Threads

Thomas Hedberg, Ph.D., P.E.
Associate Director for Education Programs, Institute for Systems Research
Mission Director, Acquisition & Industrial Security, ARLIS

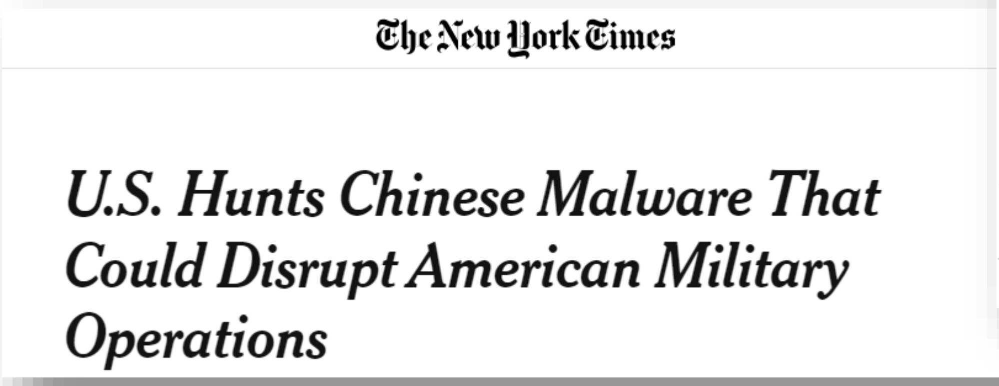
A. James Clark
School of Engineering
Institute for Systems Research

Applied Research Laboratory for
Intelligence
and Security

> “*Knowing what we know now, we would not have designed the internet like we did.*”

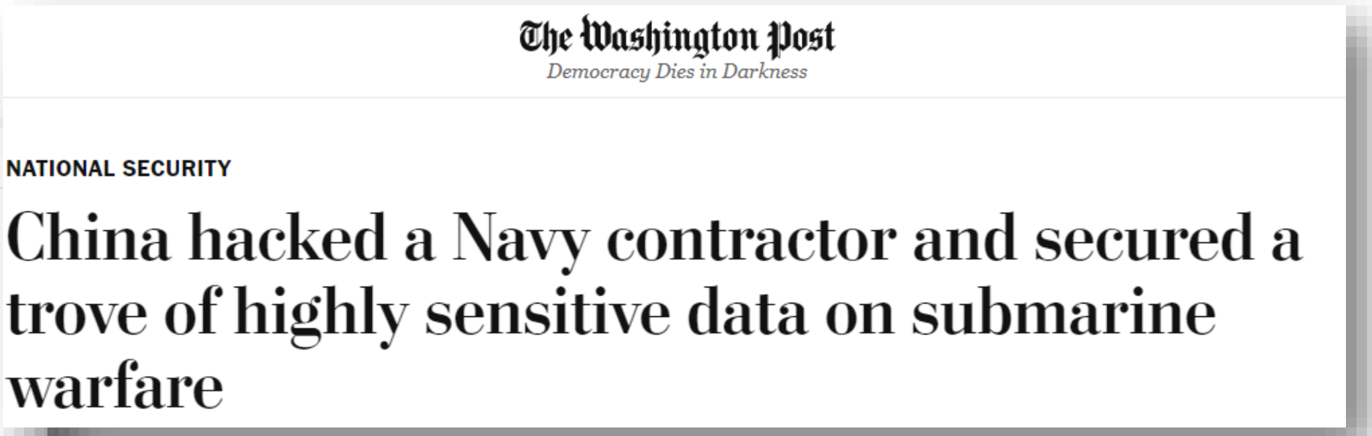
-- A conversation with Robert Kahn

Ripped from the Headlines!



The New York Times

U.S. Hunts Chinese Malware That Could Disrupt American Military Operations

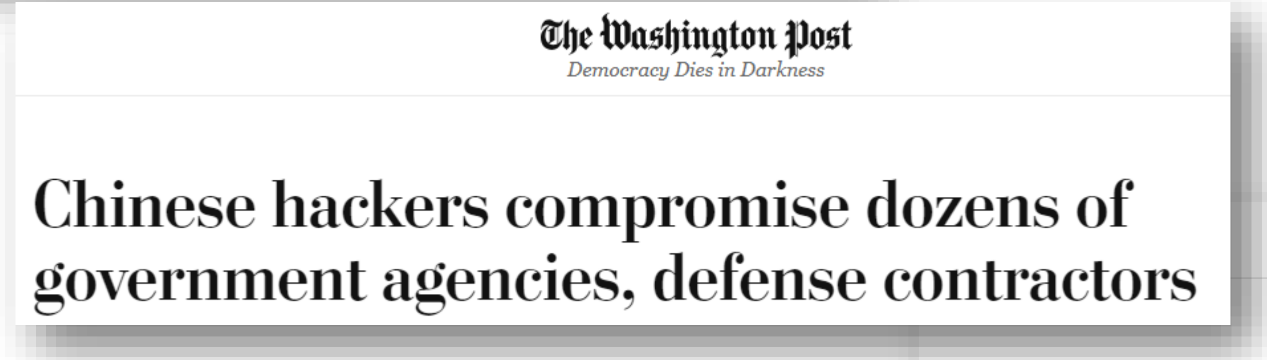


The Washington Post

Democracy Dies in Darkness

NATIONAL SECURITY

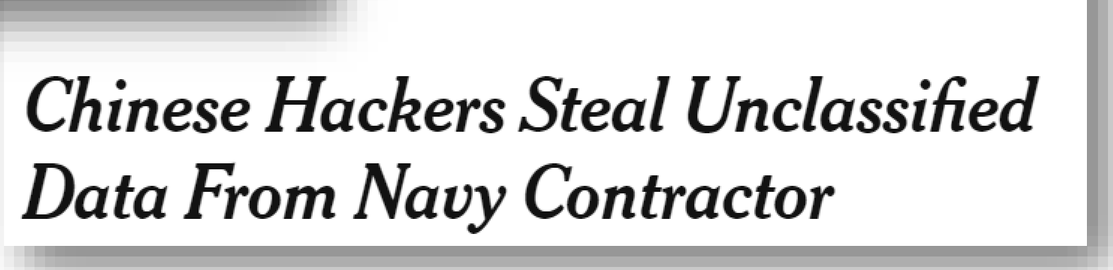
China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare



The Washington Post

Democracy Dies in Darkness

Chinese hackers compromise dozens of government agencies, defense contractors



The New York Times

Chinese Hackers Steal Unclassified Data From Navy Contractor

Presentation Outline

- What the problem?

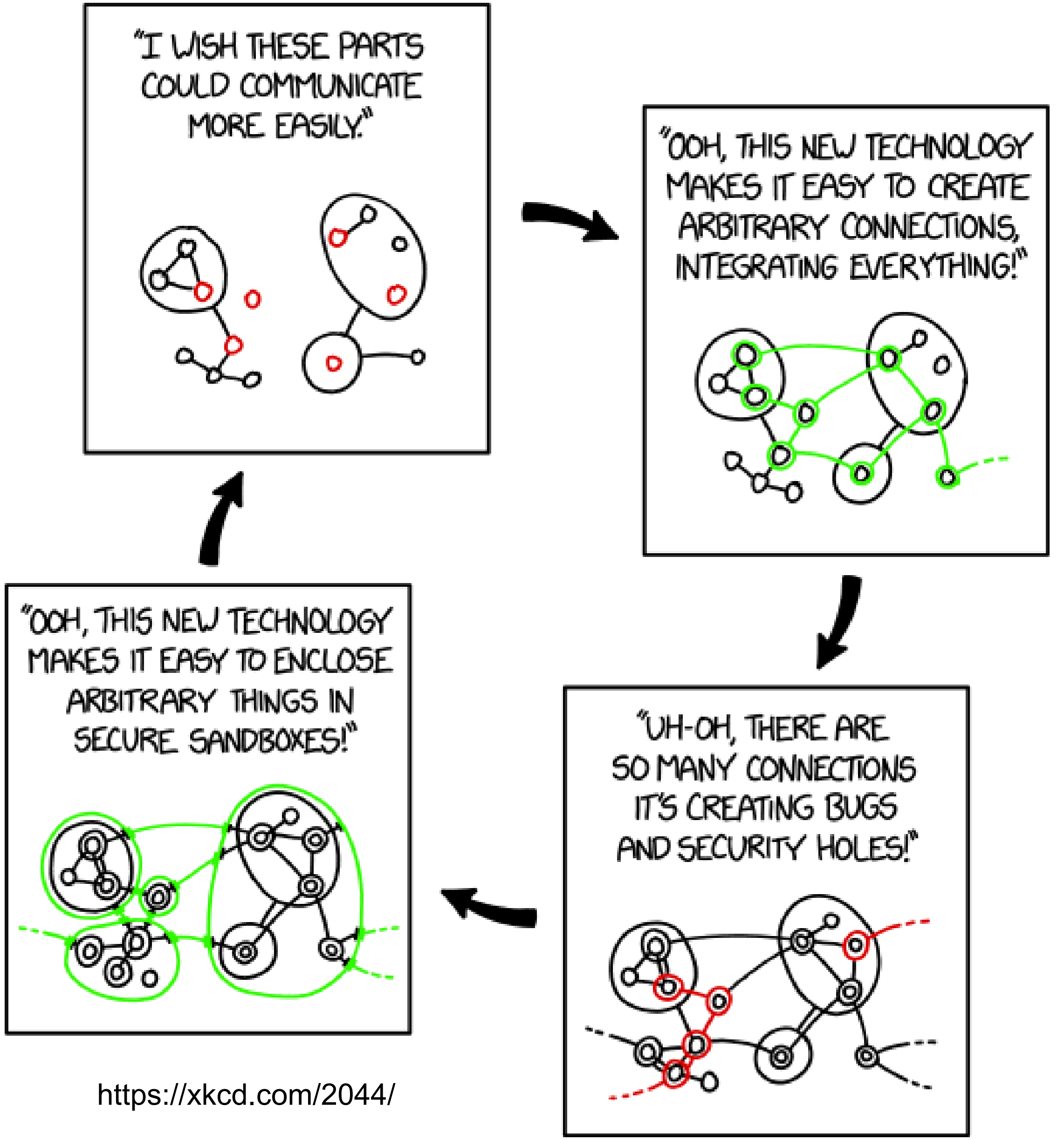
- What are we doing now?

- What can we do to mitigate risk?

The Problem

The Connection Interoperability Paradox

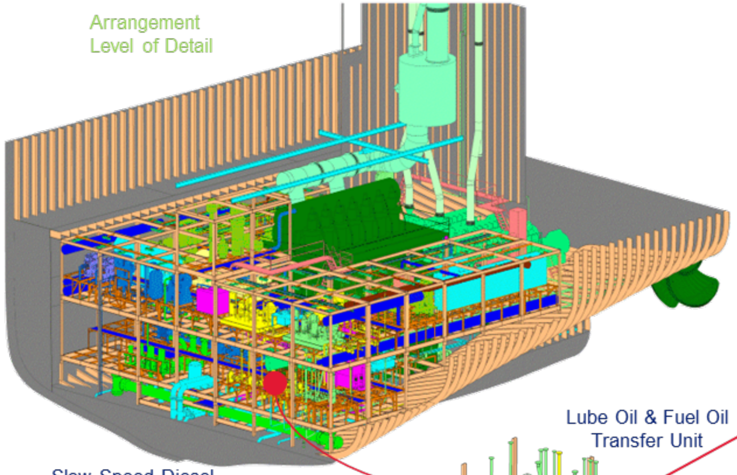
"All I want is a secure system where it's easy to do anything I want. Is that so much to ask?"


"I WISH THESE PARTS COULD COMMUNICATE MORE EASILY."
"OOH, THIS NEW TECHNOLOGY MAKES IT EASY TO CREATE ARBITRARY CONNECTIONS, INTEGRATING EVERYTHING!"
"UH-OH, THERE ARE SO MANY CONNECTIONS IT'S CREATING BUGS AND SECURITY HOLES!"
"OOH, THIS NEW TECHNOLOGY MAKES IT EASY TO ENCLOSE ARBITRARY THINGS IN SECURE SANDBOXES!"

https://xkcd.com/2044/

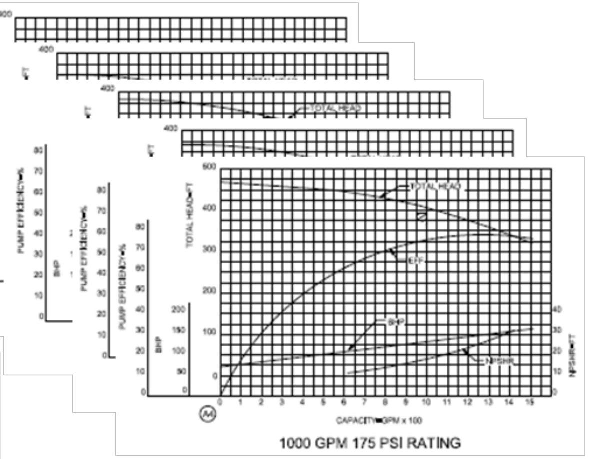
3D Model-Based Definition

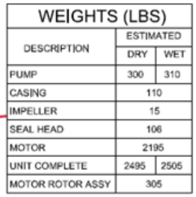
is more convoluted than we care to admit



Slow Speed Diesel Engine Room

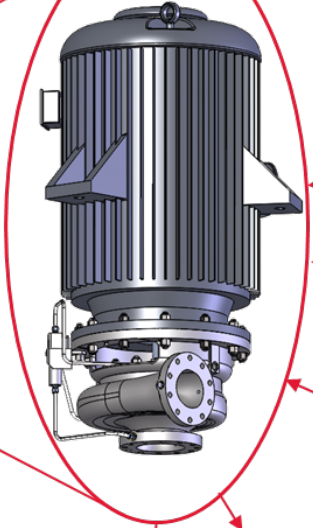
Assembly
Level of Detail



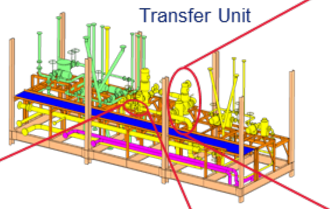


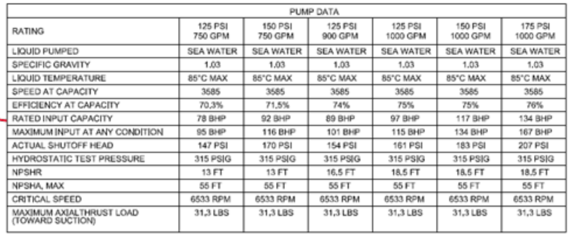
WEIGHTS (LBS)		
DESCRIPTION	ESTIMATED	
	DRY	WET
PUMP	300	310
CASING	110	
IMPELLER	15	
SEAL HEAD	106	
MOTOR	2195	
UNIT COMPLETE	2495	2505
MOTOR ROTOR ASSY	305	

Commodity Part

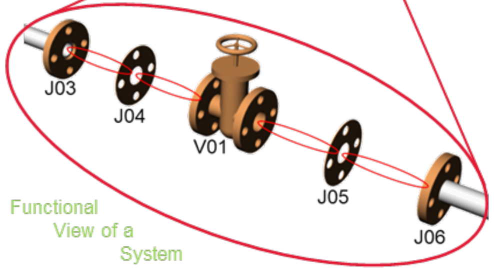


Lube Oil & Fuel Oil Transfer Unit

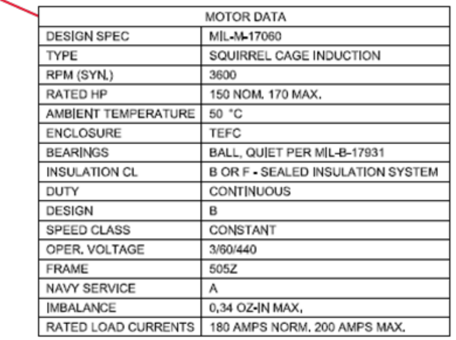




PUMP DATA						
RATING	125 PSI 750 GPM	150 PSI 750 GPM	125 PSI 900 GPM	125 PSI 1000 GPM	150 PSI 1000 GPM	175 PSI 1000 GPM
LIQUID PUMPED	SEA WATER	SEA WATER	SEA WATER	SEA WATER	SEA WATER	SEA WATER
SPECIFIC GRAVITY	1.03	1.03	1.03	1.03	1.03	1.03
LIQUID TEMPERATURE	85°C MAX	85°C MAX	85°C MAX	85°C MAX	85°C MAX	85°C MAX
SPEED AT CAPACITY	3585	3585	3585	3585	3585	3585
EFFICIENCY AT CAPACITY	70,3%	71,5%	74%	75%	75%	76%
RATED INPUT CAPACITY	78 BHP	92 BHP	89 BHP	97 BHP	117 BHP	134 BHP
MAXIMUM INPUT AT ANY CONDITION	95 BHP	116 BHP	101 BHP	115 BHP	134 BHP	167 BHP
ACTUAL SHUTOFF HEAD	147 PSI	170 PSI	154 PSI	161 PSI	183 PSI	207 PSI
HYDROSTATIC TEST PRESSURE	315 PSIG	315 PSIG	315 PSIG	315 PSIG	315 PSIG	315 PSIG
NPSHR	13 FT	13 FT	16,5 FT	18,5 FT	18,5 FT	18,5 FT
NPSHA, MAX	55 FT	55 FT	55 FT	55 FT	55 FT	55 FT
CRITICAL SPEED	6533 RPM	6533 RPM	6533 RPM	6533 RPM	6533 RPM	6533 RPM
MAXIMUM AXIALTHRUST LOAD (TOWARD SUCTION)	31,3 LBS	31,3 LBS	31,3 LBS	31,3 LBS	31,3 LBS	31,3 LBS

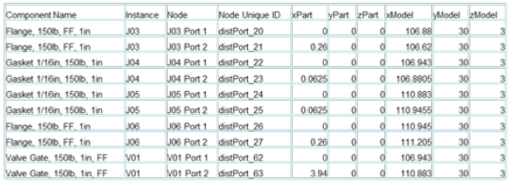


Functional View of a System



MOTOR DATA	
DESIGN SPEC	MIL-M-17060
TYPE	SQUIRREL CAGE INDUCTION
RPM (SYN.)	3600
RATED HP	150 NOM. 170 MAX.
AMBIENT TEMPERATURE	50 °C
ENCLOSURE	TEFC
BEARINGS	BALL, QUIET PER MIL-B-17931
INSULATION CL	B OR F - SEALED INSULATION SYSTEM
DUTY	CONTINUOUS
DESIGN	B
SPEED CLASS	CONSTANT
OPER. VOLTAGE	3/60/440
FRAME	505Z
NAVY SERVICE	A
IMBALANCE	0,34 OZ-IN MAX.
RATED LOAD CURRENTS	180 AMPS NORM. 200 AMPS MAX.

Manufacturing Level of Detail

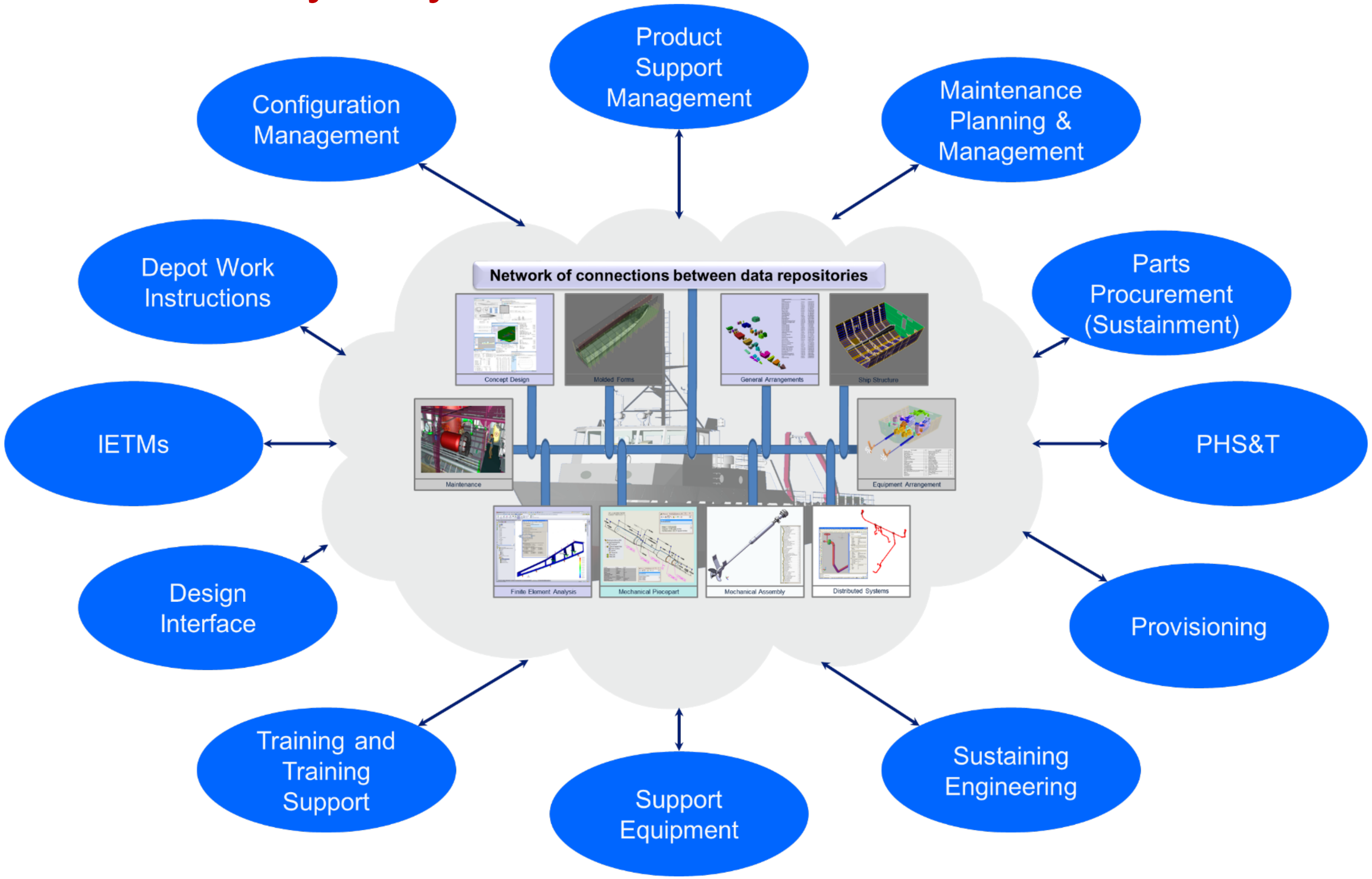


Component Name	Instance	Node	Node Unique ID	xPart	yPart	zPart	xModel	yModel	zModel
Flange, 150lb, FF, 1in	J03	J03 Port 1	distPort_20	0	0	0	106.88	30	3
Flange, 150lb, FF, 1in	J03	J03 Port 2	distPort_21	0.26	0	0	106.62	30	3
Gasket 1/16in, 150lb, 1in	J04	J04 Port 1	distPort_22	0	0	0	106.943	30	3
Gasket 1/16in, 150lb, 1in	J04	J04 Port 2	distPort_23	0.0625	0	0	106.8805	30	3
Gasket 1/16in, 150lb, 1in	J05	J05 Port 1	distPort_24	0	0	0	110.883	30	3
Gasket 1/16in, 150lb, 1in	J05	J05 Port 2	distPort_25	0.0625	0	0	110.9455	30	3
Flange, 150lb, FF, 1in	J06	J06 Port 1	distPort_26	0	0	0	110.945	30	3
Flange, 150lb, FF, 1in	J06	J06 Port 2	distPort_27	0.26	0	0	111.205	30	3
Valve Gate, 150lb, 1in, FF	V01	V01 Port 1	distPort_62	0	0	0	106.943	30	3
Valve Gate, 150lb, 1in, FF	V01	V01 Port 2	distPort_63	3.94	0	0	110.883	30	3

Do we really think there is a SINGLE Authoritative Source of Truth?

3D Model-Based Definition

has more information than everybody needs



Product Support Management

Maintenance Planning & Management

Parts Procurement (Sustainment)

PHS&T

Provisioning

Sustaining Engineering

Support Equipment

Training and Training Support

Design Interface

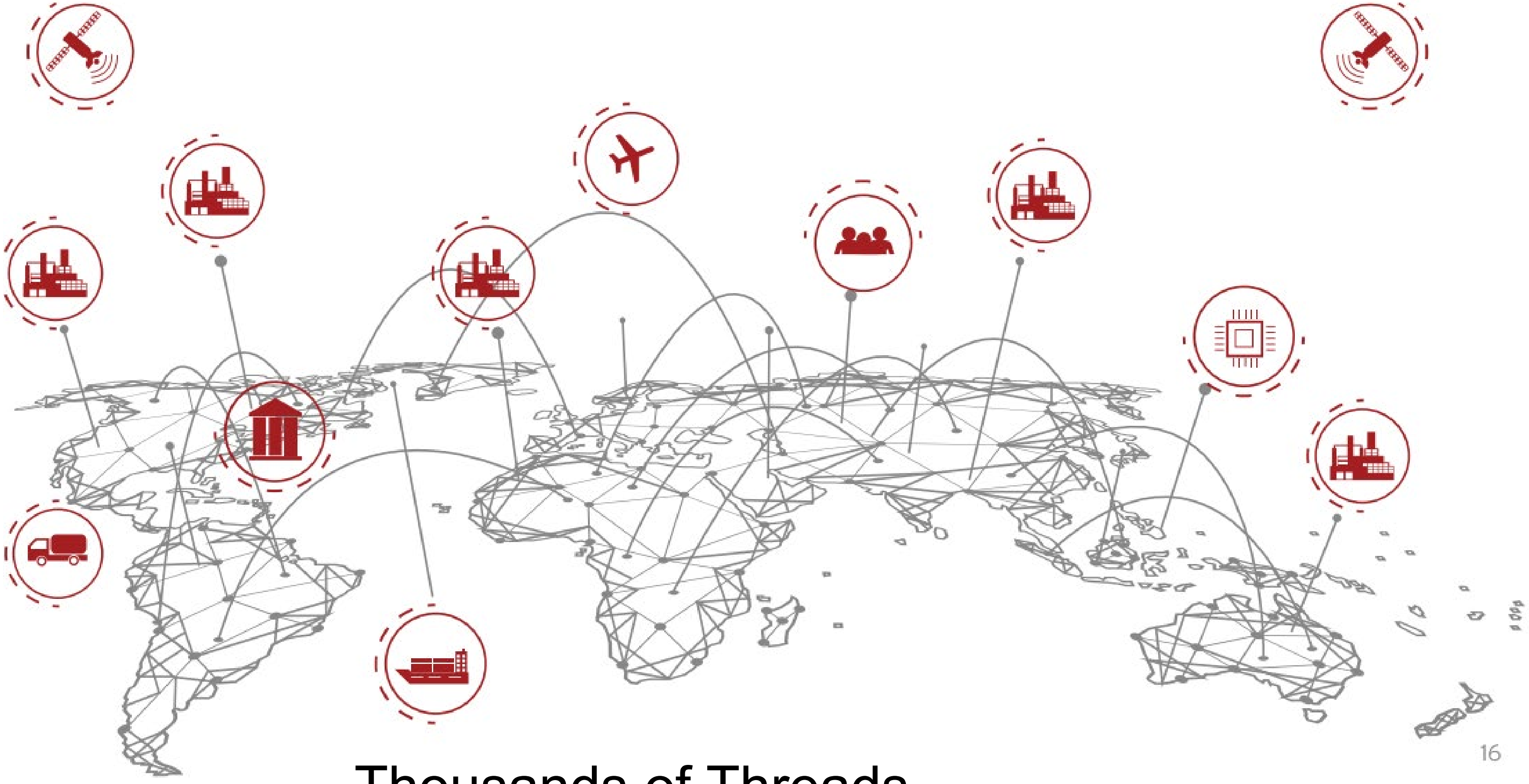
IETMs

Depot Work Instructions

Configuration Management

Do you really want to expose all data to all processes?

Digital Thread is an Information Supply Chain



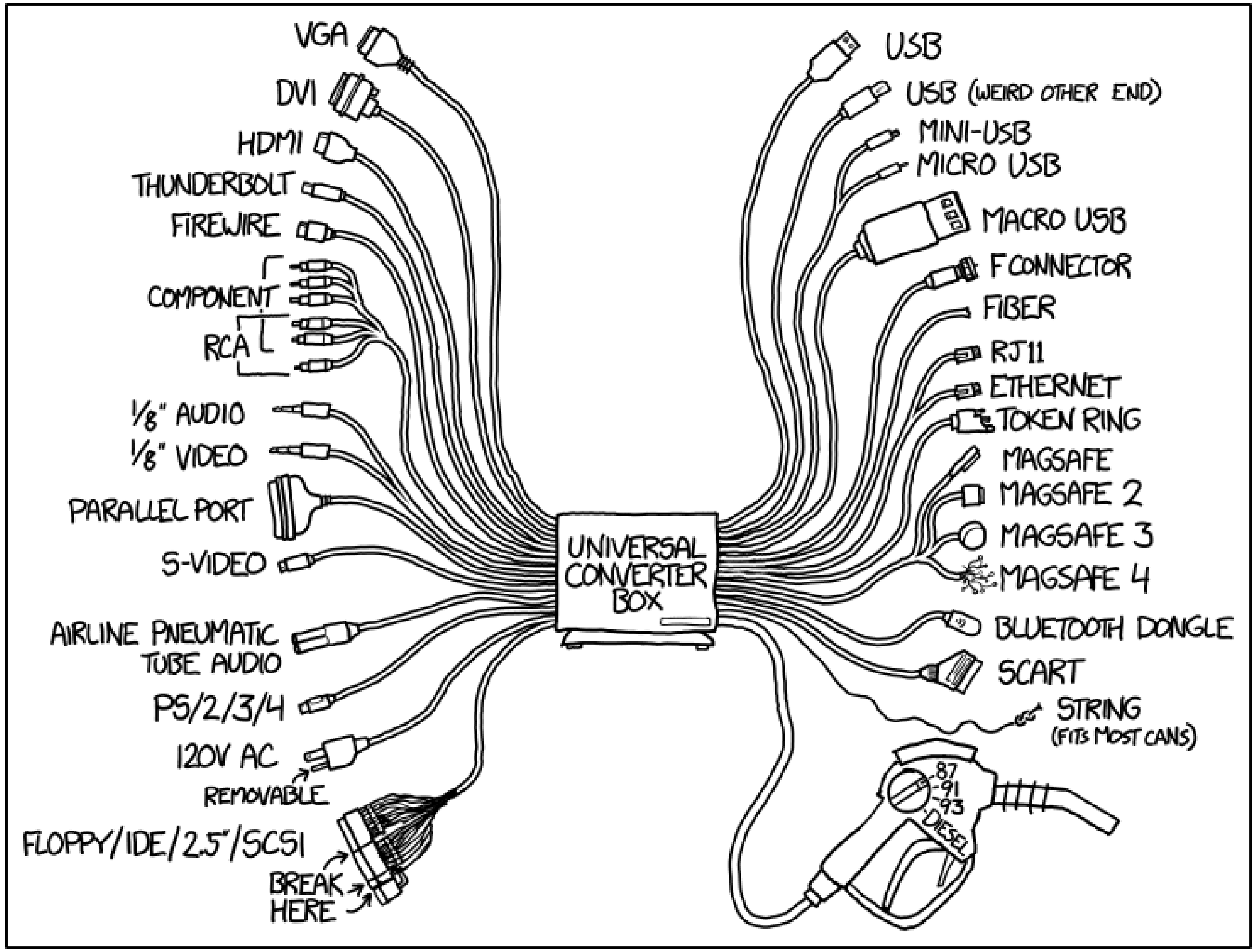
Thousands of Threads

Thousands of Opportunities for Intrusion

Thousands of Opportunities for Misdirection

State of the Art

The Connection Interoperability Paradox



https://xkcd.com/1406

But we've been saying it for years…

- DoD Digital Engineering Strategy says digital transformation will address challenges associated with complexity, uncertainty, and rapid change in deploying and using systems

- McKinsey recommends using a holistic and systematic analysis in making decisions on how and where to best deploy and maintain technologies and capabilities

- MITRE says U.S. needs better use of its existing resources to identify, protect, detect, respond to, and recover from network and supply chain threats – we must protect systems as much as we try to deploy them.

MITRE | The MITRE Center for Technology & National Security

DELIVER UNCOMPROMISED

A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War

By Chris Nissen, John Gronager, Ph.D., Robert Metzger, J.D., Harvey Rishikof, J.D.

DEPARTMENT OF DEFENSE

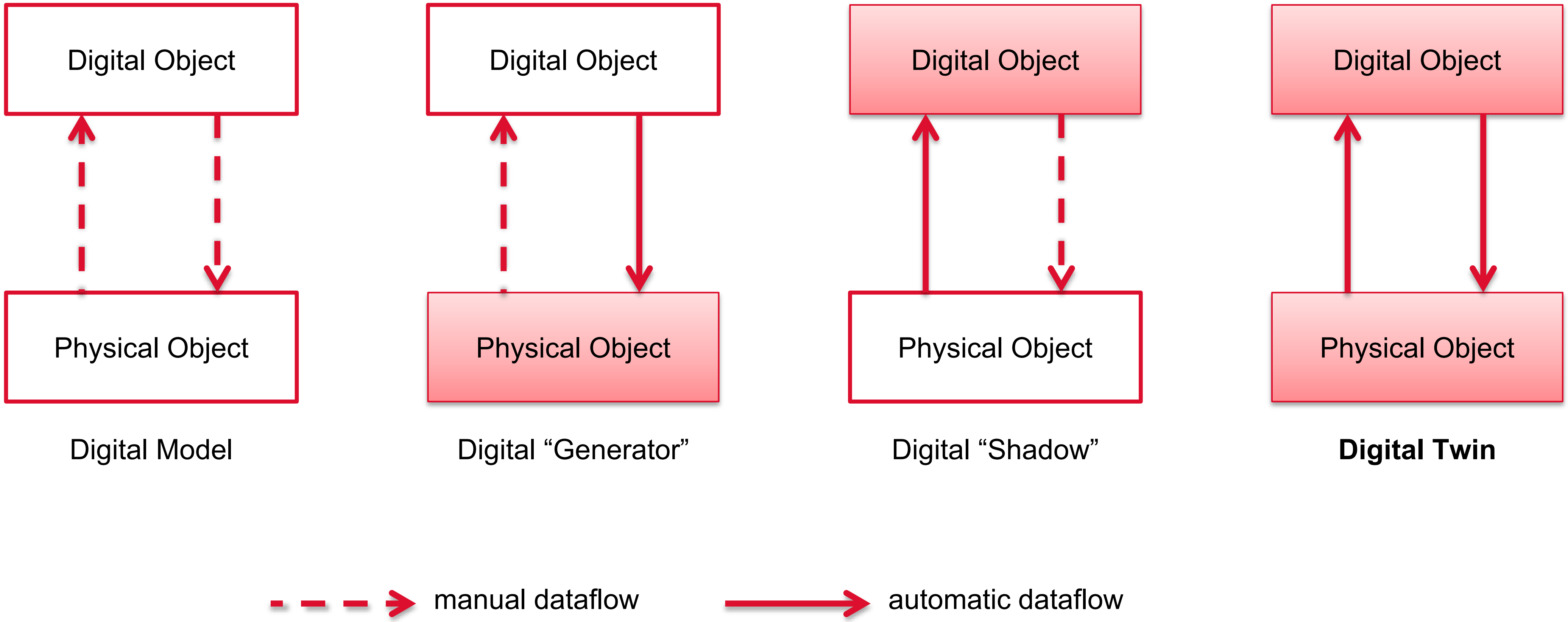
DIGITAL ENGINEERING STRATEGY

JUNE 2018

McKinsey on Digital Services

Introducing the next-generation operating model

Cyber-Physical Relationships



Digital Object

Physical Object

Digital Model

Digital Object

Physical Object

Digital “Generator”

Digital Object

Physical Object

Digital “Shadow”

Digital Object

Physical Object

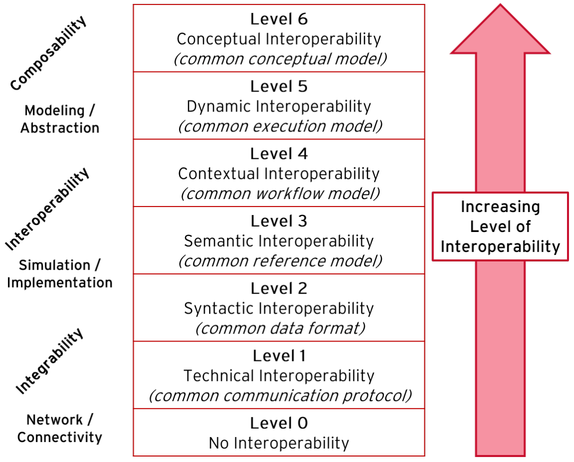
Digital Twin

manual dataflow

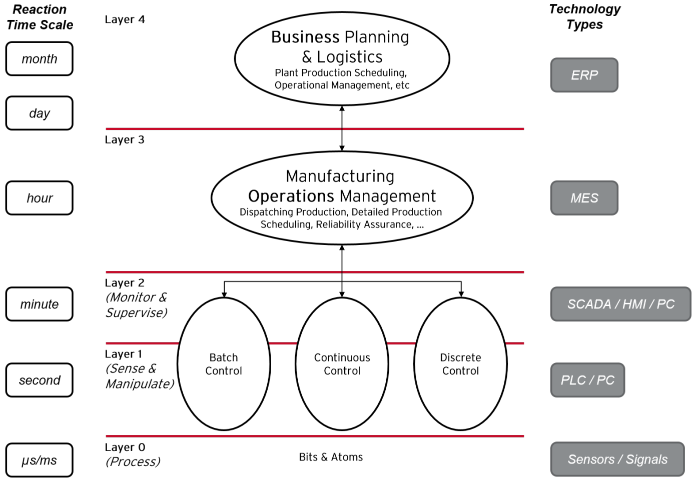
automatic dataflow

Tekinerdogan, B., & Verdouw, C. (2020). Systems Architecture Design Pattern Catalog for Developing Digital Twins. *Sensors* , *20*(18), 5103. https://doi.org/10.3390/s20185103

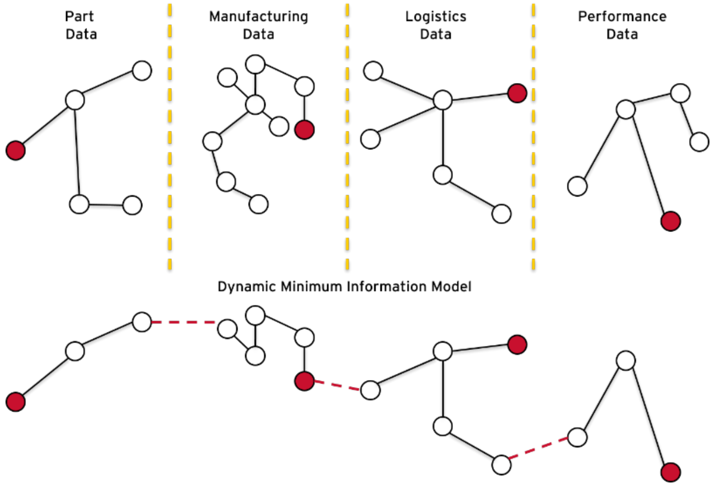
Circa 2020--2021…



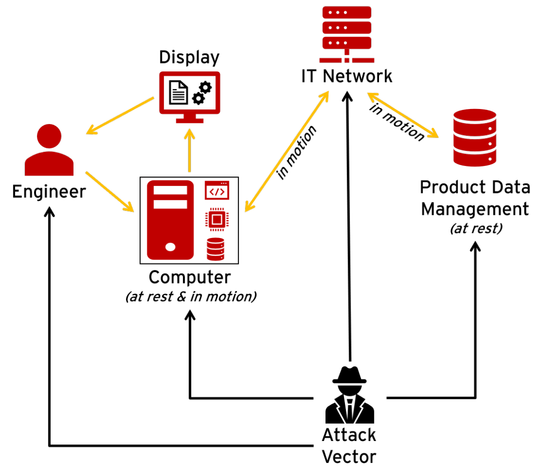
Conceptual Interoperability


Reaction Time Scale
month
day
hour
minute
second
μs/ms
Layer 4
Business Planning & Logistics
Plant Production Scheduling, Operational Management, etc
Layer 3
Manufacturing Operations Management
Dispatching Production, Detailed Production Scheduling, Reliability Assurance, ...
Layer 2 (Monitor & Supervise)
Layer 1 (Sense & Manipulate)
Batch Control
Continuous Control
Discrete Control
Layer 0 (Process)
Bits & Atoms
Technology Types
ERP
MES
SCADA / HMI / PC
PLC / PC
Sensors / Signals

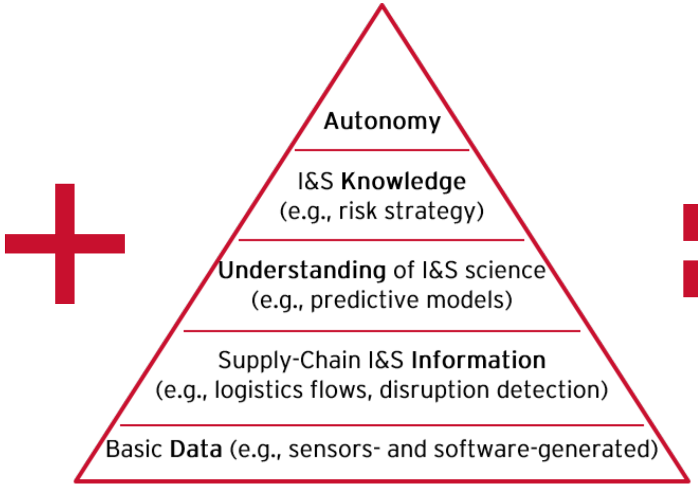
Enterprise Connectivity



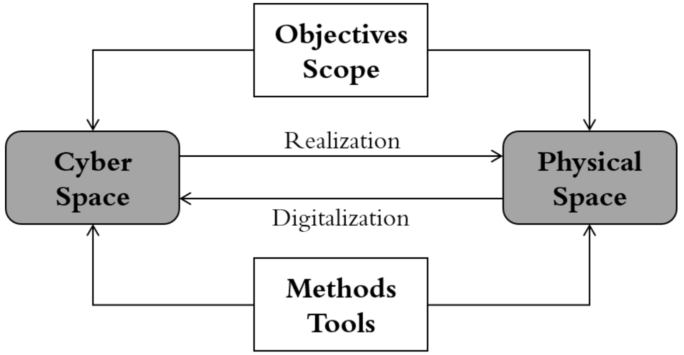
Linked Data



Trust and Traceability


Autonomy
I&S Knowledge
(e.g., risk strategy)
Understanding of I&S science
(e.g., predictive models)
Supply-Chain I&S Information
(e.g., logistics flows, disruption detection)
Basic Data (e.g., sensors- and software-generated)

Autonomous Knowledge Generation



Distributed Digital Twins

References on Slide 28

Recommendations

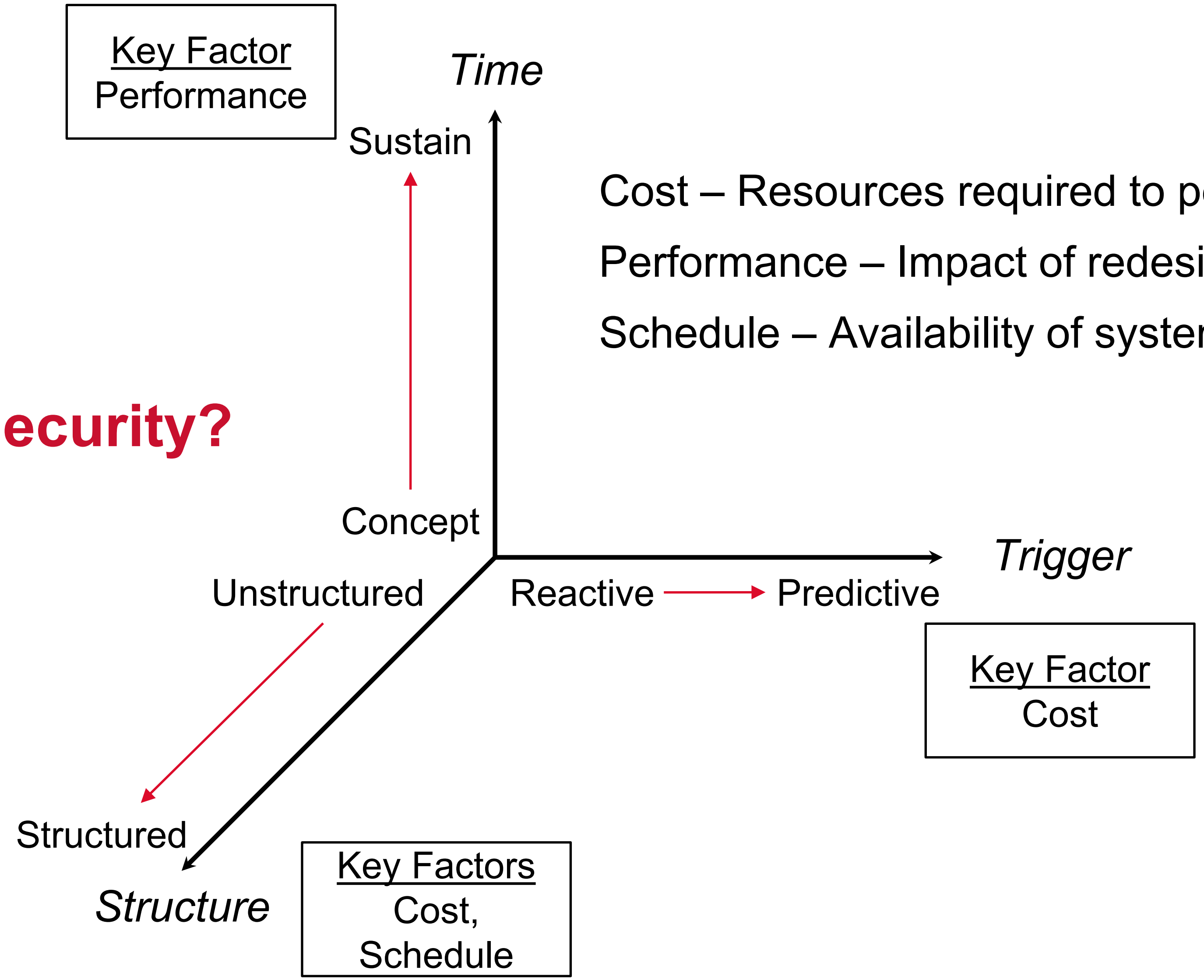
> “ *Policymakers must make a judgment about when to intervene and when to allow market forces to determine exposure to this risk. They must also judge how much they are willing to sacrifice efficiency and effectiveness in cyber systems to enhance security.* ”

-- Richard Danzig
“Surviving on a Diet of Poisoned Fruit”

Potential Approach: *Delivering Uncompromised*

- Three elements that define approach:
  - **Trigger** → Event that initiates a process
  - **Time** → Elapsed from trigger to a activity
  - **Structure** → Degree of standardization of a activity
- Desired approach typically balances **cost**, **schedule**, **performance**
- Growing need to address **security** (e.g., minimize dynamic threats, vulnerabilities, and consequences over time)
- Transition view of integration and maintenance from sunk cost to opportunity to gain value

Strategic Considerations



Cost – Resources required to perform mitigation activity

Performance – Impact of redesign decision to system

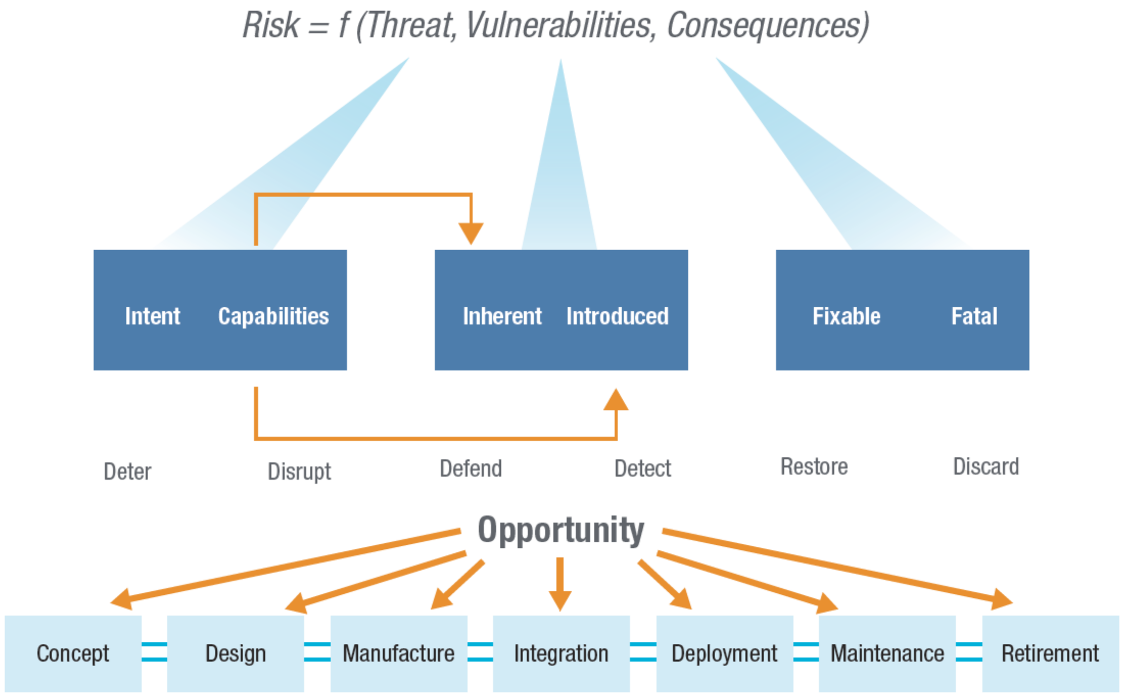
Schedule – Availability of system due to redesign

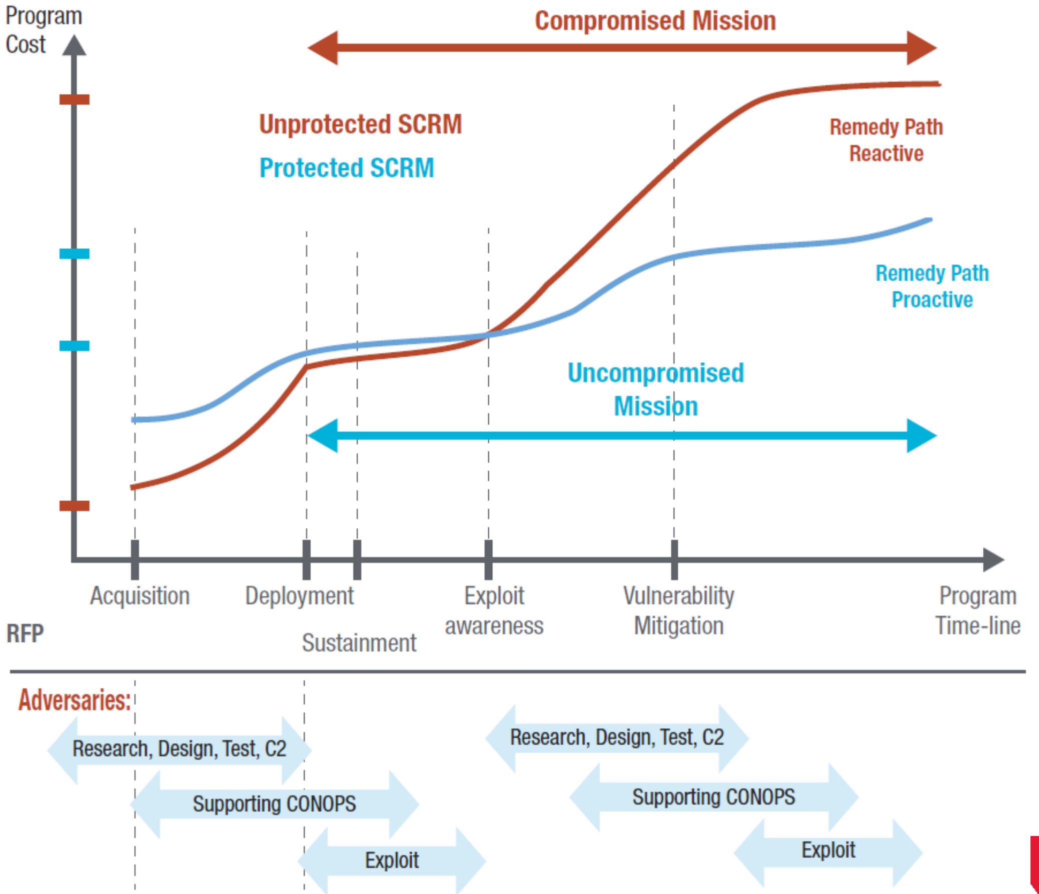
🔒 **Security?**

Deliver & Sustain Uncompromised!

For mission owners, the primary goal of DoD must be to deliver warfighting capabilities to Operating Forces without their critical information and/or technology being wittingly or unwittingly lost, stolen, denied, degraded or inappropriately given away or sold.

--- William Stephens, (Ret.) Director of Counterintelligence, DCSA



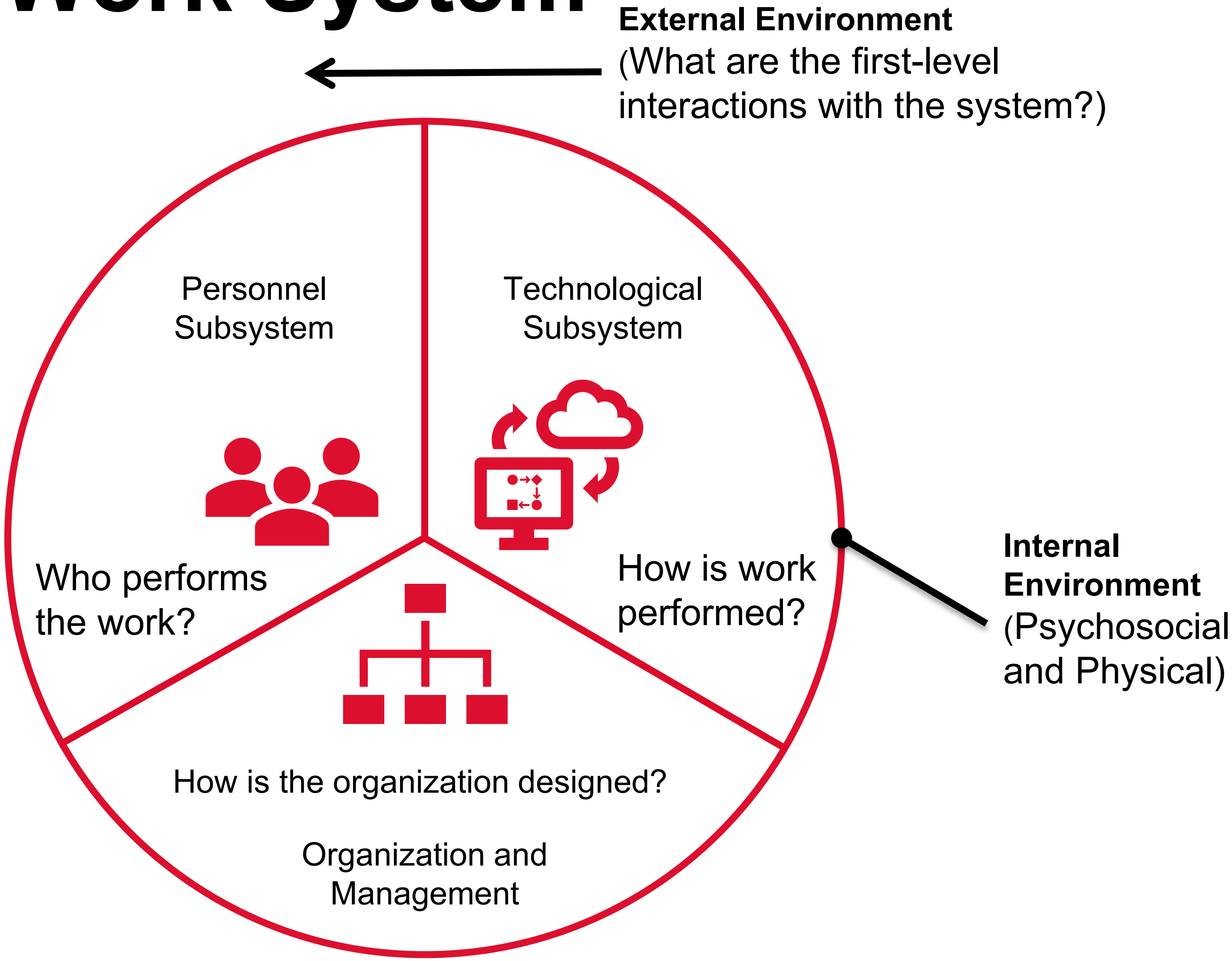


"Make Security a Forth Pillar"

Nissen, C., Gronager, J., Metzger, R., & Rishikof, H. (2018). *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*. The MITRE Corporation.

Redesign the Work System

STS Elements


External Environment
(What are the first-level interactions with the system?)
Personnel Subsystem
Technological Subsystem
Who performs the work?
How is work performed?
How is the organization designed?
Organization and Management
Internal Environment
(Psychosocial and Physical)

Kleiner, B. M. (2008). Macroergonomics: Work System Analysis and Design. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *50*(3), 461–467. https://doi.org/10.1518/001872008X288501

Beyond Robustness: Socio-technical Solutions

Humans must be part of the solution

- Develop stress testing framework for information supply chains leveraging human-machine teaming.

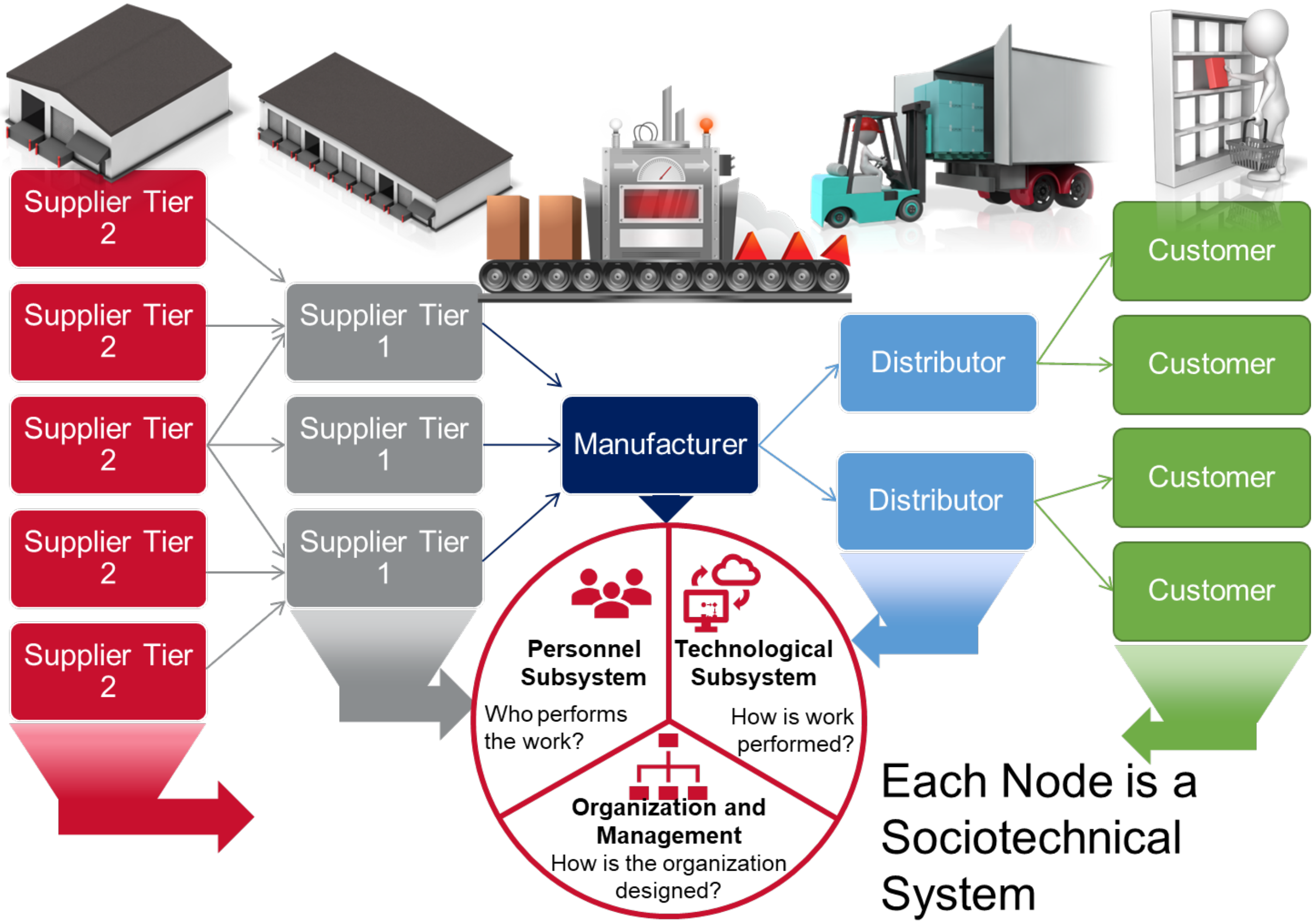
- Develop and deploy contract vehicles for supply chain coordination, in particular addressing system risk.

- Develop design methods, organizational policies, and software to enable socio-technical integration and coordination at an operational level.

Information Supply Chains

Supply Chain Resilience

- Node-level
- Sector-level
- Network-level
- End-to-end
- Full-lifecycle



Each Node is a Sociotechnical System

IT/OT Validation

- Interface between humans, digital, and physical world
- Root of data and control

What is to be made? How to make it?

Information Flows

What was made? How was it made?

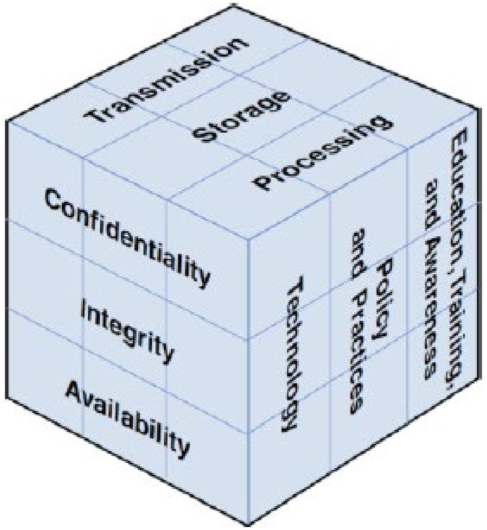
Technical Information Assurance

- Digital Engineering
- Digital Twin
- …

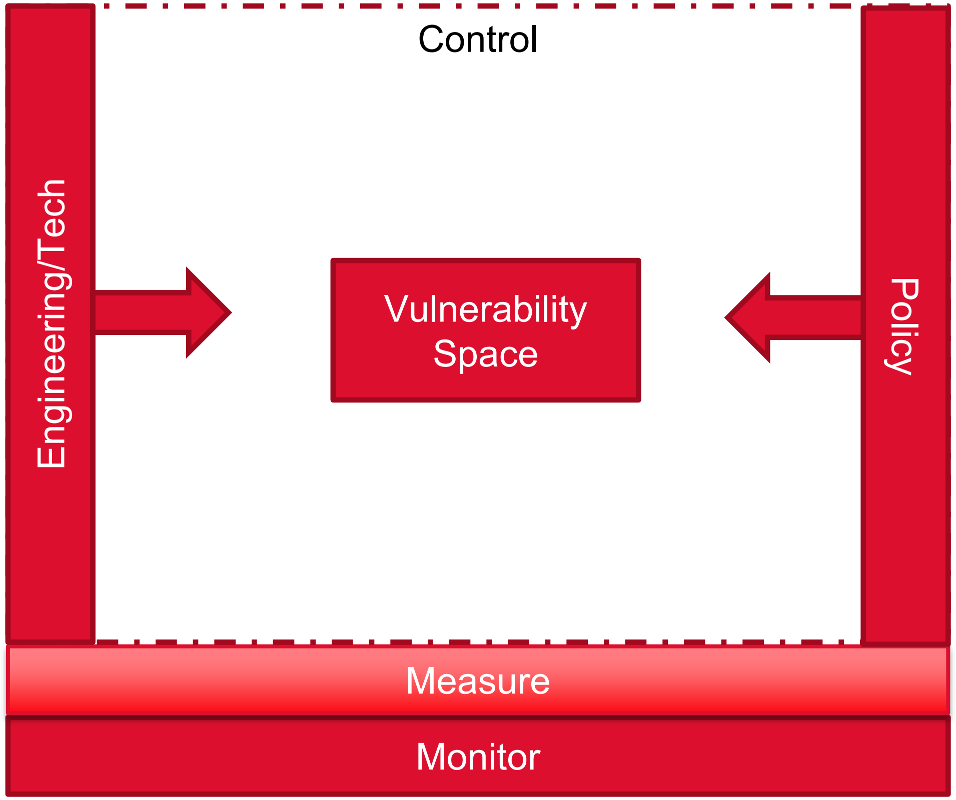
Protection is Not One Size Fits All

- Concerted Industry-wide push to deploy digital engineering to solve cost, quality, & schedule issues.
- From an information assurance perspective, it becomes tightly intertwined with cyber security concerns

A type of information assurance problem where characteristics of the data and process enable semantic/behavioral security to be built into the information system.



https://en.wikipedia.org/wiki/McCumber_cube



Control

Engineering/Tech

Vulnerability Space

Policy

Measure

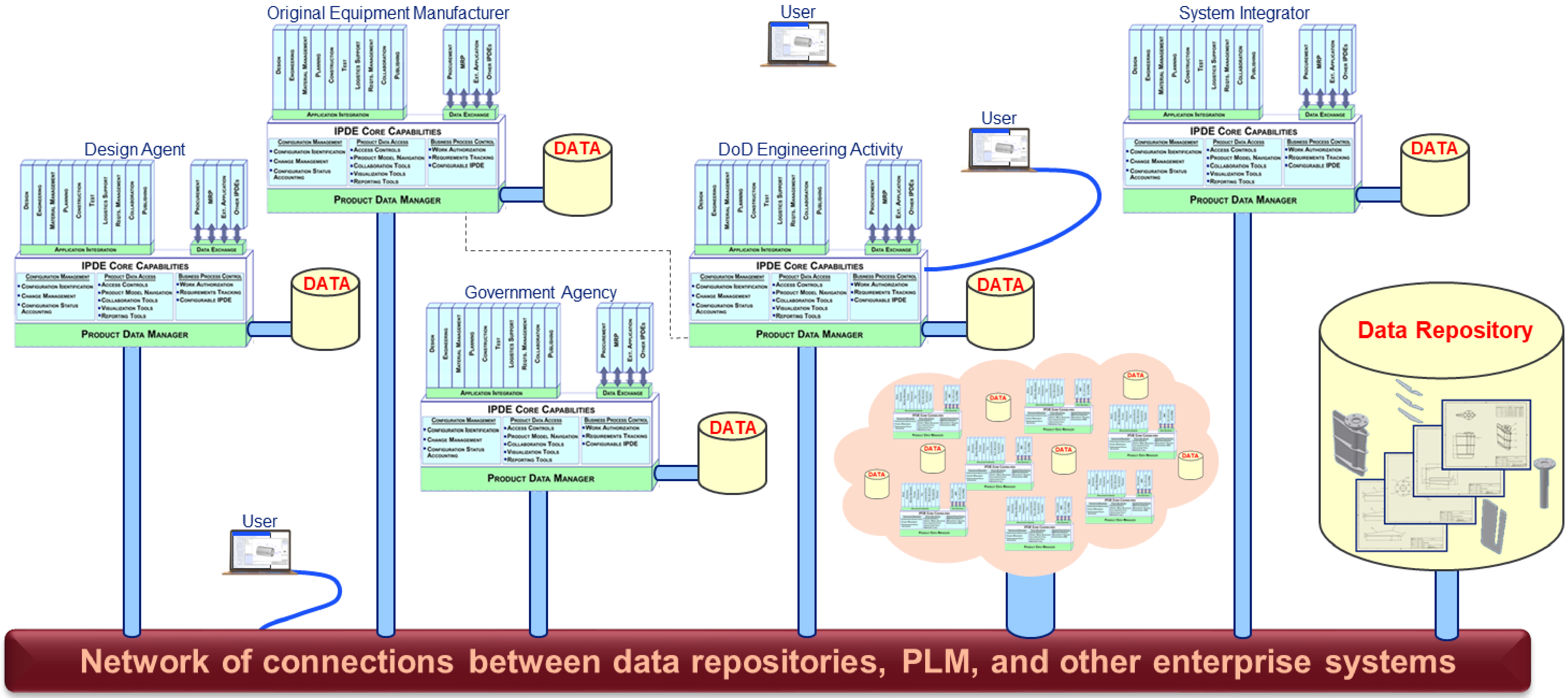
Monitor

- Cybersecurity
- Confidential Computing
- Out-of-band measures
  - Humans-in-the-loop
  - Federated authentication
  - Data zones
- Strategy of Abnegation
  - Forgoing “nice-to-have” features of DE ecosystem to balance risk exposure

Recommendation: decision-makers need to be trained, motivated, and authorized to make trade-offs between risk and other factors

Model-Based Enterprise

has more information than you need to share



Do you need data integration (i.e., connections) or data links (i.e., pointers)?

Closing Thoughts

- There's some baseline stuff that we have to do well. Then, there's harder stuff ... Then, there's the unknown unknowns.

- Information supply chains are vulnerable to disruption and compromise from passive and active threats just like physical supply chains.

- We must be willing to sacrifice efficiency and effectiveness in our systems to enhance the **uncompromisable nature** of those systems

Snapshot About Me

Education

Ph.D., Industrial and Systems Engineering
from Virginia Polytechnic Institute and State University, Blacksburg VA

M.Eng., Engineering Management
from The Pennsylvania State University, University Park PA

B.S., Aeronautical & Astronautical Engineering
Minor in Political Science focused on Science and Technology policy
from Purdue University, West Lafayette IN

Professional Experience

- Current: Research Engineer (VPR & ISR)
- 2014-2020: Program Manager, NIST
- 2005 to 2014, Aerospace Sector, Phoenix AZ

- Internationally known as the Model-Based Enterprise (MBE) Evangelist

More on LinkedIn

Thank you. Questions?

Thomas Hedberg, Ph.D., P.E.

Associate Director for Education Programs

Institute for Systems Research

Mission Director, Acquisition and Industrial Security

Applied Research Laboratory for Intelligence and Security

thedberg@umd.edu

Learn more about Supply Chain Risk and Security at:

Slide 14 References

- **Conceptual Interoperability**
  - Tolk, A., & Muguira, J. A. (2003). The levels of conceptual interoperability model. Proceedings of the 2003 Fall Simulation Interoperability Workshop, 7, 1–11. https://www.sisostds.org/DesktopModules/Bring2mind/DMX/API/Entries/Download?Command=Core_Download&EntryId=24721&PortalId=0&TabId=105
  - Wang, W., Tolk, A., & Wang, W. (2009). The Levels of Conceptual Interoperability Model: Applying Systems Engineering Principles to M&S. Proceedings of the 2009 Spring Simulation Multiconference, 1–9. https://dl.acm.org/doi/abs/10.5555/1639809.1655398
  - Helu, M., Sprock, T., Hartenstine, D., Venketesh, R., & Sobel, W. (2020). Scalable data pipeline architecture to support the industrial internet of things. CIRP Annals. https://doi.org/10.1016/j.cirp.2020.04.006
- **Enterprise Connectivity**
  - Hedberg, T. D., Jr, Manas, B., & Camelio, J. A. (2020). Using graphs to link data across the product lifecycle for enabling smart manufacturing digital threads. Journal of Computing and Information Science in Engineering, 20(1), 1–29. https://doi.org/10.1115/1.4044921
- **Linked Data**
  - Bernstein, W. Z., Hedberg, T. D., Jr, Helu, M., & Feeney, A. B. (2017). Contextualising manufacturing data for lifecycle decision-making. *International Journal of Product Lifecycle Management*, *10*(4), 326. https://doi.org/10.1504/IJPLM.2017.090328
  - Hedberg, T. D., Jr, Feeney, A. B., Helu, M., & Camelio, J. A. (2017). Toward a Lifecycle Information Framework and Technology in Manufacturing. *Journal of Computing and Information Science in Engineering*, *17*(2), 021010. https://doi.org/10.1115/1.4034132
  - Hedberg, T. D., Jr, Manas, B., & Camelio, J. A. (2020). Using graphs to link data across the product lifecycle for enabling smart manufacturing digital threads. *Journal of Computing and Information Science in Engineering*, *20*(1), 1–29. https://doi.org/10.1115/1.4044921
- **Trust and Traceability**
  - Hedberg, T., Jr, Helu, M., Krima, S., & Feeney, A. B. (2020). Recommendations on Ensuring Traceability and Trustworthiness of Manufacturing-Related Data (AMS 300-10). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AMS.300-10
  - Hedberg, T., Jr, Krima, S., & Camelio, J. A. (2019). Method for Enabling a Root of Trust in Support of Product Data Certification and Traceability. Journal of Computing and Information Science in Engineering, 19(4), 041003. https://doi.org/10.1115/1.4042839
- **Autonomous Knowledge Generation**
  - Feng, S. C., Bernstein, W. Z., Hedberg, T., Jr, & Barnard Feeney, A. (2017). Toward Knowledge Management for Smart Manufacturing. Journal of Computing and Information Science in Engineering, 17(3), 031016. https://doi.org/10.1115/1.4037178
- **Distributed Digital Twins**
  - Shao, G., & Helu, M. (2020). Framework for a digital twin in manufacturing: Scope and requirements. Manufacturing Letters, 24, 105–107. https://doi.org/10.1016/j.mfglet.2020.04.004

Disclaimer

Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of the Department of Defense (DoD). Additionally, neither the DoD nor any of its employees make any warranty, expressed or implied, nor assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process included in this publication.

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the ARLIS, the University of Maryland, or the DoD, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.