“Approved for Public Release”

Implementing Zero Trust and Distributed Ledger Technology

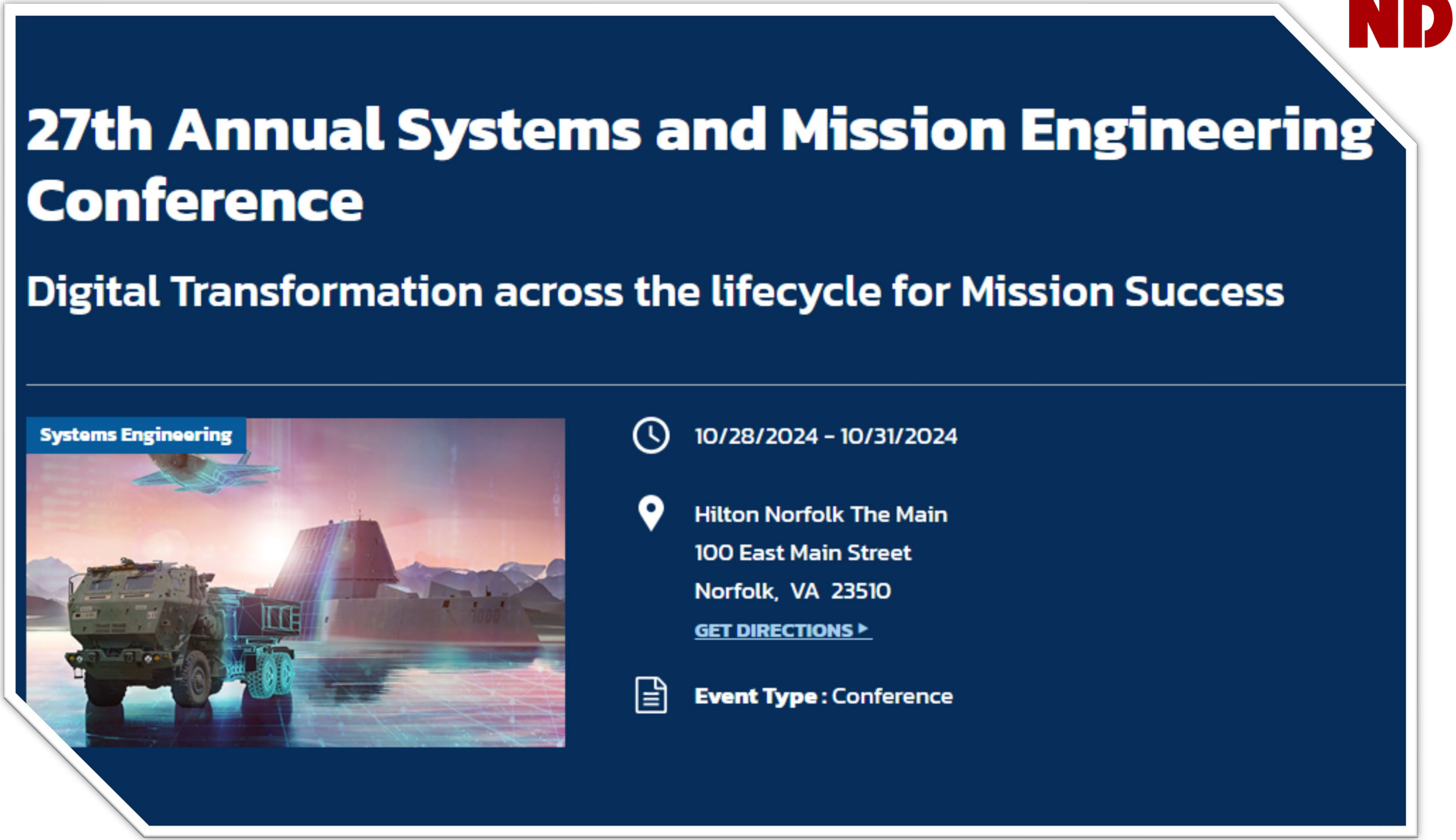
Charles Miller & Santosh Dawesar

27th Annual Systems & Mission Engineering Conference

29 October 2024

“Approved for Public Release”

NDIA



27th Annual Systems and Mission Engineering Conference

Digital Transformation across the lifecycle for Mission Success

Systems Engineering

10/28/2024 – 10/31/2024

Hilton Norfolk The Main
100 East Main Street
Norfolk, VA 23510

GET DIRECTIONS ▸

Event Type : Conference

This document does not contain technology or technical data controlled either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Simple Summary

Title:

Implementing Zero Trust and Distributed Ledger Technology

Short Focus Sentence:

The new normal is necessitating shifts in how secure operations are conducted. This talk offers a discussion centered around Cybersecurity, Zero Trust Architecture (ZTA), and Distributed Ledger Technology (DLT).

Key Terms:

Cybersecurity; Zero Trust; Distributed Ledger; Edge Computing; Machine Learning/Artificial Intelligence (ML/AI).

Simple Summary

Summary

This presentation is framed by discussion of Zero Trust methodologies (ZTM) and applied Distributed Ledger Technology (DLT). The core competencies relevant to this discussion include secure information mobility and affected logistics. Specifically, the exploration and realization through Cyber Modeling & Simulation, with a primary goal of proactively addressing operational resiliency challenges. As exploration evolves, so may our application and use of Machine Learning (ML) and Artificial Intelligence (AI) integrated into autonomous mission support.

Subject matter contexts include defense scenarios for Intelligence, Surveillance, and Reconnaissance (ISR), and communication, which can include space-based assets. These ideas are particularly relevant for supporting **Critical Infrastructure**, where maintaining security and operational resilience is paramount. The implementation of Zero Trust methodologies, Distributed Ledger technology, and integrating and advancing ML/AI systems enhance the protection and efficiency of critical infrastructure support, ensures robust defenses against emerging cyber threats.

Summary

Overview

- Zero Trust Architecture (ZTA) means securing critical infrastructure by enforcing the principles of "Never trust, Always verify". Within the course of this presentation, a summary of how ZTA affects target use cases is offered.

- Distributed Ledger Technology (DLT) can be applied in various asset contexts to enhance security, transparency, and efficiency.

- Cyber Modeling and Simulation (CMS) can significantly enhance Next Generation (NEXGEN) Manufacturing within Industry 5.0 by providing a digital development environment to explore, analyze, test, and optimize systems and strategies.

Overview Presentation Contexts

Core Principles of Zero Trust Architecture

- **Least Privilege Access grants users and devices the minimum level of access necessary to perform functionality**
- **Micro segmentation divides the network into sub-segments which isolate portions of network potentially vulnerable to breaches limiting lateral movement threats.**
- **Continuous Diagnostics and Mitigation (CDM) verifies the identity and trustworthiness of users, devices, and applications regardless of logical location within network**
- **Assume attacker is present in the network and a breach has already occurred necessitating robust and response mechanisms.**

Core Principles of Zero Trust

Zero Trust Implementation Basic Tenants

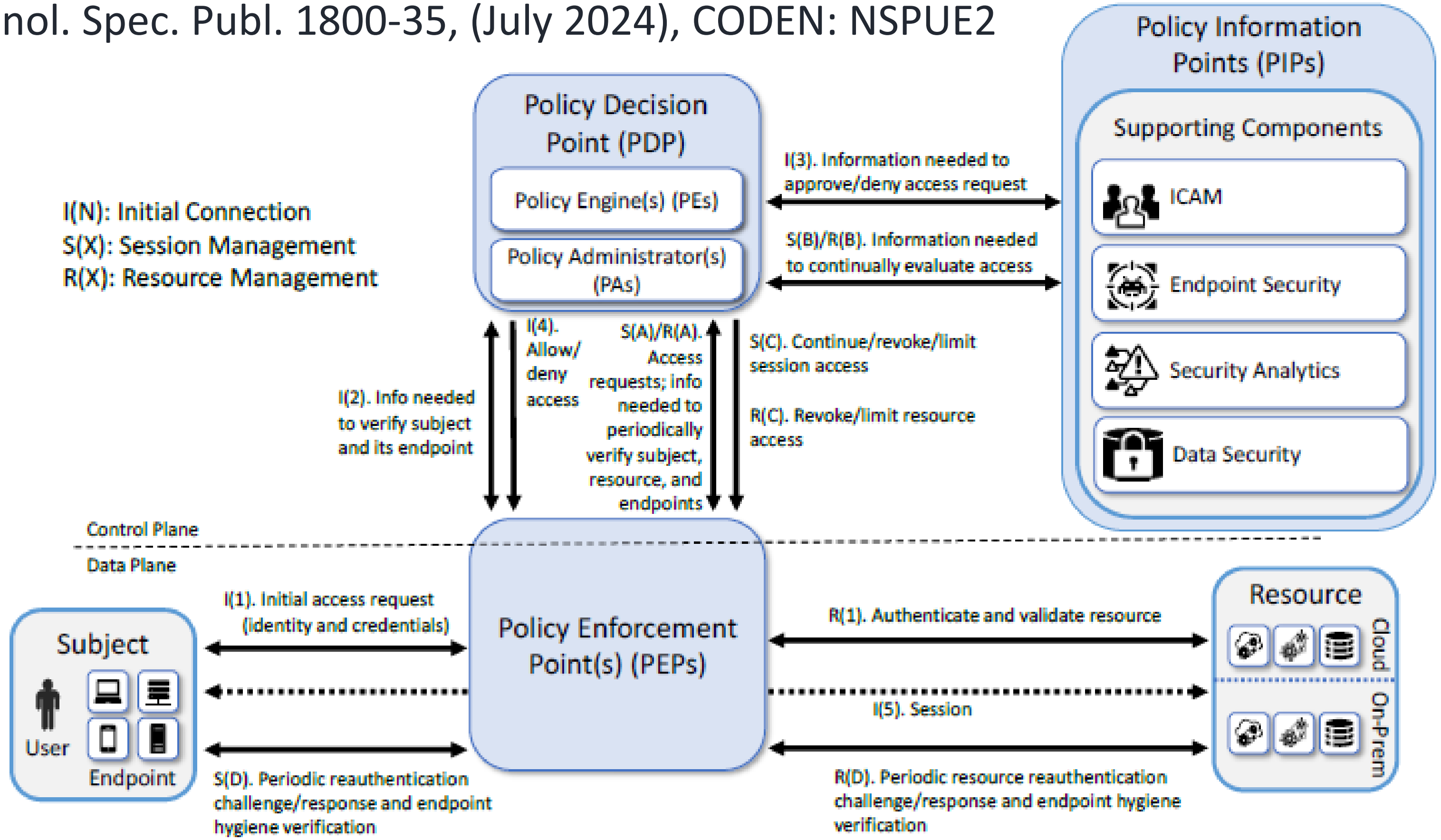
- All data sources and computing services are considered resources
- All communications is secured regardless of network location
- Access to individual enterprise resources is granted on a per-session basis
- Access to resources is determined by policy – including the observable state of multiple behavior and environmental attributes
- Enterprise monitors and measures integrity and security posture of all owned and associated assets
- All resources authenticated and authorized are dynamic and strictly enforced before access is allowed
- The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses to improve security posture

Zero Trust Implementation Tenants

“Approved for Public Release”

General ZTA Reference Architecture – NIST 1800-35

National Institute of Standards and Technology Special Publication 1800-35, Natl. Inst. Stand. Technol. Spec. Publ. 1800-35, (July 2024), CODEN: NSPUE2



I(N): Initial Connection
S(X): Session Management
R(X): Resource Management

Policy Decision Point (PDP)
- Policy Engine(s) (PEs)
- Policy Administrator(s) (PAs)

Policy Information Points (PIPs)

Supporting Components
- ICAM
- Endpoint Security
- Security Analytics
- Data Security

I(3). Information needed to approve/deny access request

S(B)/R(B). Information needed to continually evaluate access

I(2). Info needed to verify subject and its endpoint

I(4). Allow/deny access

S(A)/R(A). Access requests; info needed to periodically verify subject, resource, and endpoints

S(C). Continue/revoke/limit session access

R(C). Revoke/limit resource access

Control Plane

Data Plane

Subject
- User
- Endpoint

I(1). Initial access request (identity and credentials)

Policy Enforcement Point(s) (PEPs)

S(D). Periodic reauthentication challenge/response and endpoint hygiene verification

R(1). Authenticate and validate resource

I(5). Session

R(D). Periodic resource reauthentication challenge/response and endpoint hygiene verification

Resource
- Cloud
- On-Prem

NIST 1800-35 Offers Eight Demonstrative Use Case Examples

This document does not contain technology or technical data controlled either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

"Approved for Public Release"

Zero Trust Methodology w/ Distributed Ledger Technology

Capability

Zero Trust and Distributed Ledger Technology –Connective tech for implementations of Cyber and Space Applications

Decentralized Authority – Can be public, permissioned or private to meet the needs of the case; a permissioned distributed ledger bridges operations within Zero Trust environments

Command & Control (C2) – Distributed Ledger Technology as connection construct for Shared Situation Awareness.

Importance

Key Takeaway – DRAFT NIST 1800-35 Industry use cases

- **Cyber and Cyber-physical contexts we are engaging will continue to evolve, we need to evolve and adapt, implementation methods not third-party solutions is key.**
- **Distributed Ledger systems can help with industry wide compliance, e.g., opt-in proof and tracking, data integrity assurance across supply chains**
- **Architected to support both semi-autonomous and fully-autonomous systems operations, operational decisions at the speed of autonomy**

Developing use cases in Aerospace & Defense Industries: (1) Tracking Parts, (2) Digital exchange (TDPs), orders, deliveries (bill of lading), contracts, change orders,
(3) Additive Manufacturing
(4) Mission Support within Zero-Trust environments

Why the Air Force and Other Services are embracing zero trust now

Implementing a Zero Trust Architecture - NIST 1800-35

WHAT IS ZERO TRUST SECURITY?

NIST Distributed Ledger Technology Resource

Committed to understandable and responsible Artificial Intelligence and Machine Learning

This document does not contain technology or technical data controlled either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Cyber Modeling and Simulation (CMS)

Cyber Modeling and Simulation (CMS) can significantly enhance the effectiveness of operations within NEXGEN Manufacturing and Space-Based assets by providing a virtual environment to test, analyze, and optimize systems and strategies.

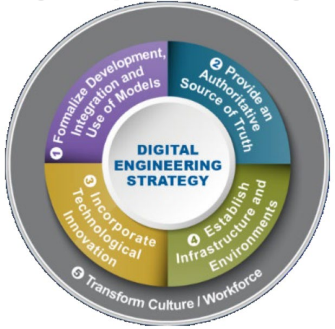
Practical Software and Systems Measurement (PSM) Digital Engineering Measurement Framework

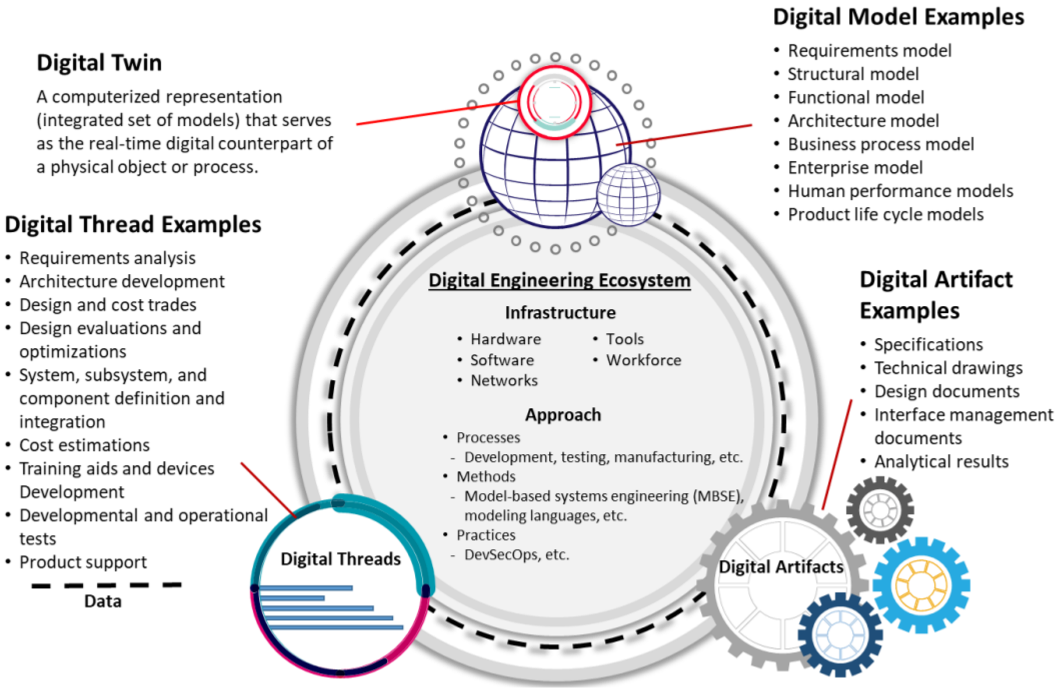
Version 1.1
June 21, 2022

DEBoK
Digital Engineering Body of Knowledge

SYSTEMS ENGINEERING & ARCHITECTURE

SUMMARY OF:
DoD INSTRUCTION 5000.97, “DIGITAL ENGINEERING”
PUBLISHED DECEMBER 21, 2023


DIGITAL ENGINEERING STRATEGY
1 Formalize Development, Integration and Use of Models
2 Provide an Authoritative Source of Truth
3 Incorporate Technological Innovation
4 Establish Infrastructure and Environments
5 Transform Culture / Workforce



Digital Twin

A computerized representation (integrated set of models) that serves as the real-time digital counterpart of a physical object or process.

Digital Model Examples

- Requirements model
- Structural model
- Functional model
- Architecture model
- Business process model
- Enterprise model
- Human performance models
- Product life cycle models

Digital Thread Examples

- Requirements analysis
- Architecture development
- Design and cost trades
- Design evaluations and optimizations
- System, subsystem, and component definition and integration
- Cost estimations
- Training aids and devices Development
- Developmental and operational tests
- Product support

Data

Digital Engineering Ecosystem

Infrastructure

- Hardware
- Software
- Networks
- Tools
- Workforce

Approach

- Processes
  - Development, testing, manufacturing, etc.
- Methods
  - Model-based systems engineering (MBSE), modeling languages, etc.
- Practices
  - DevSecOps, etc.

Digital Artifact Examples

- Specifications
- Technical drawings
- Design documents
- Interface management documents
- Analytical results

Foundations and Resources for Cyber Modeling and Simulation

This document does not contain technology or technical data controlled either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Integrating Distributed Ledger Technology (DLT)

Integrating DLT with CMS further enhances the effectiveness of these simulations by providing secure, transparent, and immutable records of all simulated events and outcomes. This integration ensures that:

- **Data Integrity: All simulation data and results are securely recorded on a blockchain, ensuring that they cannot be tampered with.**
- **Collaboration: Multiple stakeholders can access and verify simulation results in a transparent and trusted manner, facilitating better collaboration and decision-making.**
- **Auditability: The immutable nature of blockchain ensures that all actions and outcomes within the simulations are auditable, providing a clear and trustworthy record for post-simulation analysis.**

Digital Transactions Without Centralized Authority

“Approved for Public Release”

NDIA

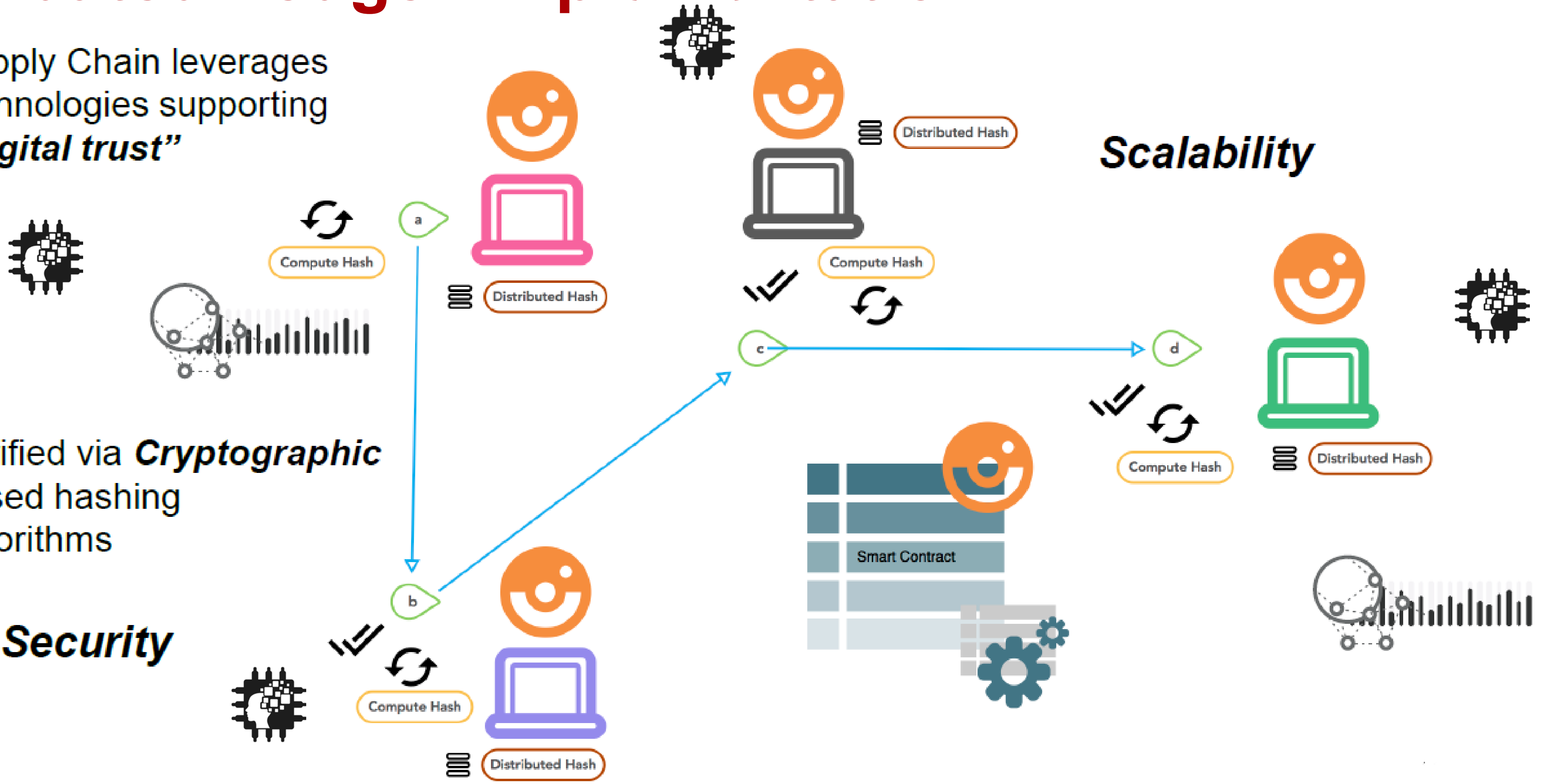
Distributed Ledger Implementation

Supply Chain leverages technologies supporting ***“digital trust”***

Verified via ***Cryptographic*** based hashing algorithms

Security

Scalability



Graphic Workflow Example of Distributed Ledger Implementation

This document does not contain technology or technical data controlled either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Tactically Resilient HMIF Network Capability

- **Human-Machine Integrated Formation (HMIF) Network**
  - Time sensitive
  - Safety critical robotic control data
  - Contested Operational Environment
  - Theoretic Deduction
  - Dynamic Management operational Radio Frequency environment
  - Built upon Modular Open Systems Approach (MOSA)

TECHNOLOGY OBJECTIVE AREA

Architecture, Security & Modularity

ASM-24-03

"The intent of this project is to provide a converged, tactically resilient HMIF network capability for the transport of time sensitive, safety critical robotic control data intermixed with sensor and mission data going between robotic platforms, control vehicles, associated payloads"

Special Notice for DAI OTA, W15QKN-23-9-D001 RPP 24-D18

This document does not contain technology or technical data controlled either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Take Aways

Zero Trust Architecture (ZTA) means securing critical infrastructure by enforcing the principles of “Never trust, Always verify”. Within the course of this presentation, a summary of how ZTA affects target use cases is offered.

Distributed Ledger Technology (DLT) can be applied in various asset contexts to enhance security, transparency, and efficiency.

Cyber Modeling and Simulation (CMS) can significantly enhance Next Generation (NEXGEN) Manufacturing within Industry 5.0 by providing a digital development environment to explore, analyze, test, and optimize systems and strategies.

Wrap Up and Questions

Thank you.

Back Up