Transforming Information Assurance and IT Service Management Through Digital Engineering

Dissertation Proposal Defense

John James Darth Vader Bonar
john.bonar@trojans.dsu.edu

The Beacom College of Computer & Cyber Sciences
Dakota State University
Madison, South Dakota, United States

Spring Research Seminar 2026

Dissertation Committee

Committee Chair
Dr. Patrick Engebretson, PhD

Committee Member
Dr. David Kenley, PhD

Committee Member
Dr. Matthew Kelso, EdD

About the Researcher

- Seven Degrees and Certifications from Dakota State University
- Program Work Environment Solution Engineer & Architect for Collins Aerospace (Part of RTX)
- Daily experience with high-compliance environments: DAAG, JSIG, CNSS, CSFC, CDS
- Research Focus: Digital Engineering for Enterprise IT and Information Assurance
- Bridging systems engineering with enterprise IT and IA practice

Research Abstract

Digital Engineering has transformed how the Department of Defense, NASA, and the aerospace industry design, develop, and sustain complex systems. Its four pillars—MBSE, digital threads, digital twin, and Product Lifecycle Management—have delivered measurable improvements in mission assurance, configuration management, and lifecycle governance.

Despite this proven operational value, these methods remain virtually untested within enterprise IT and information assurance domains. Systematic literature review documents a near-complete absence of academic research applying these proven methods to enterprise IT infrastructure or Information Assurance programs. This study employs quantitative survey methodology to establish baseline empirical data regarding professional awareness and perceived value.

Presentation Agenda

1. Problem Statement and Research Context
2. Research Questions
3. Digital Engineering Foundations (Chapter 1)
4. Literature Review: Analytical Synthesis (Chapter 2)
5. Research Methodology (Chapter 3)
6. Survey Design and Instrument
7. Analytical Approach and Rigor
8. Timeline and Schedule
9. Expected Contributions
10. Questions and Discussion

The Visibility Crisis: A Real-World Scenario

Federal Incident Response: Late 2023

When a vulnerability surfaced within federal information systems, security teams raced to identify every affected component. Weeks passed while agencies struggled to map the blast radius of potential compromise.

The Core Problem: Existing documentation bore no faithful resemblance to actual infrastructure configurations. Defenders challenged with tracing cascading impacts while adversaries retained the initiative.

Current State of Information System Management

Environmental Complexity

Organizations operate within relentless technological evolution: cloud computing, microservices, IoT devices, and operational technology have spawned intricate webs of interdependencies.

Documentation Velocity Mismatch

Static documentation approaches designed for quarterly or annual update cycles cannot maintain accuracy when systems change hourly. The structural mismatch creates systematic failures that compound over time.

Information Assurance Practice Challenges

Key Frameworks

NIST SP 800-37 Rev 2: Risk Management Framework
ISO 31000: Risk Management
NIST Cybersecurity Framework

Critical Challenge: The RMF continuous monitoring requirement exposes limitations of document-centric approaches most directly. Organizations attempting continuous monitoring through manual processes discover the labor exceeds available resources.

IT Service Management Practice Challenges

ITIL Framework Dependencies

Service Strategy — Service Design — Service Transition — Service Operation — Continual Service Improvement

Critical Challenge: Configuration Management Database implementations depend upon accuracy and currency of underlying information—accuracy that organizations consistently fail to achieve. Change management processes suffer when impact assessments rely upon incomplete dependency information.

Evidence: Visibility and Documentation Failures

Finding	Statistic	Source
Visibility Gap Metrics		
IT environment monitorable	66%	IDC/Exabeam 2023
Security teams lacking device visibility	63%	Ponemon Institute 2023
High confidence in device discovery	15%	SANS Institute 2023
Organizations with security/IT silos	55%	Ivanti 2025
Configuration Management Failures		
CMDB implementation failure rate	80%	Gartner Research
Outages from configuration issues	64%	Uptime Institute 2023
Misconfigurations from parameter errors	70-85%	Yin et al. 2011

Evidence: Security Impact Metrics

Finding	Statistic	Source
Shadow IT and Undocumented Assets		
Shadow IT as percentage of IT spend	30-40%	Gartner Research
Cloud services vs. IT estimates	15-22x higher	Cisco 2016
Projected shadow IT usage (2027)	75%	Gartner Research
Security Impact Metrics		
Mean time to identify breach	204 days	IBM/Ponemon 2024
Cloud breaches from misconfigurations	82%	Check Point 2024
Organizations with cloud breaches (18 mo)	95%	CSA 2024
Projected preventable cloud breaches (2027)	99%	Gartner Research

The Documentation-Reality Gap

The persistent gap between documentation and operational reality represents the common thread connecting failures across both domains:

- Security documentation describes control implementations that may not exist as documented
- Configuration databases contain information that no longer reflects system states
- Network diagrams depict architectures that have evolved beyond their documented form

Key Insight: This gap undermines every process that depends upon accurate system information—which includes nearly all Information Assurance and IT Service Management activities. The problem lies not in execution but in inherent limitations of document-centric methodologies.

Research Questions

RQ1: Awareness

To what extent are information technology and information assurance professionals aware of Digital Engineering capabilities, including Model-Based Systems Engineering, digital threads, digital twin technologies, and Product Lifecycle Management principles?

RQ2: Perceived Value

Do information technology and information assurance professionals perceive Digital Engineering capabilities as potentially valuable or important for their work in information assurance, security compliance, and IT service delivery?

RQ3: Anticipated Benefits

Do information technology and information assurance professionals believe that Digital Engineering practices could help them in performing their jobs, meeting compliance requirements, or enhancing organizational capabilities in information assurance and IT service delivery?

Identified Research Gap

The Literature Gap

Systematic literature review documents a near-complete absence of academic research applying proven MBSE and Digital Engineering methodologies to enterprise IT infrastructure, IT Service Management, or Information Assurance programs.

Academic applications exist for: Defense systems, aerospace engineering, unmanned aircraft, military system-of-systems design.

Academic applications absent for: Enterprise IT infrastructure, Information Assurance programs, IT Service Management.

Awareness Deficit: Henderson, McDermott, & Salado (2024) found that 22% of *systems engineering* professionals cannot clearly define MBSE. If awareness barriers persist within the originating discipline, their magnitude among IT/IA professionals demands empirical measurement.

Digital Engineering: Four Pillars

Digital Engineering capabilities address the documentation-reality gap through four integrated pillars:

Model-Based Systems Engineering

Executable models as authoritative system representations

Digital Thread

Authoritative traceability across system lifecycle

Digital Twin

Virtual replicas for development, testing, and validation

Product Lifecycle Management

Integrated lifecycle governance and configuration control

Integration among pillars distinguishes Digital Engineering from isolated tool adoption.

Pillar 1: Model-Based Systems Engineering I

Definition

MBSE shifts from document-centric to model-centric approaches. Models become the authoritative representation of system architecture, requirements, behavior, and interfaces using SysML/UML modeling languages.

Standards and Tools:

- SysML v1 $\rightarrow$ v2 evolution with textual notation and API standardization
- Commercial: Cameo Systems Modeler, IBM Rhapsody
- Open Source: Eclipse Papyrus, Capella, SysON

Application to IA/IT:

- Security architectures with explicit control-asset-threat relationships
- Authorization boundaries as executable models rather than static documents
- Configuration item dependencies modeled with inheritance and traceability

Pillar 2: Digital Thread I

Definition

The digital thread provides authoritative traceability—verified, bidirectional connections between requirements, implementations, test results, and operational configurations throughout the system lifecycle.

Policy Foundation:

- DoD DE Strategy (2018) → DoDI 5000.97 (2023): from strategic vision to mandatory requirement
- SERC digital thread research establishes authoritative source of truth concept

Application to IA/IT:

- RMF compliance chains: requirements → controls → implementation → evidence
- ITIL change impact assessment through traced dependencies
- Automated compliance verification through model-based queries

Pillar 3: Digital Twin I

Definition

Digital twins are virtual replicas of physical or logical systems that maintain synchronization with their real-world counterparts through continuous data exchange. Originated from Grieves' PLM concept; now standardized through ISO 23247 and IEC 62832.

Ecosystem:

- Standards: ISO 23247 reference architecture, NIST IR 8356, IETF network digital twin draft
- Open Source: Eclipse Ditto, BaSyx, Twinbase (Gil 2024: 14 frameworks evaluated)

Application to IA/IT:

- Security scenario simulation and defensive measure testing
- Change validation in as-configured virtual environments before deployment
- Capacity planning and performance analysis for IT service delivery

Pillar 4: Product Lifecycle Management I

Definition

PLM provides frameworks and toolsets for managing information, configurations, changes, service history, processes, and resources throughout the entire system lifecycle from conception through retirement.

Application to IA/IT:

- Configuration baseline management aligned with ITIL principles
- Maps to NIST SP 800-53 controls: CM-2 (baselines), CM-3 (change control), CM-5 (access restrictions)
- Security control maintenance throughout operation and decommissioning
- Bridges information assurance and IT operations through shared authoritative data

Institutional Endorsement of Digital Engineering I

Department of Defense

DE Strategy (2018): Five strategic goals including authoritative source of truth. DoDI 5000.97 (2023) codifies DE as mandatory practice. SE Guidebook (2022) provides implementation guidance.

NASA

HDBK-1004 (2020): DE Acquisition Framework. MBSE Vision document establishes pervasive MBSE adoption path. Independent convergence with DoD validates broad applicability.

INCOSE

Vision 2035: MBSE as dominant paradigm. SE Handbook 5th Ed. (2023). DEIEX Working Group promotes practitioner collaboration.

Institutional Endorsement of Digital Engineering II

SERC / SEBoK / NIST

DECF with 962 KSABs, DE Metrics, and SE Modernization publications. SEBoK defines DE within ISO/IEC/IEEE 15288. NIST CPS Framework (SP 1500-201) addresses systems engineering but not enterprise IT specifically.

Enterprise Architecture: The Unified Architecture Framework I

UAF as Consolidating Standard

ISO/IEC 19540-1:2022 and ISO/IEC 19540-2:2022. Consolidated DoDAF, MODAF, NAF, and commercial frameworks. The specification asserts that 90% of defense framework concepts prove equally applicable in commercial domains.

Comparative Analysis (Bankauskaite 2019)

UAF achieved highest overall rating of 2.8, surpassing TOGAF (2.3), DoDAF (1.9), MODAF (1.8), NAF (1.6), and FEAF (1.2).

Adoption

Endorsed by DoD, NATO (NAF v4), UK MoD. TOGAF complements UAF through joint Open Group-MITRE white paper. SysML integration enables model-based documentation approaches.

Digital Engineering: Measured Evidence I

Return on Investment (Rogers & Mitchell 2021)

Documented 18% improvement in systems engineering efficiency and 9% reduction in defects following MBSE adoption on a complex system-of-systems program. Such measured evidence remains rare but establishes empirical foundation.

Addressing Identified Gaps

- **Authoritative Source of Truth:** Single authoritative model eliminates conflicting documentation
- **Traceability Gap:** Digital thread provides verified connections across lifecycle artifacts
- **Visibility Gap:** Model-based approaches enable comprehensive system visibility
- **Simulation Gap:** Digital twins enable testing without production impact

Digital Engineering: Measured Evidence II

Key Question: Do IT and IA professionals recognize this potential value for their work?

Literature Review: Three Central Arguments I

Chapter 2 examines the research landscape through an analytical narrative organized around three interrelated arguments:

Argument 1: Value Demonstrated but Confined

Digital Engineering has proven value in defense and aerospace—but adoption remains confined to originating sectors with minimal cross-disciplinary transfer.

Argument 2: Barriers Beyond Technical Merit

Adoption barriers are perceptual and organizational, not merely technical. Perceived compatibility, complexity, trialability, and organizational structure mediate adoption decisions.

Argument 3: Parallel Gaps, Untested Solutions

Enterprise IT and IA domains exhibit challenges structurally analogous to those Digital Engineering addresses—yet no research connects these parallel tracks.

Literature Review: Adoption Barriers and Dynamics I

Within Systems Engineering (Call et al. 2024)

Diffusion of Innovations framework applied to MBSE adoption. Perceptions of compatibility, complexity, and trialability mediate adoption decisions among systems engineering professionals.

Organizational Structure (Henderson & Salado 2024)

Organizational flexibility and interconnectedness significantly influence adoption outcomes. Centralization may impede adoption while cross-functional connectivity promotes it.

Awareness Deficits (Henderson, McDermott & Salado 2024)

22% of systems engineering professionals cannot clearly define MBSE. Awareness deficits persist even within the originating discipline—raising the question of whether similar or greater barriers exist in domains that have never encountered these methodologies.

Literature Review: Cross-Disciplinary Transfer I

Barriers to Transfer Beyond Defense/Aerospace

- Platform-centric adoption patterns confine DE to physical systems
- Organizational separation between IT and engineering functions
- Economic factors: no demonstrated ROI outside defense contexts
- Skills gaps: enterprise IT staff lack systems engineering training

Emerging Bridge: DevSecOps Security Assurance

CMU Software Engineering Institute (2023) developed preliminary MBSE reference model for DevSecOps pipeline security—demonstrating technical feasibility for Information Assurance applications, though scope remains narrow.

Literature Review: Cross-Disciplinary Transfer II

Open Source Ecosystem

MBSE (Papyrus, Capella, SysON), digital twins (Eclipse Ditto, BaSyx), and PLM (Aras, OpenPLM) tools exist—but academic research validating enterprise IT application does not.

Research Design Overview I

Quantitative Cross-Sectional Survey Design

- Survey methodology enables standardized data collection supporting statistical analysis
- Cross-sectional design captures professional perceptions at a single point in time
- Anonymous nature encourages candid responses about knowledge gaps

Systems Engineering Approach

The research methodology itself follows a systems engineering lifecycle, demonstrating application of structured engineering principles to research design while ensuring rigorous traceability.

Methodology Justification I

Why Perceptions Matter

Technology Acceptance Model research demonstrates that perceived value influences adoption decisions regardless of demonstrated actual value. Professionals who do not perceive value will not advocate for adoption.

Why Survey Over Case Study

- Case study findings reflect particular organizational contexts
- Survey enables assessment across broad population of practitioners
- Establishes baseline awareness data before implementation research
- Implementation research presumes perceived value—this study tests that presumption

Systems Engineering Research Lifecycle I

1. **Strategic Phase:** Hypothesis, capabilities, constraints, goals, stakeholders
2. **Requirements Phase:** Derived requirements following ISO 15288:2023 standards
3. **Architecture Phase:** High-level outline and structure for survey
4. **Design Phase:** Survey instrument with complete traceability
5. **Results Phase:** Data capture and analysis with model traceability
6. **Report Phase:** Dissertation chapters traced to requirements

Target Population and Sampling I

Target Population

Professionals actively working in IT and Information Assurance roles: IT service delivery, infrastructure management, security operations, compliance management, security architecture.

Sampling Strategy

Non-probability convenience sampling through multiple channels:

- Professional organizations: ISACA, (ISC)^2, ITIL communities
- LinkedIn professional groups
- Industry conferences and professional development events

Sample Size Determination I

Statistical Requirements

Target: 95% confidence level with 5% margin of error

$$n = \frac{Z^2 \times p \times (1-p)}{E^2} = \frac{1.96^2 \times 0.5 \times 0.5}{0.05^2} = 384.16$$

Target Sample

- Minimum required: 385 completed responses
- Target with oversampling: 450 completed responses
- Oversampling accommodates 10-15% incomplete response rates
- Requires distribution to approximately 1,500–1,800 professionals

Survey Instrument Structure I

27 Questions Across Six Sections

1. Awareness and Familiarity with Digital Engineering (2 questions)
2. Understanding of Digital Engineering Capabilities (6 questions)
3. Applicability of Digital Engineering (6 questions)
4. Value Assessment for Information Technology (5 questions)
5. Value Assessment for Information Assurance and Cybersecurity (7 questions)
6. Interest and Demographic Information (4 questions)

Estimated Completion Time: Approximately 10 minutes

Question Format and Scale Selection I

Five-Point Likert Scale

Familiarity Scale: Not at all familiar → Extremely familiar

Agreement Scale: Strongly disagree → Strongly agree

Justification

- Likert scales validated since 1932 for measuring attitudes and perceptions
- Five-point format provides optimal discrimination while remaining cognitively manageable
- Consistent with TAM and UTAUT frameworks for technology acceptance research

Likert Scale Analytical Treatment I

The Ordinal–Interval Debate

Longstanding methodological debate regarding whether Likert responses constitute ordinal or interval data. Norman (2010) and subsequent research demonstrate that parametric methods yield valid results with Likert data even when distributional assumptions are violated.

Dual-Reporting Approach

- **Parametric:** Means and standard deviations reported for composite scores and cross-study comparison
- **Non-parametric:** Medians and interquartile ranges reported alongside for individual Likert items
- Enables readers holding either position to evaluate findings against their preferred framework

Survey-to-Research Question Mapping I

Section	Questions	Research Question
Section 1: Awareness	1.1, 1.2	RQ1: Awareness
Section 2: Understanding	2.1–2.6	RQ1: Awareness
Section 3: Applicability	3.1–3.6	RQ2 / RQ3
Section 4: IT Value	4.1–4.5	RQ3: Anticipated Benefits
Section 5: IA Value	5.1–5.7	RQ3: Anticipated Benefits
Section 6: Demographics	6.1–6.4	Subgroup Analysis

Each question maintains explicit traceability to research questions within the systems engineering model.

Data Analysis: Descriptive and Comparative I

Descriptive Statistics

- Central tendency and dispersion for all Likert-scale responses
- Frequency distributions for categorical and binary responses
- Response pattern visualization across survey sections

Comparative Analysis

- Analysis across professional subgroups (IT vs. IA professionals)
- Analysis across experience levels
- Composite score calculation with Cronbach's alpha reliability assessment

Data Analysis: Inferential Testing and Error Management I

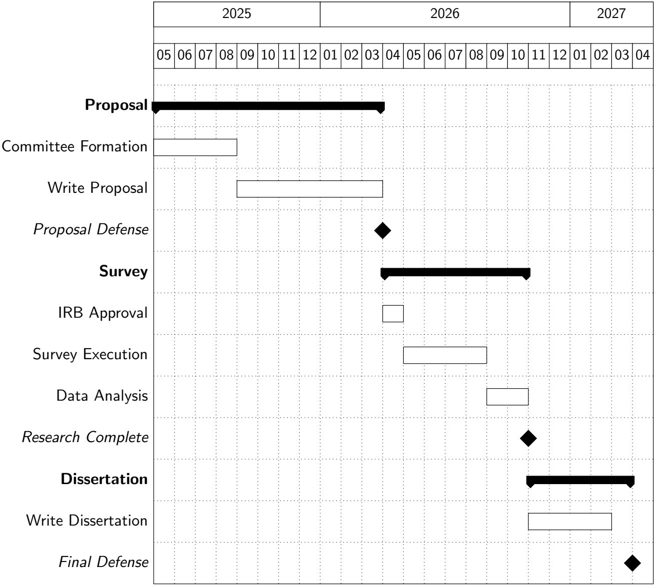
Inferential Statistical Tests

- Parametric (t-tests, ANOVA) or non-parametric alternatives (Mann-Whitney U, Kruskal-Wallis) based on Shapiro-Wilk normality assessment
- Chi-square tests of independence for categorical associations
- Effect sizes reported: Cohen's d for group comparisons, Cramér's V for chi-square

Multiple Comparison Correction

- Holm-Bonferroni sequential correction applied within logical families of related tests
- Effect size assessment ensures observed differences reflect practically meaningful magnitudes

Research Timeline: 22-Month Schedule I



Timeline Phase Details I

Phase 1–2: Proposal (May 2025 – March 2026)

Committee formation (completed January 2026), proposal development, iterative refinement, proposal defense

Phase 3–4: IRB and Survey Execution (April – August 2026)

IRB approval, platform configuration, recruitment through multiple professional channels, data collection targeting 450 responses

Phase 5–6: Analysis and Writing (September 2026 – March 2027)

Data analysis (September–November), results interpretation, dissertation writing, final defense

Validity and Reliability I

Content Validity

Systematic mapping of survey questions to research questions; alignment with established Digital Engineering frameworks from INCOSE, NASA, and DoD

Construct Validity

Question formats and scale anchors drawn from validated TAM and UTAUT instruments

Reliability

Internal consistency assessed through Cronbach's alpha; standardized question format supports response consistency

Pilot Testing and Instrument Refinement I

Spring 2024 Pilot Study

An earlier version of the instrument was administered to IT and information assurance professionals during the Spring 2024 semester. The pilot study evaluated:

- Question clarity and comprehension among target population representatives
- Completion time and respondent fatigue
- Response distribution across scale points (no floor or ceiling effects observed)

Empirical Contributions to Instrument Design

- Question wording refined to balance context with priming avoidance
- Confirmed substantial variation in Digital Engineering awareness across respondents

Response Bias Mitigation I

Proactive Mitigation Strategies

- **Self-selection bias:** Recruitment messaging encourages participation across the awareness spectrum; no prior Digital Engineering knowledge required
- **Acquiescence bias:** Neutral midpoint option and explicit "No" / "Unsure" options on investment willingness questions
- **Social desirability:** Anonymous design (no PII)

Analytical Safeguards

- Wave analysis comparing early and late respondents to assess non-response bias
- Familiarity-stratified comparison of value perceptions to diagnose potential priming effects from contextual descriptions

Research Limitations I

- Non-probability sampling limits generalizability to broader population
- Self-selection bias may over-represent professionals with existing Digital Engineering awareness
- Social desirability bias may influence perceived value responses
- Self-reported awareness may not reflect actual knowledge
- Cross-sectional design captures single point in time
- Survey measures perceived value rather than actual experienced benefits

Expected Contributions: Academic I

Addressing the Literature Gap

- First empirical investigation of Digital Engineering awareness among IT/IA professionals
- Establishes baseline data for future research in this nascent application domain
- Validates or challenges theoretical framework positing DE value for enterprise contexts

Methodological Contribution

Demonstrates systems engineering approach to research design with traceability between questions, instruments, and analysis

Expected Contributions: Industry I

Industry Benefits

- Informs tool vendor and service provider development priorities
- Guides professional development and training initiatives
- Identifies which DE capabilities professionals recognize as addressing their needs
- Indicates whether adoption initiatives would find receptive audiences

Expected Contributions: Commonwealth and Society I

Commonwealth Benefits

- Enhances protection of government systems and critical infrastructure
- Enables rapid, accurate impact assessment for security incidents affecting federal and national security systems
- Reduces compliance verification burden while improving documentation currency

Societal Benefits

- Potentially enable better security capabilities for organizations serving underserved populations
- Democratize sophisticated documentation capabilities beyond large enterprises
- May reduce compliance burden for resource-constrained organizations serving communities with limited resources

Ethical Considerations I

Human Subjects Protection

- **Anonymity:** No personally identifiable information collected
- **Voluntary:** Participation voluntary with no consequences for non-participation
- **Minimal Risk:** Similar to normal daily internet activity
- **Informed Consent:** Obtained through participation notice
- **Data Protection:** Secure storage with encryption

IRB approval will proceed after successful proposal defense.

Proposal Summary I

Research Purpose

Investigate whether IT and Information Assurance professionals recognize potential value in Digital Engineering capabilities for their work

Approach

Quantitative survey methodology with 27 questions targeting 385–450 IT/IA professionals across multiple sectors

Significance

Establishes empirical foundation for strategic decisions regarding Digital Engineering adoption in enterprise IT and Information Assurance domains

Questions and Discussion I

Thank you for attending.

Questions?

Proposal Presentation:
https://github.com/jbone81/DissertationProposalPresentation

Thank You

John James Darth Vader Bonar

john.bonar@trojans.dsu.edu

Committee:
Dr. Patrick Engebretson (Chair)
Dr. David Kenley
Dr. Matthew Kelso

The Beacom College of Computer & Cyber Sciences
Dakota State University

References I

[1] A. Abhaya, “UAF (Unified Architecture Framework) Based MBSE (UBM) Method to Build a System of Systems Model,” *INCOSE International Symposium*, vol. 31, no. 1, pp. 515–530, 2021. DOI: 10.1002/j.2334-5837.2021.00835.x [Online]. Available: https://incose.onlinelibrary.wiley.com/doi/abs/10.1002/j.2334-5837.2021.00835.x

[2] The Aerospace Corporation, *Unified Architecture Framework (UAF)*, Online, 2023. Accessed: Jan. 3, 2025. [Online]. Available: https://aerospace.org/story/unified-architecture-framework-uaf

[3] N. Alhumam et al., “A Comprehensive Review on Cybersecurity of Digital Twins: Issues, Challenges, and Future Research Directions,” *IEEE Access*, vol. 13, pp. 1–25, 2025. DOI: 10.1109/ACCESS.2025.3545004

[4] L. Apvrille and Y. Roudier, “SysML-Sec: A Model Driven Approach for Designing Safe and Secure Systems,” in *2015 3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD)*, IEEE, 2015, pp. 655–664. DOI: 10.5220/0005402006550664

[5] J. Autiosalo, J. Siegel, and K. Tammi, “Twinbase: Open-Source Server Software for the Digital Twin Web,” *IEEE Access*, vol. 9, pp. 140 779–140 798, 2021. DOI: 10.1109/ACCESS.2021.3119487

[6] L. Baker, P. Clemente, B. Cohen, L. Permenter, B. Purves, and P. Salmon, “System Architecture and Model-Based Systems Engineering for Complex Systems Governance,” *Systems Engineering*, vol. 23, no. 3, pp. 345–358, 2020. DOI: 10.1002/sys.21525

[7] J. Bankauskaite, “Comparative Analysis of Enterprise Architecture Frameworks,” in *CEUR workshop proceedings IVUS 2019 international conference on information technologies: proceedings of the international conference on information technologies, Kaunas, Lithuania*, CEUR-WS, vol. 2470, Apr. 2019, pp. 61–64. Accessed: Jan. 3, 2025. [Online]. Available: https://ceur-ws.org/Vol-2470/p19.pdf

[8] C. Banse, I. Kunz, A. Schneider, and K. Weiss, “Cloud Property Graph: Connecting Cloud Security Assessments with Static Code Analysis,” in *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*, IEEE, 2021, pp. 13–19. DOI: 10.1109/CLOUD53861.2021.00014

[9] J. Beese, S. Aier, K. Haki, and R. Winter, “The Impact of Enterprise Architecture Management on Information Systems Architecture Complexity,” *European Journal of Information Systems*, vol. 32, no. 6, pp. 1070–1090, 2023. DOI: 10.1080/0960085X.2022.2103045

References II

[10] H. Benbya and B. McKelvey, “Toward a Complexity Theory of Information Systems Development,” *Information Technology & People*, vol. 19, no. 1, pp. 12–34, 2006. DOI: 10.1108/09593840610649952

[11] H. Benbya, N. Nan, H. Tanriverdi, and Y. Yoo, “Complexity and Information Systems Research in the Emerging Digital World,” *MIS Quarterly*, vol. 44, no. 1, pp. 1–17, 2020. DOI: 10.25300/MISQ/2020/13304 [Online]. Available: https://misq.umn.edu/complexity-and-information-systems-research-in-the-emerging-digital-world.html

[12] F. Bento, M. Tagliabue, and F. Lorenzo, “Organizational Silos: A Scoping Review Informed by a Behavioral Perspective on Systems and Networks,” *Societies*, vol. 10, no. 3, p. 56, 2020. DOI: 10.3390/soc10030056

[13] O. Grabov, *The Future of Open Source in PLM: Can It Solve Key Problems?* Beyond PLM Blog, 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://beyondplm.com/2024/09/23/the-future-of-open-source-in-plm-can-it-solve-key-problems/

[14] B. Bokan and J. Santos, “Managing Cybersecurity Risk Using Threat Based Methodology for Evaluation of Cybersecurity Architectures,” in *2021 Systems and Information Engineering Design Symposium (SIEDS)*, IEEE, 2021, pp. 1–6. DOI: 10.1109/SIEDS52267.2021.9483736

[15] J. Bonar and J. Hastings, “Transforming Information Systems Management: A Reference Model for Digital Engineering Integration,” in *2024 Cyber Awareness and Research Symposium (CARS)*, IEEE, 2024, pp. 1–9. DOI: 10.1109/CARS61786.2024.10778791

[16] M. A. Bone, M. R. Blackburn, D. H. Rhodes, D. N. Cohen, and J. A. Guerrero, “Transforming Systems Engineering Through Digital Engineering,” *The Journal of Defense Modeling and Simulation*, vol. 16, no. 4, pp. 339–355, 2019. DOI: 10.1177/1548512917751873

[17] T. Brée and E. Karger, “Challenges in Enterprise Architecture Management: Overview and Future Research,” *Journal of Governance and Regulation*, vol. 11, no. 2, pp. 8–21, 2022. DOI: doi.org/10.22495/jgrv11i2siart15

[18] C. J. Call et al., “The Effects of the Assessed Perceptions of MBSE on Adoption,” *INCOSE International Symposium*, vol. 34, no. 1, pp. 358–373, 2024. DOI: 10.1002/iis2.13157 [Online]. Available: https://incose.onlinelibrary.wiley.com/doi/10.1002/iis2.13157

References III

[19] D. R. Call and D. R. Herber, “Applicability of the Diffusion of Innovation Theory to Accelerate Model-Based Systems Engineering Adoption,” *Systems Engineering*, vol. 25, no. 6, pp. 574–583, 2022. DOI: 10.1002/sys.21638

[20] J. Campagna, E. Markopoulos, and A. Soylu, “Strategic Adoption of Digital Innovations Leading to Digital Transformation: A Literature Review and Discussion,” *Systems*, vol. 12, no. 4, p. 118, 2024. DOI: 10.3390/systems12040118

[21] D. Cannon, *ITIL: IT Service Management Practices. Volume 1: Service Strategy* (AXELOS - Global Best Practice), 2011 ed., 2nd impr. London, United Kingdom: TSO, The Stationery Office, 2013, ISBN: 978-0-11-331304-4.

[22] Eclipse Foundation, *Capella: Open Source MBSE Tool*, Online, 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://mbse-capella.org/

[23] M. Chami and J.-M. Bruel, “A Survey on Model-Based Systems Engineering: Challenges and Perceptions,” in *Proceedings of the 6th International Conference on Model-Driven Engineering and Software Development*, SCITEPRESS, 2018, pp. 213–220. DOI: 10.5220/0006607802130220 [Online]. Available: https://hal.science/hal-02124402v1/document

[24] Check Point Software Technologies and Cybersecurity Insiders, “2024 cloud security report: Navigating the intersection of cybersecurity and ai,” Check Point Software Technologies Ltd., Tech. Rep., May 2024. Accessed: Jan. 2, 2026. [Online]. Available: https://engage.checkpoint.com

[25] Cybersecurity and Infrastructure Security Agency, “Emergency Directive 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities,” Cybersecurity and Infrastructure Security Agency, Emergency Directive, Jan. 2024. Accessed: Jan. 3, 2025. [Online]. Available: https://www.cisa.gov/news-events/directives/ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities

[26] Cisco Systems, Inc., *You can’t manage what you can’t see: Cisco helps businesses address shadow IT*, Cisco Investor Relations, Jan. 2016. Accessed: Jan. 17, 2026. [Online]. Available: https://investor.cisco.com/news/news-details/2016/You-Cant-Manage-What-You-Cant-See-Cisco-Helps-Businesses-Address-Shadow-IT/default.aspx

References IV

[27] T. A. Chick, S. Pavetti, and N. Shevchenko, "Using Model-Based Systems Engineering (MBSE) to Assure a DevSecOps Pipeline," Carnegie Mellon University Software Engineering Institute, Technical Report CMU/SEI-2023-TR-001, 2023. [Online]. Available: https://www.sei.cmu.edu/documents/6140/Using_MBSE_to_Assure_DevSecOps_Pipelines.pdf

[28] Carnegie Mellon University Software Engineering Institute, "Threat Modeling with Model-Based Systems Engineering (MBSE)," CMU SEI, Technical Note, 2023. Accessed: Jan. 3, 2025. [Online]. Available: https://www.sei.cmu.edu/library/threat-modeling-with-model-based-systems-engineering-mbse/

[29] Committee on National Security Systems, "Security Categorization and Control Selection for National Security Systems," CNSS, Instruction CNSSI 1253, 2022. [Online]. Available: https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[30] L. S. Cook, G. E. Gann, K. V. Ray, and X. Zhang, "IT Service Management Implementation Challenges: A Review," *Issues in Information Systems*, vol. 22, no. 2, pp. 196–208, 2021. DOI: 10.48009/2_iis_2021_196-208 [Online]. Available: https://www.iacis.org/iis/2021/2_iis_2021_196-208.pdf

[31] Cloud Security Alliance, "Cloud Security Study 2024," Cloud Security Alliance, Research Report, Jul. 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://cloudsecurityalliance.org/research/

[32] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, NIST Cybersecurity Framework, 2014. Accessed: Jan. 3, 2025. [Online]. Available: https://www.nist.gov/cyberframework

[33] Defense Acquisition University, *DoD Architecture Framework (DoDAF)*, Acquipedia, 2024. Accessed: Jan. 3, 2025. [Online]. Available: https://www.dau.edu/acquipedia-article/dod-architecture-framework-dodaf

[34] J. C. F. de Winter and D. Dodou, "Five-point Likert items: T test versus Mann-Whitney-Wilcoxon," *Practical Assessment, Research, and Evaluation*, vol. 15, no. 11, pp. 1–12, 2010. DOI: 10.7275/bj1p-ts64

[35] M. Dietz and G. Pernul, "Digital Twin: Empowering Enterprises Towards a System-of-Systems Approach," *IEEE Security & Privacy*, vol. 18, no. 5, pp. 46–53, 2020. DOI: 10.1109/MSEC.2020.2983348

DAKOTA STATE UNIVERSITY

References V

[36] International Council on Systems Engineering (INCOSE), *Digital Engineering Information Exchange Working Group*, Online. Accessed: Jan. 3, 2025. [Online]. Available: https://www.incose.org/communities/working-groups-initiatives/digital-engineering-information-exchange

[37] D. A. Dillman, J. D. Smyth, and L. M. Christian, *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*, 4th. Hoboken, NJ: John Wiley & Sons, 2014, ISBN: 978-1118456149.

[38] Department of Defense, "Digital Engineering Strategy," Office of the Deputy Assistant Secretary of Defense for Systems Engineering, Strategic Document, Jun. 2018. Accessed: Jan. 3, 2025. [Online]. Available: https://ac.cto.mil/digital_engineering/

[39] Office of the Under Secretary of Defense for Research and Engineering, *Systems Engineering Guidebook*. Department of Defense, Feb. 2022. Accessed: Jan. 3, 2025. [Online]. Available: https://ac.cto.mil/wp-content/uploads/2022/02/Systems-Eng-Guidebook_Feb2022-Cleared-slp.pdf

[40] Department of Defense, "DoD Architecture Framework Version 2.02," Department of Defense, Chief Information Officer, Framework Document, 2009. Accessed: Jan. 3, 2025. [Online]. Available: https://dodcio.defense.gov/Library/DoD-Architecture-Framework/

[41] Department of Defense, "DoD Instruction 5000.97: Digital Engineering," Department of Defense, Instruction, Dec. 2023. Accessed: Jan. 3, 2025. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500097p.pdf

[42] Digital Twin Consortium, *Digital Twin Open-Source Collaboration Initiative*, GitHub Repository, 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://www.digitaltwinconsortium.org/initiatives/open-source/

[43] M. Eckhart and A. Ekelhart, "Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook," in *Security and Quality in Cyber-Physical Systems Engineering*, Springer, 2019, pp. 383–412. DOI: 10.1007/978-3-030-25312-7_14 [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-25312-7_14

[44] Eclipse Foundation, *Eclipse BaSyx: Open Source Industry 4.0 Middleware*, Online, 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://eclipse.dev/basyx/

References VI

[45] Eclipse Foundation, *Eclipse Ditto: Open Source Framework for Digital Twins in the IoT*, Online, 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://eclipse.dev/ditto/

[46] Eclipse Foundation, *Papyrus: Open Source UML and SysML Modeling Environment*, Online, 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://eclipse.dev/papyrus/

[47] R. Eichmann, S. Melzer, and R. God, "Model-based Development of a System of Systems Using Unified Architecture Framework (UAF): A Case Study," in *2019 IEEE International Systems Conference (SysCon)*, IEEE, 2019, pp. 1–6. DOI: 10.1109/SYSCON.2019.8836749 [Online]. Available: https://ieeexplore.ieee.org/document/8836749

[48] M. El-Hajj, T. Itäpelto, and T. Gebremariam, "Systematic Literature Review: Digital Twins' Role in Enhancing Security for Industry 4.0 Applications," *Security and Privacy*, vol. 7, no. 5, e396, 2024. DOI: 10.1002/spy2.396

[49] National Aeronautics and Space Administration — Office of the Chief Engineer, "NASA Digital Engineering Acquisition Framework Handbook," National Aeronautics and Space Administration, Washington, DC, Technical Handbook NASA-HDBK-1004, Apr. 2020. [Online]. Available: https://standards.nasa.gov/standard/NASA/NASA-HDBK-1004

[50] W. Fan and Z. Yan, "Factors Affecting Response Rates of the Web Survey: A Systematic Review," *Computers in Human Behavior*, vol. 26, no. 2, pp. 132–139, 2010. DOI: 10.1016/j.chb.2009.10.015

[51] International Organization for Standardization, "ISO 31000:2018 Risk Management — Guidelines," International Organization for Standardization, Standard, 2018. [Online]. Available: https://www.iso.org/standard/65694.html

[52] R. Ross et al., "Security and privacy controls for information systems and organizations," National Institute of Standards and Technology, Gaithersburg, MD, Special Publication (NIST SP) NIST SP 800-53 Rev. 5, Sep. 2020. DOI: 10.6028/NIST.SP.800-53r5 [Online]. Available: https://csrc.nist.gov/pubs/sp/800/53/r5/final

References VII

[53] Forrester Research, "It's Go Time For Application And Infrastructure Dependency Mapping (AIDM)," Forrester Research, Research Report RES141653, 2018. Accessed: Jan. 9, 2025. [Online]. Available: https://www.forrester.com/report/Its-Go-Time-For-Application-And-Infrastructure-Dependency-Mapping-AIDM/RES141653

[54] Forrester Research, *The State of Configuration Management*, Forrester Research Report, 2020.

[55] C. Betz, "CMDB Is Dead—Long Live The IT Management Graph,", Oct. 2025. Accessed: Jan. 9, 2025. [Online]. Available: https://www.forrester.com/blogs/cmdb-is-dead-long-live-the-it-management-graph/

[56] Freshworks, *Change Management Best Practices*, Online, Nov. 2025. Accessed: Jan. 3, 2025. [Online]. Available: https://www.freshworks.com/change-management/best-practices/

[57] S. Friedenthal, A. Moore, and R. Steiner, *A Practical Guide to SysML: The Systems Modeling Language*, 3rd. Morgan Kaufmann, 2014, ISBN: 978-0128002025.

[58] D. Fürstenau, H. Rothe, and M. Sandner, "Leaving the Shadow: A Configurational Approach to Explain Post-Identification Outcomes of Shadow IT Systems," *Business & Information Systems Engineering*, vol. 63, no. 2, pp. 97–111, 2021. DOI: 10.1007/s12599-020-00635-2

[59] Gartner, *Top Threats to Cloud Computing and Security Trends 2024*, Gartner Research, 2024. Accessed: Dec. 21, 2025. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024

[60] Gartner, *Why CMDB Projects Fail and How to Avoid Their Mistakes*, Gartner Research, 2019. Accessed: Jan. 3, 2026. [Online]. Available: https://www.gartner.com/en/documents/3970851

[61] Gartner, *CMDB Data Quality: Critical Success Factors*, Gartner Research, 2020. Accessed: Oct. 21, 2025. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/cmdb-configuration-management-database

[62] Gartner, *Shadow IT: The Risks and How to Manage Them*, Gartner Research, 2022. Accessed: Jan. 3, 2026. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/shadow-it

References VIII

[63] S. Gil, P. H. Mikkelsen, C. Gomes, and P. G. Larsen, "Survey on open-source digital twin frameworks — a case study approach," *Software: Practice and Experience*, vol. 54, no. 6, pp. 929–960, DOI: https://doi.org/10.1002/spe.3305 eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/spe.3305.

[64] J. Gregory, L. Berthoud, T. Tryfonas, and A. Sherlock, "Model Based Engineering (MBE): An Examination of Current Practice in UK Defence," in *INCOSE International Symposium*, vol. 29, 2019, pp. 614–628. DOI: 10.1002/j.2334-5837.2019.00623.x

[65] M. Grieves, "Digital Twin: Manufacturing Excellence through Virtual Factory Replication," *Digital Twin*, vol. 3, pp. 1–35, 2023. DOI: 10.12688/digitaltwin.17469.2

[66] A. A. Hassan and W. M. Bahgat, "A Framework for Translating a High Level Security Policy into Low Level Security Mechanisms," in *2009 IEEE/ACS International Conference on Computer Systems and Applications*, IEEE, May 2009, pp. 504–511. DOI: 10.1109/AICCSA.2009.5069371

[67] M. Hauder, F. Matthes, and S. Roth, "Challenges for Automated Enterprise Architecture Documentation," in *Lecture Notes in Business Information Processing*, vol. 131, Springer, 2012, pp. 21–39. DOI: 10.1007/978-3-642-34163-2_2

[68] M. Hause, "Evaluation of the DoDAF Meta-model's Support of Systems Engineering," in *Procedia Computer Science*, vol. 61, Elsevier, 2015, pp. 254–260. DOI: 10.1016/j.procs.2015.09.208

[69] K. Henderson, T. McDermott, and A. Salado, "MBSE Adoption Experiences in Organizations: Lessons Learned," *Systems Engineering*, vol. 27, no. 1, pp. 214–239, 2024. DOI: 10.1002/sys.21717 Accessed: Nov. 11, 2025.

[70] K. Henderson and A. Salado, "Value and Benefits of Model-Based Systems Engineering (MBSE): Evidence from the Literature," *Systems Engineering*, vol. 24, no. 1, pp. 51–66, 2021. DOI: 10.1002/sys.21566 Accessed: Aug. 3, 2025.

[71] K. Henderson and A. Salado, "The Effects of Organizational Structure on MBSE Adoption in Industry: Insights from Practitioners," *Engineering Management Journal*, vol. 36, no. 1, pp. 117–143, 2024. DOI: 10.1080/10429247.2023.2210494 Accessed: Jan. 3, 2026.

References IX

[72] J. Huff, H. Medal, and K. Griendling, "A Model-Based Systems Engineering Approach to Critical Infrastructure Vulnerability Assessment and Decision Analysis," *Systems Engineering*, vol. 22, no. 3, pp. 214–231, 2019. DOI: 10.1002/sys.21460

[73] N. Hutchinson et al., *WRT-1006 Technical Report: Developing the Digital Engineering Competency Framework (DECF) Phase 2*. Systems Engineering Research Center, 2021. Accessed: Nov. 17, 2023. [Online]. Available: https://sercproddata.s3.us-east-2.amazonaws.com/technical_reports/reports/1616668486.A013_SERC%20WRT%201006_Technical%20Report%20SERC-2021-TR-005_FINAL.pdf

[74] N. Hutchison et al., *WRT-1001: Digital Engineering Metrics*. Systems Engineering Research Center, 2020. Accessed: Nov. 17, 2023. [Online]. Available: https://sercuarc.org/wp-content/uploads/2020/06/SERC-TR-2020-002-DE-Metrics-6-8-2020.pdf

[75] IBM, *The Cost of Poor Data Quality*, IBM Research, 2020. Accessed: Jan. 17, 2026. [Online]. Available: https://www.ibm.com/thought-leadership/institute-business-value/

[76] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2024," IBM Corporation, Research Report, Jul. 2024. Accessed: Jan. 9, 2026. [Online]. Available: https://www.ibm.com/reports/data-breach

[77] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2025," IBM Corporation, Research Report, 2025. Accessed: Jan. 9, 2026. [Online]. Available: https://www.ibm.com/reports/data-breach

[78] IDC and Exabeam, "The State of Threat Detection, Investigation, and Response," IDC, Research Report, 2023. Accessed: Jan. 3, 2026. [Online]. Available: https://www.exabeam.com/wp-content/uploads/REPORT-Exabeam-The-State-of-TDIR-2023-NA-EN.pdf

[79] IETF Network Management Research Group, *Network Digital Twin Architecture*, Internet-Draft, 2024. Accessed: Jan. 3, 2025. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-nmrg-network-digital-twin-arch/

[80] International Council on Systems Engineering, *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, 5th. Wiley, 2023, ISBN: 978-1119814290. DOI: 10.1002/9781119814436

DAKOTA STATE UNIVERSITY

References X

[81] International Council on Systems Engineering, *Systems Engineering Vision 2035*. International Council on Systems Engineering, 2021. Accessed: Jan. 3, 2025. [Online]. Available: https://www.incose.org/about-systems-engineering/se-vision-2035

[82] Information Systems Audit and Control Association (ISACA), *COBIT 2019 Framework: Introduction and Methodology*. Schaumburg, IL: Information Systems Audit and Control Association, 2018, ISBN: 978-1-60420-644-9.

[83] International Organization for Standardization, "ISO 23247: Automation Systems and Integration – Digital Twin Framework for Manufacturing," International Organization for Standardization, Standard, 2021. [Online]. Available: https://www.iso.org/standard/75066.html

[84] International Organization for Standardization, "Information technology - Service management - Part 1: Service management system requirements," International Organization for Standardization, Standard ISO/IEC 20000-1:2018, Sep. 2018.

[85] International Organization for Standardization, "ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements," International Organization for Standardization, Standard, 2022. DOI: 10.1109/IEEESTD.2023.10123367 [Online]. Available: https://www.iso.org/standard/27001

[86] IT Process Institute, "The Visible Ops Handbook: Implementing ITIL in 4 Practical and Auditable Steps," IT Process Institute, Handbook, 2004.

[87] AXELOS Limited, *ITIL Foundation: ITIL 4th Edition*. Norwich, UK: The Stationery Office (TSO), 2019, Official ITIL 4 Guidance, ISBN: 9780113316076.

[88] Ivanti, "State of Cybersecurity Trends Report 2025," Ivanti, Research Report, 2025. Accessed: Jan. 9, 2026. [Online]. Available: https://www.ivanti.com/resources/research-reports/state-of-cybersecurity-report

[89] Cybersecurity and Infrastructure Security Agency, *Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways — CISA*, Government Cybersecurity Advisory, Washington, District of Columbia, Feb. 2024. Accessed: Jan. 17, 2026. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

References XI

[90] S. Jamieson, "Likert scales: How to (ab)use them," *Medical Education*, vol. 38, no. 12, pp. 1217–1218, 2004. DOI: 10.1111/j.1365-2929.2004.02012.x

[91] K. P. Joshi, L. Elluri, and A. Nagar, "An Integrated Knowledge Graph to Automate Cloud Data Compliance," *IEEE Access*, vol. 8, pp. 148 541–148 555, 2020. DOI: 10.1109/ACCESS.2020.3008964

[92] H. J. Junior and G. H. Travassos, "Consolidating a common perspective on technical debt and its management through a tertiary study," *Information and Software Technology*, vol. 149, p. 106 964, 2022, ISSN: 0950-5849. DOI: https://doi.org/10.1016/j.infsof.2022.106964 Accessed: Mar. 15, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950584922001057

[93] E. Karaarslan and M. Babiker, "Digital Twin Security Threats and Countermeasures: An Introduction," in *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, IEEE, 2021, pp. 7–11. DOI: 10.1109/ISCTURKEY53027.2021.9654360

[94] L. U. Khan, W. Saad, D. Niyato, Z. Han, and C. S. Hong, "Digital-Twin-Enabled 6G: Vision, Architectural Trends, and Future Directions," *IEEE Communications Magazine*, vol. 60, no. 1, pp. 74–80, 2022. DOI: 10.1109/MCOM.001.21143

[95] Z. Kleinwaks, "Technical Debt in Systems Engineering: A Systematic Literature Review," *Systems Engineering*, vol. 26, no. 6, pp. 710–726, 2023. DOI: 10.1002/sys.21681

[96] S. Klotz, A. Kopper, M. Westner, and S. Strahringer, "Causing Factors, Outcomes, and Governance of Shadow IT and Business-Managed IT: A Systematic Literature Review," *International Journal of Information Systems and Project Management*, vol. 7, no. 1, pp. 15–43, 2019. DOI: 10.12821/ijispm070102

[97] S. Kotusev, "Enterprise Architecture and Enterprise Architecture Artifacts: Questioning the Old Concept in Light of New Findings," *Journal of Information Technology*, vol. 34, no. 2, pp. 102–128, 2019. DOI: 10.1177/0268396218816273

[98] I. Koufos, M. Christopoulou, G. Xilouris, M.-A. Kourtis, M. Souvalioti, and P. Trakadas, "Towards the Automation of Attack Graph-Based Risk Assessment with OSCAL," in *Distributed Computing and Artificial Intelligence, Special Sessions I (DCAI 2024)*, ser. Lecture Notes in Networks and Systems, vol. 1198, Springer, 2025, pp. 319–328. DOI: 10.1007/978-3-031-76459-2_30

References XII

[99] S. Kurnia, S. Kotusev, G. Shanks, R. Dilnutt, and S. Milton, "Stakeholder Engagement in Enterprise Architecture Practice: What Inhibitors Are There?" *Information and Software Technology*, vol. 134, p. 106 536, 2021. DOI: 10.1016/j.infsof.2021.106536

[100] J. Campos, J. Kortelainen, and E. Jantunen, "Industrial Open Source Solutions for Product Life Cycle Management," *Cogent Engineering*, vol. 1, no. 1, pp. 1–15, Aug. 2014. DOI: 10.1080/23311916.2014.939737

[101] Z. Li, P. Avgeriou, and P. Liang, "A Systematic Mapping Study on Technical Debt and Its Management," *Journal of Systems and Software*, vol. 101, pp. 193–220, 2015. DOI: 10.1016/j.jss.2014.12.027

[102] N. Liu, J. Wang, Y. Zhang, D. Li, and M. Ju, "Top-down military system-of-systems design using MBSE based on UAF: A case study," in *Complex Systems Design & Management*, D. Krob, L. Li, X. Zhang, J. Yao, and M. Guo, Eds., Singapore: Springer Nature Singapore, 2023, pp. 210–219, ISBN: 978-981-99-6511-3. DOI: 10.1007/978-981-99-6511-3_19

[103] A. M. Madni and M. Sievers, "Model-Based Systems Engineering: Motivation, Current Status, and Research Opportunities," *Systems Engineering*, vol. 21, no. 3, pp. 172–190, 2018. DOI: 10.1002/sys.21438

[104] A. M. Madni and M. Sievers, "Leveraging Digital Twin Technology in Model-Based Systems Engineering," *Systems*, vol. 6, no. 1, p. 7, 2018. DOI: 10.3390/systems6010007 [Online]. Available: https://www.mdpi.com/2079-8954/6/1/7

[105] M. Marrone and L. M. Kolbe, "Impact of IT Service Management Frameworks on the IT Organization," *Business & Information Systems Engineering*, vol. 3, no. 1, pp. 5–18, 2011. DOI: 10.1007/s12599-010-0141-5 [Online]. Available: https://link.springer.com/article/10.1007/s12599-010-0141-5

[106] D. Mažeika and R. Butleris, "Integrating Security Requirements Engineering into MBSE: Profile and Guidelines," *Security and Communication Networks*, vol. 2020, pp. 1–12, 2020. DOI: 10.1155/2020/5137625

References XIII

[107] H. Myrbakken and R. Colomo-Palacios, "DevSecOps: A Multivocal Literature Review," in *Software Process Improvement and Capability Determination (SPICE 2017)*, ser. Communications in Computer and Information Science, vol. 770, Springer, 2017, pp. 17–29. DOI: 10.1007/978-3-319-67383-7_2

[108] National Aeronautics and Space Administration, "NASA Digital Engineering Acquisition Framework Handbook," NASA, Handbook NASA-HDBK-1004, Apr. 2020. Accessed: Jan. 3, 2025. [Online]. Available: https://standards.nasa.gov/standard/NASA/NASA-HDBK-1004

[109] National Aeronautics and Space Administration, "Future Model-Based Systems Engineering Vision and Strategy Bridge for NASA," NASA, Technical Memorandum NASA/TM-20210014025, 2021. Accessed: Jan. 3, 2025. [Online]. Available: https://ntrs.nasa.gov/citations/20210014025

[110] NATO, "NATO Architecture Framework Version 4," North Atlantic Treaty Organization, Architecture Framework, 2018. Accessed: Jan. 3, 2025. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_157575.htm

[111] National Defense Industrial Association Systems Engineering Division, "Evaluation of DoDAF Meta-model Support for Systems Engineering," National Defense Industrial Association, Technical Report, 2011.

[112] P. H. Nguyen, S. Ali, and T. Yue, "Model-Based Security Engineering for Cyber-Physical Systems: A Systematic Mapping Study," *Information and Software Technology*, vol. 83, pp. 116–135, 2017. DOI: 10.1016/j.infsof.2016.11.004

[113] National Institute of Standards and Technology, "Framework for Cyber-Physical Systems: Volume 1, Overview," NIST, Special Publication NIST SP 1500-201, 2017. DOI: 10.6028/NIST.SP.1500-201 [Online]. Available: https://www.nist.gov/publications/framework-cyber-physical-systems-volume-1-overview

[114] M. Helu and T. Hedberg, "Security and Trust Considerations for Digital Twin Technology," National Institute of Standards and Technology, Internal Report NIST IR 8356, 2025. DOI: 10.6028/NIST.IR.8356 [Online]. Available: https://csrc.nist.gov/pubs/ir/8356/final

[115] National Institute of Standards and Technology, "Open Security Controls Assessment Language (OSCAL)," NIST, Technical Specification, 2023. Accessed: Jan. 3, 2025. [Online]. Available: https://pages.nist.gov/OSCAL

References XIV

[116] National Institute of Standards and Technology, "Guide for Security-Focused Configuration Management of Information Systems," National Institute of Standards and Technology, Special Publication 800-128, 2019. DOI: 10.6028/NIST.SP.800-128 [Online]. Available: https://csrc.nist.gov/pubs/sp/800/128/final

[117] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," National Institute of Standards and Technology, Special Publication 800-160 Vol. 2 Rev. 1, Dec. 2021. DOI: 10.6028/NIST.SP.800-160v2r1 [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final

[118] Joint Task Force Transformation Initiative, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," National Institute of Standards and Technology, Special Publication NIST Special Publication (SP) 800-37, Rev. 2, Dec. 2018. DOI: 10.6028/NIST.SP.800-37r2

[119] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, "Developing cyber-resilient systems: A systems security engineering approach," National Institute of Standards and Technology, NIST Special Publication (SP) 800-160 Vol. 2 Rev. 1, Dec. 2021. DOI: 10.6028/NIST.SP.800-160v2r1 [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final

[120] G. Norman, "Likert scales, levels of measurement and the "laws" of statistics," *Advances in Health Sciences Education*, vol. 15, no. 5, pp. 625–632, 2010. DOI: 10.1007/s10459-010-9222-y

[121] Object Management Group, "Unified Architecture Framework (UAF) Specification Version 1.2," Object Management Group, Standard ISO/IEC 19540-1:2022 and ISO/IEC 19540-2:2022, 2022. Accessed: Jan. 3, 2025. [Online]. Available: https://www.omg.org/spec/UAF/1.2

[122] Object Management Group, *About the Unified Architecture Framework Specification*, Online, 2024. Accessed: Jan. 3, 2025. [Online]. Available: https://www.omg.org/spec/UAF/About-UAF/

[123] Object Management Group, "Unified Architecture Framework (UAF) Domain Metamodel Version 1.2," Object Management Group, Specification, 2022. Accessed: Jan. 3, 2025. [Online]. Available: https://www.omg.org/spec/UAF/1.2/DMM

References XV

[124] M. Hause, G. Bleakley, and A. Morkevicius, "Technology Update on the Unified Architecture Framework (UAF)," Object Management Group, Conference Paper, 2017. DOI: 10.1002/j.2334-5837.2015.00066.x

[125] The Open Group and MITRE Corporation, "Using TOGAF to Define and Govern Service-Oriented Architectures," The Open Group, White Paper, 2013. [Online]. Available: https://www.opengroup.org/togaf

[126] Ponemon Institute, "Global Study on Closing the IT Security Gap," Ponemon Institute, Research Report, 2023. Accessed: Jan. 9, 2025. [Online]. Available: https://ponemonsullivanreport.com/2023/07/closing-the-it-security-gap-what-are-high-performers-doing-differently

[127] R. N. Rajapakse, M. Zahedi, M. A. Babar, and H. Shen, "Challenges and Solutions When Adopting DevSecOps: A Systematic Review," *Information and Software Technology*, vol. 141, p. 106 700, 2022. DOI: 10.1016/j.infsof.2021.106700

[128] E. B. Rogers and S. W. Mitchell, "MBSE Delivers Significant Return on Investment in Evolutionary Development of Complex SoS," *Systems Engineering*, vol. 24, no. 6, pp. 385–408, 2021. DOI: 10.1002/sys.21592 [Online]. Available: https://incose.onlinelibrary.wiley.com/doi/full/10.1002/sys.21592

[129] R. Ross, M. Winstead, and M. McEvilley, *Engineering Trustworthy Secure Systems* (NIST Special Publication 800-160 Vol. 1 Rev. 1). National Institute of Standards and Technology, Nov. 2022. DOI: 10.6028/NIST.SP.800-160v1r1 [Online]. Available: https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final

[130] SANS Institute, "SOC Survey 2023," SANS Institute, Research Report, 2023. Accessed: Jan. 9, 2025. [Online]. Available: https://www.sans.org/white-papers

[131] L. Mendes, C. Cerdeiral, and G. Santos, "Documentation technical debt: A qualitative study in a software development organization," in *Proceedings of the XXXIII Brazilian Symposium on Software Engineering*, ser. SBES '19, ACM, 2019, pp. 447–451. DOI: 10.1145/3350768.3350773

[132] SEBoK Authors, *The Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 2.13*, N. Hutchison, Ed., www.sebokwiki.org, 2025.

References XVI

[133] Systems Engineering Research Center, "Enterprise System-of-Systems Model for Digital Thread Enabled Acquisition," SERC, Technical Report SERC-2018-TR-109, 2018. [Online]. Available: https://sercuarc.org/technical-reports/

[134] Systems Engineering Research Center, "Systems Engineering Modernization: Digital Engineering, MOSA, Mission Engineering, and Agile/DevOps Integration," SERC, Technical Report SERC-2022-TR-009, 2022. [Online]. Available: https://www.cto.mil/wp-content/uploads/2023/06/SERC-WRT-1051-2023.pdf

[135] G. Shao, *Use Case Scenarios for Digital Twin Implementation Based on ISO 23247* (NIST Advanced Manufacturing Series 400-2). National Institute of Standards and Technology, May 2021. DOI: 10.6028/NIST.AMS.400-2 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.400-2.pdf

[136] G. Shao, S. Frechette, and V. Srinivasan, "An Analysis of the New ISO 23247 Series of Standards on Digital Twin Framework for Manufacturing," in *ASME 2023 18th International Manufacturing Science and Engineering Conference*, ASME, 2023. DOI: 10.1115/MSEC2023-101127 [Online]. Available: https://www.nist.gov/publications/analysis-new-iso-23247-series-standards-digital-twin-framework-manufacturing

[137] M. Stojkov, N. Dalčeković, B. Markoski, B. Milosavljević, and G. Sladić, "Towards Cross-Standard Compliance Readiness: Security Requirements Model for Smart Grid," *Energies*, vol. 14, no. 21, p. 6862, 2021. DOI: 10.3390/en14216862

[138] G. M. Sullivan and A. R. Artino, "Analyzing and interpreting data from Likert-type scales," *Journal of Graduate Medical Education*, vol. 5, no. 4, pp. 541–542, 2013. DOI: 10.4300/JGME-5-4-18

[139] Obeo, *SysON: The NextGen SysML Modeling Tool*, Online, 2025. Accessed: Jan. 9, 2025. [Online]. Available: https://mbse-syson.org/

[140] H. Thompson, M. Anderson, and S. Johnson, "Integrating mbse with it service management: A practical approach," *Journal of Enterprise Architecture*, vol. 15, no. 3, pp. 42–55, Aug. 2019, ISSN: 1556-9365.

[141] The Open Group, *TOGAF Standard, Version 9.2*. Reading, UK: The Open Group, 2018, ISBN: 978-9401802833. Accessed: Jun. 3, 2023. [Online]. Available: https://www.opengroup.org/togaf

DAKOTA STATE UNIVERSITY

References XVII

[142] M. Torkjazi et al., "Model-Based Systems Engineering (MBSE) Methodology for Integrating Autonomy into a System of Systems Using the Unified Architecture Framework," *INCOSE International Symposium*, vol. 34, no. 1, pp. 726–742, 2024. DOI: 10.1002/iis2.13195 [Online]. Available: https://incose.onlinelibrary.wiley.com/doi/10.1002/iis2.13195

[143] Uptime Institute, "Annual Outage Analysis 2023," Uptime Institute, Research Report, 2023. Accessed: Jan. 3, 2026. [Online]. Available: https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[144] M. Vielberth, M. Dietz, D. Gollmann, and G. Pernul, "A Digital Twin-Based Cyber Range for SOC Analysts," in *Data and Applications Security and Privacy XXXV*, Springer, 2021, pp. 293–311. DOI: 10.1007/978-3-030-81242-3_17 [Online]. Available: https://dl.acm.org/doi/10.1007/978-3-030-81242-3_17

[145] A. Vogelsang, T. Amorim, F. Pudlitz, P. Gersing, and J. Philipps, "Should I Stay or Should I Go? On Forces that Drive and Prevent MBSE Adoption in the Embedded Systems Industry," in *Product-Focused Software Process Improvement (PROFES 2017)*, ser. Lecture Notes in Computer Science, vol. 10611, Springer, 2017, pp. 182–198. DOI: 10.1007/978-3-319-69926-4_14

[146] S. Wolny, A. Mazak, C. Carpella, V. Geist, and M. Wimmer, "Thirteen Years of SysML: A Systematic Mapping Study," *Software and Systems Modeling*, vol. 19, no. 1, pp. 111–169, 2020. DOI: 10.1007/s10270-019-00735-y Accessed: Feb. 17, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s10270-019-00735-y

[147] A. Wooley and J. Womack, "Digital Engineering: A Systematic Literature Review of Strategies, Components, and Implementation Challenges," *Systems*, vol. 13, no. 12, p. 1046, 2025. DOI: 10.3390/systems13121046 Accessed: Jan. 3, 2026. [Online]. Available: https://www.mdpi.com/2079-8954/13/12/1046

[148] Z. Yin, X. Yuan, Y. Lu, et al., "An Empirical Study on Configuration Errors in Commercial and Open Source Systems," in *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*, ser. SOSP '11, ACM, 2011, pp. 159–172. DOI: 10.1145/2043556.2043572

References XVIII

[149] J. A. Zachman, "The Concise Definition of the Zachman Framework," *Zachman International*, 2008. Accessed: Jan. 3, 2026. [Online]. Available: `https://www.zachman.com/about-the-zachman-framework`

[150] J. A. Zachman, "The Zachman Framework Evolution," *Zachman International Enterprise Architecture*, 2011. Accessed: Jan. 3, 2025. [Online]. Available: `https://www.zachman.com`

[151] H. Zhang and F. Moller, "Architecture-Centric Model-Based Systems Engineering for Complex Systems," in *Proceedings of the International Conference on Software Engineering and Knowledge Engineering*, IEEE, 2021, pp. 123–130.