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

DAKOTA STATE UNIVERSITY

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. This research investigates whether IT and Information Assurance professionals recognize the potential that Digital Engineering capabilities hold for their work.

This study employs quantitative survey methodology to establish baseline empirical data regarding professional awareness and perceived value. The findings shall inform strategic decisions regarding future research investment, industry adoption initiatives, and academic curricula development.

Presentation Agenda

1. Problem Statement and Research Context
2. Research Questions
3. Literature Review Highlights
4. Digital Engineering Foundations
5. Research Methodology
6. Survey Design and Instrument
7. Timeline and Schedule
8. Expected Contributions
9. 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 — NIST SP 800-53 Rev 5: Security Controls

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.

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 IT and Information Assurance professionals perceive Digital Engineering capabilities as potentially valuable or important for their work?

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.

Literature Review: Enterprise Architecture

Unified Architecture Framework (UAF)

Now codified as ISO/IEC 19540-1:2022 and ISO/IEC 19540-2:2022, UAF emerged as the consolidating standard. The specification asserts that 90% of concepts in military frameworks prove equally applicable in commercial domains.

Comparative Framework Analysis (Bankauskaite 2019)

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

Literature Review: DoD Digital Engineering Strategy

Five Strategic Goals (DoD DE Strategy 2018)

1. Formalize model development and integration for enterprise decisions
2. Provide an authoritative source of truth
3. Incorporate technological innovation to improve practice
4. Establish a Digital Engineering ecosystem
5. Transform culture and workforce for Digital Engineering adoption

DoD Instruction 5000.97 (December 2023) codifies Digital Engineering requirements, mandating programs leverage digital artifacts as the authoritative source of system information.

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 simulation and testing

Product Lifecycle Management

Integrated lifecycle governance and configuration control

Pillar 1: Model-Based Systems Engineering

Definition

MBSE represents a fundamental shift from document-centric to model-centric approaches. Models become the authoritative representation of system architecture, requirements, behavior, and interfaces.

Application to IA/IT:

- Models can capture security architectures with explicit relationships between controls, assets, and threats
- Authorization boundaries represented as executable models rather than static documents
- Relationships between configuration items modeled with inheritance and dependencies

Pillar 2: Digital Thread

Definition

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

Application to IA/IT:

- Traceability from security requirements through control implementations to assessment evidence
- Automated compliance verification through model-based queries
- Change impact analysis that traces modifications across interconnected systems

Pillar 3: Digital Twin

Definition

Digital twins are virtual replicas of physical systems that enable simulation, analysis, and testing without impacting production environments. Twins maintain synchronization with their physical counterparts.

Application to IA/IT:

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

Pillar 4: Product Lifecycle Management

Definition

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

Application to IA/IT:

- Configuration baseline management aligned with ITIL principles
- Change coordination across interconnected systems
- Security control maintenance throughout system operation and decommissioning
- Integration of security and IT operations through shared authoritative data

Digital Engineering Value Proposition

Addressing Identified Gaps

- **Authoritative Source of Truth Gap:** 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

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

Research Design Overview

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

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

Systems Engineering Research Lifecycle

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

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

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

Survey Instrument Structure

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 (7 questions)
6. Interest and Demographic Information (4 questions)

Estimated Completion Time: Approximately 10 minutes

Question Format and Scale Selection

Five-Point Likert Scale

Familiarity Scale: Not at all familiar $\rightarrow$ Extremely familiar

Agreement Scale: Strongly disagree $\rightarrow$ 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

Survey-to-Research Question Mapping

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: Perceived Value
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 Approach

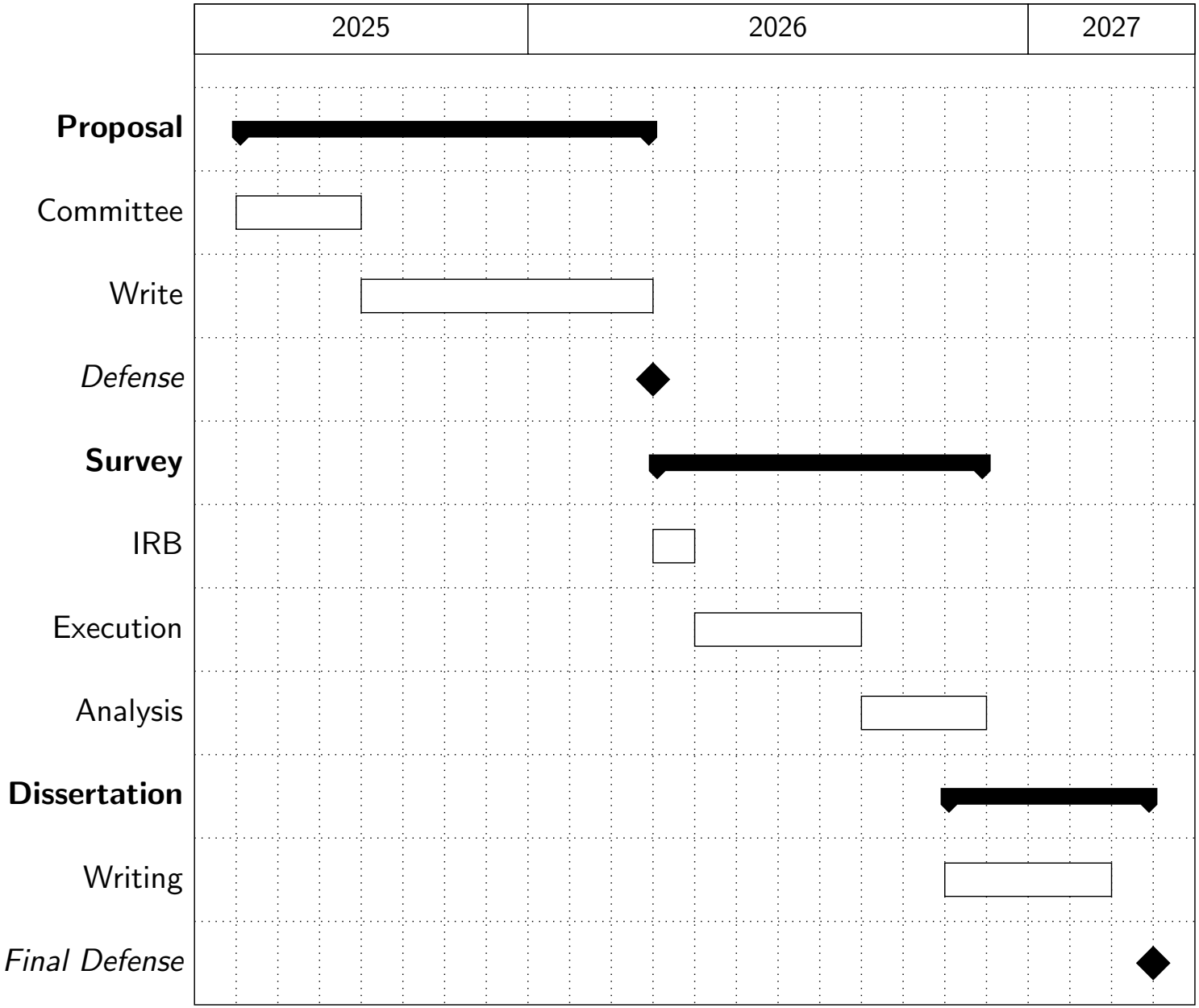
Descriptive Statistics

- 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

Research Timeline: 22-Month Schedule



DAKOTA STATE UNIVERSITY

Timeline Phase Details

Phase 1–3: Proposal (May 2025 – April 2026)

Committee formation, proposal development, proposal defense, IRB approval

Phase 4: Survey Execution (May – August 2026)

Platform configuration, recruitment through multiple professional channels, data collection targeting 450 responses

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

Data analysis, results interpretation, dissertation writing, final defense

Validity and Reliability

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

Research Limitations

- 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

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 and Society

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

Societal Benefits

- Enhances protection of government systems and critical infrastructure
- Potentially enables better security capabilities for organizations serving underserved populations
- Democratizes sophisticated documentation capabilities beyond large enterprises

Ethical Considerations

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

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

Thank you for attending.

Questions?

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

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] C. J. Alberts, S. G. Behrens, R. D. Pethia, and W. R. Wilson, "Operationally critical threat, asset, and vulnerability evaluation (octave) framework, version 1.0," Carnegie Mellon University, Software Engineering Institute (SEI), Technical Report CMU/SEI-99-TR-017, Jun. 1999. DOI: 10.1184/R1/6575906.v1 [Online]. Available: https://doi.org/10.1184/R1/6575906.v1

[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, "Enterprise Architecture Frameworks Analysis," in *CEUR Workshop Proceedings*, vol. 2470, 2019, pp. 141–149. Accessed: Jan. 3, 2025. [Online]. Available: https://ceur-ws.org/Vol-2470/p19.pdf

[8] 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

[9] 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

References II

[10] 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

[11] 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/

[12] 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

[13] 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

[14] 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: 10.22495/jgrv11i2art1

[15] D. G. Broo and J. Schooling, "Digital Twins in Infrastructure: Definitions, Current Practices, Challenges and Strategies," *International Journal of Construction Management*, vol. 23, no. 7, pp. 1254–1263, 2023. DOI: 10.1080/15623599.2021.1966980 [Online]. Available: https://doi.org/10.1080/15623599.2021.1966980

[16] 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

[17] 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

References III

[18] 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.

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

[20] E. R. Carroll and R. J. Malins, "Systematic Literature Review: How is Model-Based Systems Engineering Justified?" Sandia National Laboratories, Technical Report SAND2016-2607, 2016. DOI: 10.2172/1561164 [Online]. Available: https://www.osti.gov/servlets/purl/1561164

[21] 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

[22] 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

[23] 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

[24] 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

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

References IV

[26] 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/

[27] 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

[28] 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

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

[30] 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

[31] 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

[32] Deloitte, *Model-Based Enterprise Capabilities*, Industry Report, 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://www.deloitte.com/us/en/what-we-do/capabilities/mergers-acquisitions-restructuring/articles/model-based-enterprise-capabilities.html

[33] 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

References V

[34] 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

[35] 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.

[36] 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/

[37] 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

[38] 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/

[39] 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

[40] 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/

[41] 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

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

References VI

[43] 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/

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

[45] 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

[46] W. El-Hajj et al., "Systematic Literature Review: Digital Twins' Role in Enhancing Security for Industry 4.0 Applications," *Security and Privacy*, vol. 7, no. 2, e396, 2024. DOI: 10.1002/spy2.396 [Online]. Available: https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.396

[47] 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

[48] 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

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

[50] 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

[51] 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

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

[53] 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/

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

[55] J. Freund and J. Jones, *Measuring and Managing Information Risk: A FAIR Approach*, 2nd. Elsevier, 2025, ISBN: 978-0443116790.

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

[57] 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

[58] Gartner, *Why CMDB Projects Fail and How to Avoid Their Mistakes*, Gartner Research, 2019. Accessed: Jan. 3, 2025. [Online]. Available: https://www.gartner.com/en/documents/3970851

[59] Gartner, *CMDB Data Quality: Critical Success Factors*, Gartner Research, 2020. Accessed: Jan. 3, 2025. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/cmdb-configuration-management-database

[60] Gartner, *Shadow IT: The Risks and How to Manage Them*, Gartner Research, 2022. Accessed: Jan. 3, 2025. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/shadow-it

References VIII

[61] S. Gil, C. Martín, and M. Díaz, "Survey on Open-Source Digital Twin Frameworks: A Case Study Approach," *Software: Practice and Experience*, vol. 54, no. 1, pp. 108–145, 2024. DOI: 10.1002/spe.3305

[62] K. Goher, E. Shehab, and A. Al-Ashaab, "Model-Based Definition and Enterprise: State-of-the-art and Future Trends," *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, vol. 235, no. 14, pp. 2288–2311, 2021. DOI: 10.1177/0954405420971087

[63] 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

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

[65] M. Grieves and J. Vickers, "Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems," in *Transdisciplinary Perspectives on Complex Systems*, Springer, 2017, pp. 85–113. DOI: 10.1007/978-3-319-38756-7_4 [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-38756-7_4

[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 [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050915030380

[69] K. Henderson, T. McDermott, and A. Salado, "Understanding MBSE Adoption: A Mixed Methods Study of Organizational Experiences," *Systems Engineering*, vol. 27, no. 2, pp. 250–267, 2024. DOI: 10.1002/sys.21717 Accessed: Nov. 11, 2025. [Online]. Available: https://incose.onlinelibrary.wiley.com/doi/10.1002/sys.21717

References IX

[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. [Online]. Available: https://incose.onlinelibrary.wiley.com/doi/10.1002/sys.21566

[71] K. Henderson and A. Salado, "Organizational Factors Associated with MBSE Adoption Success," *Engineering Management Journal*, vol. 36, no. 1, pp. 45–62, 2024. DOI: 10.1080/10429247.2023.2210494 Accessed: Jan. 3, 2026. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/10429247.2023.2210494

[72] 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

[73] 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

[74] 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/

[75] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2024," IBM Corporation, Research Report, Jul. 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://www.ibm.com/reports/data-breach

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

[77] 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

References X

[78] 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/

[79] 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

[80] 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

[81] 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.

[82] 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

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

[84] 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

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

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

References XI

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

[88] 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

[89] D. Jones, C. Snider, A. Nassehi, J. Yon, and B. Hicks, "Characterising the Digital Twin: A Systematic Literature Review," *CIRP Journal of Manufacturing Science and Technology*, vol. 29, pp. 36–52, 2020. DOI: 10.1016/j.cirpj.2020.02.002 Accessed: Oct. 20, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1755581720300110

[90] N. S. A. Junior and G. H. Travassos, "Consolidating a Common Perspective on Technical Debt and Its Management through a Tertiary Study," *Information and Software Technology*, vol. 150, p. 106 991, 2022. DOI: 10.1016/j.infsof.2022.106991

[91] 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

[92] 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

[93] 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

[94] M. Laili, S. Pekkola, and J. Kääriäinen, "Industrial Open Source Solutions for Product Life Cycle Management," *Cogent Engineering*, vol. 1, no. 1, p. 939 737, 2014. DOI: 10.1080/23311916.2014.939737

[95] 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

References XII

[96] Z. Liu et al., "Top-Down Military System-of-Systems Design Using MBSE Based on UAF: A Case Study," in *Advances in Guidance, Navigation and Control*, Springer, 2023, pp. 203–214. DOI: 10.1007/978-981-99-6511-3_19 [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-99-6511-3_19

[97] 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

[98] 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

[99] D. Mažeika and R. Butleris, "Integrating security requirements engineering into mbse: Profile and guidelines," *Security and Communication Networks*, vol. 2020, no. 1, p. 5 137 625, 2020.

[100] J. Fabius and R. Graubart, "Beyond compliance: Addressing the political, cultural and technical dimensions of applying the risk management framework," The MITRE Corporation, McLean, VA, Tech. Rep., 2019. Accessed: Jan. 7, 2026. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-14-3551-beyond-compliance-applying-risk-management-framework.pdf

[101] 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

[102] 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

[103] 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

References XIII

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

[105] 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

[106] 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

[107] National Institute of Standards and Technology, *Model-Based Enterprise Summit 2018*, Conference Proceedings, 2018. Accessed: Jan. 9, 2025. [Online]. Available: https://www.nist.gov/el/systems-integration-division-73400/model-based-enterprise-mbe

[108] 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/

[109] 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

[110] 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

[111] 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

References XIV

[112] 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

[113] 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

[114] 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/

[115] 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

[116] 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

[117] 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

[118] 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/

[119] R. K. Rogers and P. D. Mitchell, "MBSE Delivers Significant Return on Investment in Evolutionary Development of Complex SoS," *Systems Engineering*, vol. 24, no. 6, pp. 419–432, 2021. DOI: 10.1002/sys.21592 [Online]. Available: https://incose.onlinelibrary.wiley.com/doi/full/10.1002/sys.21592

References XV

[120] 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

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

[122] G. Santos et al., "Documentation Technical Debt," in *Proceedings of the XXXIII Brazilian Symposium on Software Engineering*, ser. SBES '19, ACM, 2019, pp. 304–313. DOI: 10.1145/3350768.3350773

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

[124] 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/

[125] 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

[126] 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

[127] 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

[128] J. Song and F. Le Gall, "Digital Twin Standards, Open Source, and Best Practices," in *The Digital Twin*, Springer, 2023, pp. 497–530. DOI: 10.1007/978-3-031-21343-4_18

References XVI

[129] T. Spyridopoulos et al., "Model-Based Systems Engineering Cybersecurity for Space Systems," *Aerospace*, vol. 10, no. 2, p. 116, 2023. DOI: 10.3390/aerospace10020116 [Online]. Available: https://www.mdpi.com/2226-4310/10/2/116

[130] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, "The First Collision for Full SHA-1," in *Annual International Cryptology Conference*, Springer, 2017, pp. 570–596. DOI: 10.1007/978-3-319-63688-7_19

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

[132] M. Boucher, "Adopting a Model-Based Enterprise (MBE) Strategy: What You Should Know," Tech-Clarity, Research Report, 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://tech-clarity.com/model-based-enterprise-mbe/11616

[133] 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.

[134] 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

[135] 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

[136] 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

[137] 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

References XVII

[138] 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

[139] 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

[140] J. 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

[141] 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

[142] 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

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

[144] 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.

[145] P. Zimmerman, "Digital engineering strategy and implementation," in *Proceedings of the 10th Model-Based Enterprise (MBE) Summit*, Gaithersburg, MD: National Institute of Standards and Technology, Apr. 2019. [Online]. Available: https://www.nist.gov/system/files/documents/2019/04/05/10_zimmerman_destrategyimp_nist_mbe_summit_vf.pdf