SYM-AM-19-037

PROCEEDINGS
OF THE
SIXTEENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

WEDNESDAY SESSIONS
VOLUME I

Acquisition Research:
Creating Synergy for Informed Change

May 8–9, 2019

Published: April 30, 2019

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

Acquisition Cybersecurity Management Framework

Dr. Randy William Maule—has been with the Naval Postgraduate School since 2000, serving as naval and joint forces enterprise developer, knowledge manager, and technical analyst in Sea Trial and coalition exercises where he conducted systems test and measurement. His enterprise tool suite and cyber test and measurement architecture operated on ships, in maritime and network operations centers, and in forward-deployed commands for nearly 15 years. Prior to this, he spent 10 years in Silicon Valley high technology industries researching intelligent networks and service architecture, and prior to this developing enterprise knowledge systems and artificial intelligence (AI) at a federal supercomputer center. [rwmaule@nps.edu]

Abstract

Current organizational structures have proven insufficient for cyber and information assurance. The acquisition role may be resourced and expanded to support information assurance and systems compliance. A supply chain audit and assessment process within acquisition departments will better support emerging cybersecurity requirements. This project advances technical and workflow models, an assessment framework, and implementation methods to support expansion of the acquisition department role to include cybersecurity and information assurance across the systems lifecycle—from supply chain, through test and measurement, to maintenance and obsolescence. Analysis methodology and model-based system engineering techniques successfully employed in naval and joint forces field research for technology and cybersecurity evaluation for nearly two decades, along with best practices from Silicon Valley high technology industries, were applied in the acquisition cybersecurity management framework. A shift of cybersecurity assessment from distributed units into centralized acquisition departments should significantly lessen the inter- and intra-organizational boundaries which have traditionally hindered cybersecurity.

Research Objective: Establish methodology and models to support the cybersecurity and information assurance needs of naval forces and provide decision makers with an evaluation framework and workflow to inform acquisition decisions and better ensure systems security.

Research Questions: Will the centralization of cybersecurity and information assurance away from individual units into acquisition departments lessen inter- and intra-organizational boundaries that have historically limited cyber effectiveness? Will the workflow and audit models suffice for acquisition departments to implement security controls across the systems lifecycle—from initial acquisition to maintenance and obsolescence?

Introduction

Current organizational structures have proven insufficient for cyber and information assurance. Acquisition departments may be expanded to help ensure cybersecurity. This research advances the acquisition role to support information assurance throughout the supply chain and across the lifecycle of the equipment. This is proposed as an enhancement to current acquisition processes. Model-based system engineering techniques are applied for systems test and measurement and integrated into audit processes within the acquisition workflow. Techniques, procedures, roles and responsibilities are based on lessons learned in naval and joint forces exercises and best practices in Silicon Valley high technology industries. The proposed supply chain audit and assessment process extends from initial equipment purchase order, through acquisition, to maintenance and lifecycle compliance assessment, to obsolescence and destruction.

Research Background

Business, industry, and government collectively struggle with cybersecurity compliance, information assurance, and data security. Resources and processes to support audits, assessment and reporting are insufficient. While the terminology and architecture are slightly different from industry to government, the problems are similar and can often be traced to the supply chain—from counterfeit and compromised components, to improper/malevolent code, to unsecured systems and maintenance processes. The acquisition role may be best suited to remedy current shortcomings. This will require significant expansion of that role and its resources to support supply chain information assurance.

Cybersecurity compliance assessment as a component of supply chain management will shift audit responsibilities from vendors, program offices and departments into centralized acquisition departments. This will significantly lessen the inter- and intra-organizational boundaries which have traditionally hindered cybersecurity and information assurance. The shift of systems verification from vendors and their contractors or sponsors to independent government auditors will remove bias while increasing the comprehensiveness of the process as auditors are able to look across department boundaries to examine the integration interfaces where systems are most vulnerable. Model-Based System Engineering (MBSE) and supporting analysis methodology successfully employed in naval and joint forces field research for technology and cybersecurity evaluation for nearly two decades provide the foundation for the acquisition modeling framework and analysis workflow.

The process begins with technical models and expert systems for best practices, then procedures and workflows for technical assessment, followed by systems integration audits. Next are methods and procedures for in-service audits for cybersecurity and information assurance, systems verification and data validation. Technical models are integrated with audit workflows for comprehensive lifecycle systems assessment to include maintenance and the declaration of software/hardware obsolescence and destruction.

Literature Review

Supply chain modeling and analysis is advanced within the context of complexity science, which assumes both technical and human phenomena that interface to determine system readiness and operational effectiveness. The following is evidence of complexity in naval systems:

1. Multi-layered communication architecture
2. Multiple organizational structures to produce a capability
3. Organizational boundaries which impact engineering and analysis
4. Adversary capabilities for advanced electronic and multi-layered cyberattack.

The methodology herein advances multi-disciplinary research techniques to include evaluation of all variables that we have found to impact the validity of naval systems and data, including cross-organizational technology integration, variance in the RF spectrum, and human influence (Maule, 2017). There is a research history that provides perspective for supply chain cyber analytics.

Network science studies complex networks (Tiropanis et al., 2015) at a level of detail sufficient to generate predictive models. For example, tools that we use in naval technical analysis map data flows between systems over network connections to monitor routing, processes and data. Supporting each variable are algorithms to assess defined metrics and data validity based on components in the routing, integration and transformation path.

Network-centric warfare and information dominance are considered within the vocabulary of network science (National Research Council, 2005). When cybersecurity is layered into the analysis, the number of metrics for measurement expands exponentially.

Complexity science spans computer science, mathematics, and operations research and includes the study of distributed, interactive computing (Du & Ko, 2014). Complexity theory investigates how subcomponents of a system integrate to produce a collective behavior of that system (Ladyman, Lambert, & Wiesner, 2013). Pertinent to naval systems analysis is that complexity can be characterized within the context of equilibrium—as required for high-performance communications in challenged environments. Absent system synchronization, we do not achieve equilibrium, so data relied upon for decisions may be latent, corrupt or compromised. A sub-discipline of complexity science, adaptive systems, uses probabilistic measures to quantify complex variables—such as systems readiness and human effectiveness.

Adaptive systems are characterized by the capability to change and learn from experience. Machine learning can be applied to help understand the complexity. We observe adaptive behaviors in naval exercises as we instrument networks to monitor complex data flows across geographic regions. The components of systems interact, with the result of those interactions dependent on dynamic contextual variables. An example is changes made as sailors and systems adapt to rapidly changing tactical scenarios. Evaluation addresses the dynamic interplay of adaptive, complex variables over time. Failure to address this complexity results in an inability to monitor systems to recognize a performance variance or cyber intrusion, or to adapt the analysis to changes in systems operational context—leading to incorrect data.

Test and measurement of naval systems in live operations have established that the relationship between systems, components, and other systems is nonlinear (Maule, Jensen, & Gallup, 2014). It is not possible to precisely define the inputs such that there is a direct relationship to the outputs. Cause–effect relationships can be determined only within technical, operational and environmental context. Systems performance tends to exhibit divergent patterns under stress—such as challenged communications, jamming or electronic attack, and of course cyber manipulation.

This leads to the final construct of adaptive complexity—namely, that while it is possible to establish linear relationships in a static architecture, these relationships may no longer be relevant when integrated into dynamic scenarios. Researchers have noted the need for probabilistic algorithms for multiple dimensions of analysis when contexts are dynamic and expanding (McMullen, 2015). Assessment is over time, within the full range of technical, operational and environmental contexts in which the system will operate (Maule, 2016).

Probabilistic algorithms also fit nicely with artificial intelligence (AI) tools for decision support. In warfare, the large number of dynamic variables, together with the large number of possible technical, operational and environmental contexts to be assessed in an engagement, necessitate statistical analysis. There is never a single answer; the result is always within context. Probabilistic approaches, together with machine learning and neural networks, can address this complexity to provide a solution for tactical supply chain cyber analysis.

The need is acute. Problems with unsecured open architecture and open source products persist (Dorofee et al., 2013; Cooper, 2009; Lindqvist & Jonsson, 1998). There are problems when vendors publish system specifications to the Internet and problems with deployment practices that do not carefully control firmware updates (Kern, 2014; Camp et al., 2006). There is little protection if purchasing computer chips which have already been compromised (Center for Public Integrity, 2014; Rossi, 2012; Johnson, 2011; Adee, 2008; Grow et al., 2008; Dean & Li, 2002).

Another rationale for a direct connection between the audit process and the acquisition role is so that compromised systems can be immediately destroyed and replaced. Historically, after we identify a breach, we can only file a report. These reports are not typically well-received, and systems may continue to operate. In the proposed supply chain cybersecurity workflow, the auditors have a more direct means for remediation.

As needed, events can be reconstructed for detailed cyber analysis. We use live cyberattacks on components in offline laboratories to validate findings. The analytics produce quantitative system readiness coefficients and confidence levels for those coefficients (Maule, 2017).

Method

Adaptive complexity for supply chain cyber analysis is applied as an extension of the Cybersecurity Figure of Merit (CFOM). CFOM is a mathematical framework of weighted qualitative and quantitative metrics that provide an expression of the relative effectiveness of an information technology in terms of the completeness and sufficiency of its cyber security properties throughout its lifecycle (Space and Naval Warfare Systems Command [SPAWAR], 2015).

The NPS Service Evaluation Architecture (SEA) CFOM implementation is based on assessments conducted in live naval, joint forces and coalition exercises where the focus was on systems readiness and resiliency in electronic engagements against adversaries that had imposed D-DIL or A2AD conditions on blue forces (Maule & Lewis, 2011).

Models, metrics, and analytics are derived from cumulative naval system test results, beginning with Fleet Battle Experiments in 2000 and then FORCEnet and Joint Forces Command (JFCOM) Sea Trials from 2003–2015, which included Trident Warrior, RIMPAC, Valiant Shield, and numerous limited objective experiments with NATO and coalition forces.

Supply Chain Standards

Next is to address foundations for the supply chain cybersecurity framework to help structure the analysis. The International Organization for Standardization (ISO) is a global network of national standards bodies which develop and publish International Standards. Members are the foremost standards organizations in their countries. The ISO collaborates closely with the International Electrotechnical Commission (IEC) and the Institute for Electrical and Electronics Engineers (IEEE). Some of the standards are specific to supply chain management, including cybersecurity, quality management, and audits (ISO, n.d.). Standards pertinent to the acquisition cybersecurity management framework include the following:

- SO 9000: Quality management systems
- ISO/TS 10303-1307: Industrial automation systems and integration
- ISO 16678: Guidelines to deter counterfeiting and illicit trade
- ISO/TR 17370: Data carriers for supply chain management

- ISO/IEC 20243: Mitigating maliciously tainted and counterfeit products[1]
- ISO/TS 22375: Security and resilience guidelines for complexity assessment
- ISO/IEC 27036: Information security for supplier relationships
- ISO 28000: Supply chain security management systems—Specifications
- ISO 28001: Supply chain security management systems—Assessments
- ISO 28002: Supply chain security management systems—Resilience
- ISO 28003: Supply chain security management systems—Audit and certification
- ISO/IEC/IEEE 41062: Software engineering

Supply Chain Acquisition Framework

The acquisition cybersecurity management framework and supply chain cyber analytics process apply the previously mentioned standards through an extension to the traditional acquisition workflow. The extension provides cybersecurity management from initial equipment request through vendor selection, then across the systems lifecycle to include maintenance and obsolescence. The intent is to provide a comprehensive security structure for naval systems from acquisition to destruction (Figure 1). This includes the system support structure and command management, staffing, contracting and outsourcing. Time requirements along with expertise, budgeting and comparative analysis are addressed.

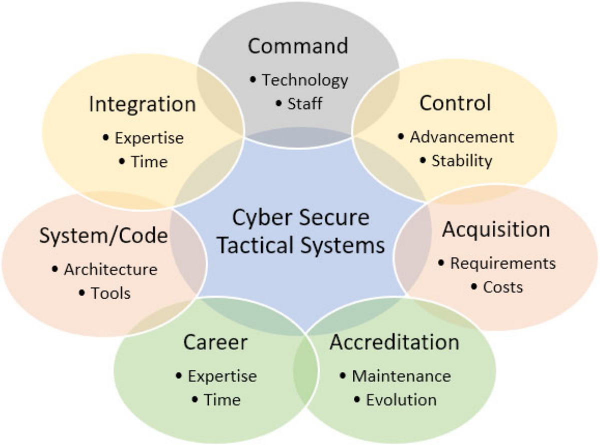


Figure 1. Variables for Supply Chain Cyber Assessment

Evaluation techniques are based in statistical analysis with AI and machine learning to provide decision support. Probabilities are based on defined metrics and measurements from independent government auditors. The methodology can be applied to help acquisition decision makers better evaluate technologies for possible cybersecurity impact and tactical forces to better understand the implications of their purchase requests, the degree to which their systems may have been compromised, and the validity of the data in their systems.

[1] https://www.iso.org/standard/74399.html; https://www.iso.org/obp/ui/#iso:std:iso-iec:20243:-1:ed-1:v1:en

The assumption herein is that when naval architecture is suspected of compromise and the cyber adversary may have enacted automated routines to alter data to impact systems performance or invalidate information in command decision systems, mechanisms will be required to determine the impact on warfighter readiness. The proposed enhancement to the systems acquisition process will help remedy this situation through real-time audit monitors and controls.

Figure 2 denotes the basic acquisition process and the current financial and vendor selection process. Along the left axis is equipment selection and the purchase request. The green arrows indicate legacy operations. Below the basic acquisition process is the proposed cybersecurity enhanced acquisition process. Red arrows denote the additional workflows and data streams.

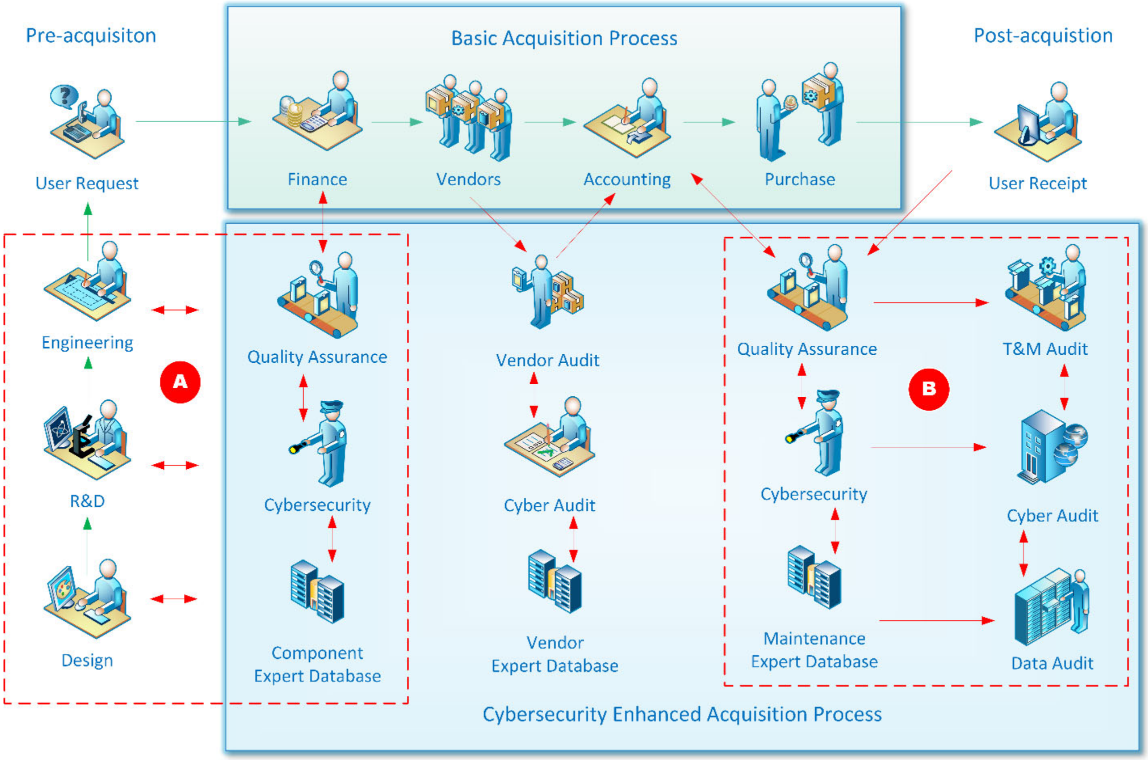


Figure 2. Supply Chain Basic and Cybersecurity Enhanced Acquisition Framework

Within the enhanced process are databases for quality assurance and cybersecurity, along with expert systems to interface with engineers during design and development—preliminary to product request and submission to the purchasing agents. The green arrows indicate the current workflows, and the red arrows are the interfaces to the new specialized systems.

The dashed red box designated as Section "A" is preliminary to the acquisition when the system proponent begins the purchase order. Here the purchaser interacts with expert systems as machine learning agents assess the technology through comparative analysis and provide recommendations. A record stream for acquisition decision makers and financial personnel is generated. Functions in this area are discussed in the solution section later in this report.

The dashed red box designated as Section "B" is the post-purchase process and consists of a series of independent government monitors and audits. Most can be automated and have been successfully tested in naval operations. These monitors and audits recognize that the purchase is not the end of the acquisition process, but rather a step in the systems lifecycle. Before the purchase, the cybersecurity concerns are with the computer chips and embedded components, drivers and software. After the purchase, the cybersecurity concerns are with the integration, maintenance and evolution of the software and components within the system, impact on other systems, and the validity of the processed data. Functions in this area are advanced in more detail in the next section and are discussed again in the solution set later in this report.

The unbound area in the middle of the figure addresses the physical components—from the vendor, to the suppliers to the vendor, to the involved personnel. This is a comprehensive area for assessment that is beyond the scope of this project and is reserved for future research. Techniques advanced in Sections "A" and "B" can be applied, albeit with an exponential expansion of detail and complexity.

Supply Chain Audit Framework

The audit framework begins with test and measurement models that show components, systems, spectrum, interfaces, sensors and software. All are assessed within the technical, operational and environmental context in which they operate to provide a more accurate analysis for acquisition decision makers. Collected data includes packets, system logs, sensor data, human interface and interaction results, and fusion/integration artifacts (Figure 3).

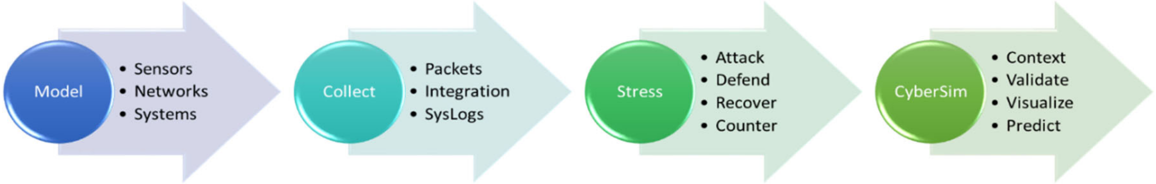


Figure 3. High Level Supply Chain Cyber Audit Workflow

Analysis of cyber effects begins with stressing systems through network and process load to determine points of failure and countermeasures to achieve resilience. Cyber effects are layered to assess system capabilities to recover from and/or counter cyber stress. Assessment involves a continuous, comprehensive monitoring of systems, networks and applications. CyberSim is for offline tests with live malware against the components to provide a more accurate cybersecurity assessment for systems verification and data validity. This data feeds the AI routines for algorithmic prediction of systems operational readiness.

In more detail, the supply chain cyber audit framework (Figure 4) supports in-service test and measurement for continuous systems cybersecurity assessment–using many of the same techniques successfully implemented on forward-deployed ships and in network and maritime operations centers in Sea Trials and coalition exercises. Our audits include not only new innovations but also updates to program of record systems.

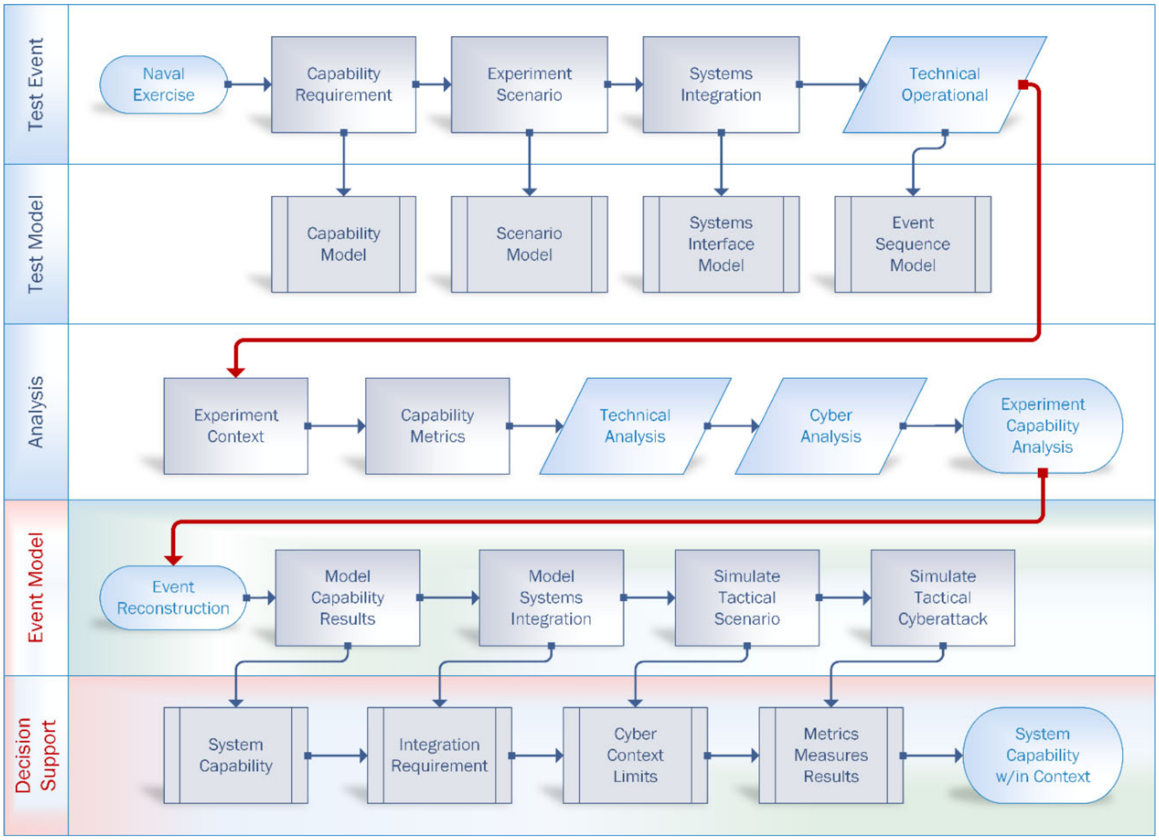


Figure 4. Supply Chain Technical Analysis Framework and Workflow

Cyber analytics is conceptualized as a continuing flow of tests across the operational lifecycle of a system. Each operational context, test scenario, vignette, and attack advance the machine learning algorithms and predictive capability of the audit models. In the previous example, the analysis is focused on ships in A2AD and communication-challenged environments. Systems are under electronic attack—our typical live event scenario throughout the Sea Trials.

The audit workflow starts with Department of Defense Architecture Framework (DoDAF) models of the system, for which at-rest baselines are established. Systems are then evaluated against these models in at-sea tests with active jamming and cyber/electronic attack. Communications between components/sensors require evaluation of satellite communications, tactical radios, and airborne over-the-horizon capabilities.

Cyberattacks are analyzed for their results on the acquisition component, including system failures, data corruption or manipulation, and degradation of situational awareness of supported command decision systems. Cyber performance and operational measures update or verify models and validate the quality of the data. The process iterates.

Solution

This section applies the previously discussed acquisition framework and analytics process as an extension of a traditional systems lifecycle to provide structure for naval systems supply chain cyber analysis.

Integration DEFinition (IDEF) models are common in the DoD to represent operations (IDEF, n.d.). Like DoDAF, the IDEF models range from high-level functional models to low-level object-oriented design and simulation. For a supply chain analytics workflow, the IDEF modeling approach provides useful operational representations in addition to precise data/information metrics for decision support.

The solution set integrates the previously discussed supply chain framework and workflow (pre- and post-acquisition) with implementation constructs for systems verification and data validation through the addition of

a. Experts and expert systems to the pre-acquisition engineering processes
b. Independent audits for information assurance and systems verification
c. Machine learning for AI support to supply chain decision makers

Core processes (Figure 5) include IDEF0 inputs, outputs, controls and mechanisms plus additional audit and AI layers. Core inputs are the purchase order and budget; outputs are the purchase and supporting maintenance agreements. Controls address guidelines and approvals required for submitters and purchasing agents. Mechanisms include the system, software or component requirements and specifications.

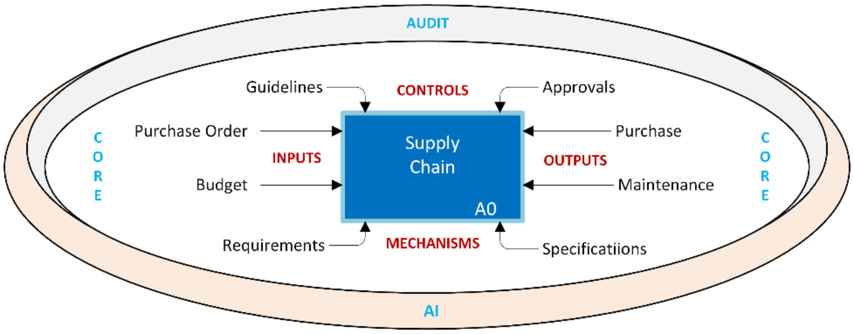


Figure 5. IDEF A0 High-Level Solution Framework

Core Workflow

Figure 6 presents IDEF steps A1–A5 as the high-level components of the supply chain cybersecurity workflow. Assessment begins with user requirements and controls to determine whether specifications have adequately addressed technical, operational and environmental variables that impact the integrity of the equipment in its intended operations.

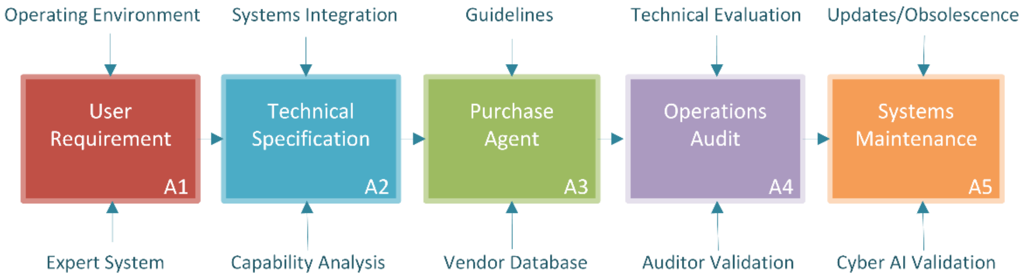


Figure 6. Core Workflow for Supply Chain Cybersecurity Integrity Analysis

Next are technical specifications with systems integration controls. This becomes a primary data set for the machine learning algorithms to address process conflict or constrained environments and will be one of the more extensive programming efforts due to the number of variables in a complex and dynamic naval architecture.

In operation, the purchasing agent receives the recommendation from the machine learning output and is simultaneously presented with the option to review the specific criteria upon which the recommendation is based. Controls include restrictions specific to the unit.

Upon receipt of the system (hardware, software, service, etc.) the responsibility for verification and validation shifts to the auditor. Upon auditor approval, the system is transferred to the end user.

Finally, the maintenance phase monitors equipment throughout its lifecycle, including patches and updates, until the declaration of obsolescence and verification of destruction. Important is the means to verify that the system or software has been destroyed due to the cyber risk from unsupported components.

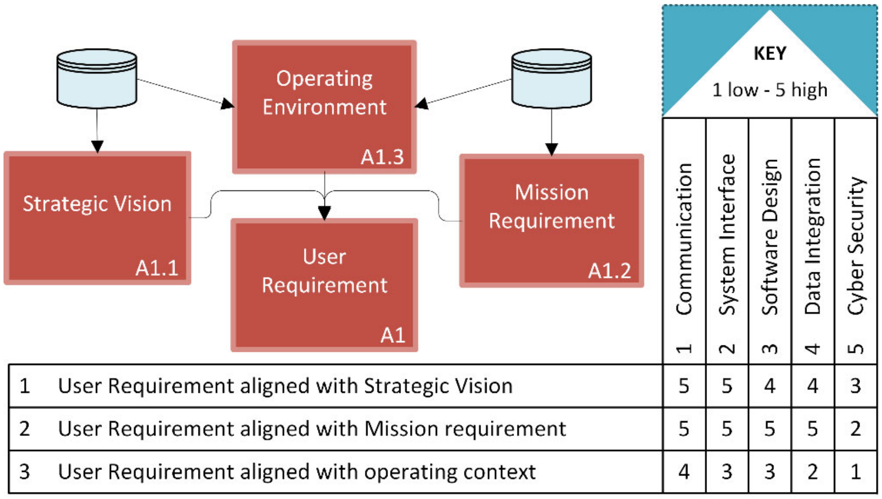
The next two sections examine A1 and A2 in more detail (A3–A5 are reserved for future research). In Figure 2, both are represented in the initial block "A" which occurs prior to the purchase. In future research, the approach followed for the technical specifications will also be applied in the operations audit (A4) and maintenance (A5) phases—albeit with the addition of metrics for technical, operational and environmental context to address the added complexity of live operations.

Requirement Audit

Audits are key to integrity validation across the supply chain. Auditors need to be properly trained and equipped, and with the capability to act independently without fear of reprisal. Nor should they have a vested interest in the success or failure of the system. All are common problems we encounter in analysis.

In Section "A" (Figure 2), with enough audits and a supporting database of audit results, the requirements review can be automated such that the purchaser interacts with an expert system and AI agents provide feedback and recommendations.

Figure 7 models the process and breaks out the Quality of Service (QoS) variables, metrics for those variables, and ratings key. Variables include (1) alignment with the strategic vision, (2) alignment with the mission statement, and (3) alignment with the operating environment. These variables can be programmed into an expert system.



		1 Communication	2 System Interface	3 Software Design	4 Data Integration	5 Cyber Security
1	User Requirement aligned with Strategic Vision	5	5	4	4	3
2	User Requirement aligned with Mission requirement	5	5	5	5	2
3	User Requirement aligned with operating context	4	3	3	2	1

Figure 7. User Requirement Initial Audit Phase With Metrics and Ratings

More difficult are the metrics and ratings which require in-depth understanding of the components of the system and the complexities of the operating environment and software. A typical approach is to begin analysis with the user's requirements for communications to assess alignment with the vision and mission, then the specifics of the operating context, including the organizational, technical and environmental conditions in which the equipment will operate.

The system interface metric examines innovation integration with components of the strategic plan, and then the specific mission area(s) in which it will operate. The context addresses interfaces to technical, operational and environmental conditions but at a deeper level. Technical context addresses the specifics of the physical interface—an area for further refinement and additional audit layers in future research. The environmental context categorizes the innovation through physical presence—for example, mobile device versus server, ship versus shore deployment, calm seas versus challenged communications. The operational baseline establishes whether the test is static or dynamic within the specifics of the test scenario. This area will also require much deeper analysis in future research.

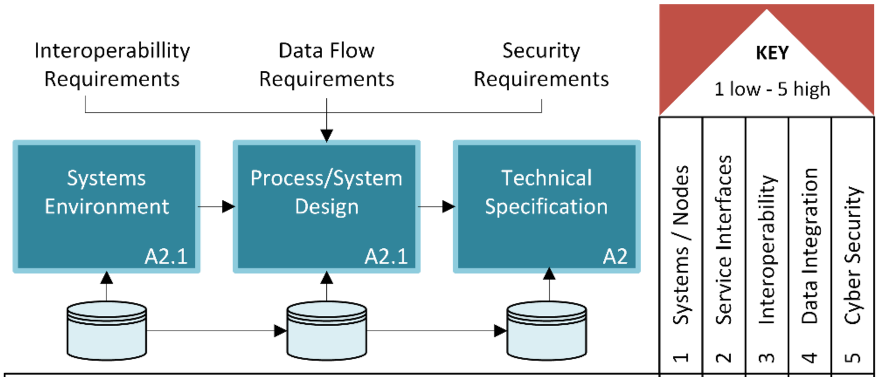
Software design is more straightforward and looks at the innovation in the context of currently active capabilities. For example, is this a redundant capability? Is the system rated by one of the major laboratories? Is this to be purchased? Developed in-house? Outsourced?

In a similar vein, data integration addresses the alignment of the innovation with the vision, mission, and end state: Will data be merged? Will this capability build on the output of another device? Create new insight? QoS variables are addressed from a command decision perspective.

Finally, the cybersecurity. Too often this is an after-thought, but this placement in the initial audit helps ensure that cybersecurity is at the forefront of the supply chain assessment workflow and aligned with the vision, mission and operating context. A2, below, adds more detail and addresses the actual engineering technical measurement process.

Specification Audit

The A2 technical audit identifies specifics within the systems environment, looking at system/service/process integration and interfaces (Figure 8). The first QoS variable assesses alignment of the technical specifications with the designated systems environment in which the equipment will operate to establish baselines. Until baselines are established, it may be difficult to discern a performance anomaly or cyber intrusion.



		1 Systems / Nodes	2 Service Interfaces	3 Interoperability	4 Data Integration	5 Cyber Security
1	Technical specifications address operational environment	5				2
2	Technical specifications address systems environment	4	4			4
3	Technical specifications address system integration	4		3	2	2
4	Technical specifications address data, processes and services	4	4	4	2	4
5	Architecture details operations within context (OV-1)	4				2
6	Architecture details systems interfaces (SV-1)	5	5			2
7	Architecture details systems integration (SV-2)	4		4	2	4
8	Architecture details data and service, process flows (OV-6c)	4	3	3	2	2

Figure 8. Technical Specification and Architecture Audit Phase, Metrics and Ratings

Performance, interoperability, and integration metrics are assessed for (a) the technology, (b) the technology within the operating environment, (c) interaction of the technology with the other systems in that environment, and (d) the technology under full operational load from all systems in the environment in a cyber/electronic warfare engagement. Process and data flows are assessed, as is the cybersecurity of the system for each process and data flow.

Systems integration functions are similarly evaluated for performance, interoperability, and integration. This step examines the impact of other systems on the equipment and the impact of the new equipment on the existing configuration. Data and process flows are examined at the interface level.

The auditors assign weights/ratings to the tests, and these data populate training databases for machine learning. AI helps the decision makers understand the findings while reducing the complexity of the audit metrics.

Conclusion

Supply chain integrity analysis requires assessment of a complex mix of dynamic and adaptive variables. Systems lifecycle evaluation includes not only the equipment being tested, but also the impact of the collective enterprise, interplay of hosting networks and intervening systems, and remote data processes. Measurements are against metrics derived from models and their variables—prior to acquisition for alignment and post-acquisition for in-service analysis. The method advanced in this report provides a technique to evaluate supply chains to address variables that impact systems integrity and a workflow for in-service auditing and assessment.

Initial levels of analysis were presented, with examples for high-level audit variables, their metrics, and measurement methods. The research addresses the problem of engineering practices which do not adequately address cybersecurity, information assurance, and data validity over the lifecycle of a system. The method, framework and techniques were active for 15 years on ships, in network operations and fusion centers, and in deployed shore facilities to assess naval and joint forces technologies. This included field tests of over 500 complex systems-of-systems innovations in live operations. Through this research, the supply chain problems became readily apparent. Techniques advanced herein were proven to verify systems and validate data.

The approach layers independent audits with information assurance and cybersecurity as facets of quality management and associated performance controls. Audit layers were presented as enhancements to the basic acquisition process. Separation of assessment into an independent unit reporting to acquisition departments will help avoid entanglements that impact auditors in naval systems analysis.

To evaluate the framework and workflow, a proof-of-concept will be developed. AI and multi-database capabilities will be presented in the final report. In future research, AI may be further applied to help with supply chain decisions and ensure systems integrity. Preliminary tests with weights for the machine learning algorithms seem promising and worthy of development. For acquisition personnel, the AI prediction capabilities for equipment viability based on specifications and previous test results seem promising. Development of machine learning processes into repeatable formal methods is an additional area for future research.

References

Adee, S. (2008). The hunt for the kill switch: Are chip makers building electronic trapdoors in key military hardware? *IEEE Spectrum*. Retrieved from http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch

Camp, L., Goodman, S., House, C., Jack, W., Ramer, R., & Stella, M. (2006). Offshoring risks and exposures. In W. Aspray, F. Mayadas, & M. Vardi (Eds.), *Globalization and offshoring of software* (Ch. 6). New York, NY: Association for Computing Machinery.

Center for Public Integrity. (2014). Counterfeit chips plague Pentagon weapons systems. Retrieved from https://www.publicintegrity.org/2011/11/07/7323/counterfeit-chips-plague-pentagon-weapons-systems

Cooper, S. (2009). How China steals U.S. military secrets. *Popular Mechanics*. Retrieved from https://www.popularmechanics.com/military/a746/3319656/

Dean, J., & Li, L. (2002). Issues in developing security wrapper technology for COTS software products. In *Proceedings of the First International Conference on COTS-Based Software Systems*. New York, NY: Springer.

Dorofee, A., Woody, C., Alberts, C., Creel, R., & Ellison, R. (2013). *A systemic approach for assessing software supply-chain risk*. Washington, DC: U.S. Department of Homeland Security.

Du, D., & Ko, K. (2014). *Theory of computational complexity*. New York, NY: Wiley.

Grow, B., Tschang, C., Edwards, C., & Burnsed, B. (2008). Dangerous fakes: How counterfeit, defective computer components from China are getting into U.S. warplanes and ships. *Business Week*. Retrieved from https://www.bloomberg.com/news/articles/2008-10-01/dangerous-fakes

IDEF. (n.d.). IDEF family of methods: A structured approach to enterprise modeling & analysis. Retrieved from http://www.idef.com/

ISO. (n.d.). International Organization for Standardization: Standards. Retrieved from https://www.iso.org/standards.html

Johnson, R. (2011). The Navy bought fake Chinese microchips that could have disarmed U.S. missiles. *Business Insider*. Retrieved from http://www.businessinsider.com/navy-chinese-microchips-weapons-could-have-been-shut-off-2011-6

Kern, C. (2014, September). Securing the tangled web: Preventing script injection vulnerabilities through software design. *Communications of the ACM*, *57*(9), 38–47.

Ladyman, J., Lambert, J., & Wiesner, K. (2013). What is a complex system? *European Journal for Philosophy of Science, 3*, 33–67.

Lindqvist, U., & Jonsson, E. (1998). A map of security risk associated with using COTS. *IEEE Computer*, *31*(6), 60–66.

Maule, R. (2016). Complex quality of service lifecycle assessment methodology. In *Proceedings of the 5th International Conference on Big Data*. San Francisco, CA: IEEE.

Maule, R. (2017). *SEA Cyber Figure of Merit (CFOM): Tactical systems cybersecurity assessment*. Monterey, CA: Naval Postgraduate School.

Maule, R., Jensen, J., & Gallup, S. (2014). *Trident Warrior Analysis Reports 2011–2013.* Norfolk, VA: U.S. Fleet Forces Command.

Maule, R., & Lewis, W. (2011). Performance and QoS in service-based systems. In *Proceedings of the World Congress on Services Computing*. Washington, DC: IEEE.

McMullen, T. (2015). It probably works. *Communications of the ACM*, *58*(11), 50–54.

National Research Council. (2005). *Network science*. Washington, DC: National Academies Press.

Rossi, B. (2012). Security backdoor found in China-made US military chip. *Information Age*. Retrieved from https://www.information-age.com/security-backdoor-found-in-china-made-us-military-chip-2105468/

Space and Naval Warfare Systems Command (SPAWAR). (2015). *Cybersecurity figure of merit*. San Diego, CA: SPAWAR 58000.

Tiropanis, T., Hall, W., Crowcroft, J., Contractor, N., & Tassiulas, L. (2015). Network science, web science, and Internet science. *Communications of the ACM*, *58*(8), 76–82.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CA 93943

www.acquisitionresearch.net