Constructing an Authoritative Source of Truth in a Changing Information Landscape

Tyler Smith, tyler.smith@adventiumlabs.com; Charles Payne; charles.payne.@adventiumlabs.com; and John Shackleton, john.shackleton@adventiumlabs.com

This work was supported by the United States (US) Army Combat Capabilities Development Command Aviation & Missile Center under the Joint Multi-Role Mission Systems Architecture Demonstration Capstone project. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of US Army Combat Capabilities Development Command Aviation & Missile Center.

Abstract
In support of the US Army Mission System Architecture Demonstration, Adventium Labs conducted a series of interviews and demonstrations to determine requirements, best practices, and available tool capabilities for building and maintaining an Authoritative Source of Truth (ASoT). An ASoT is a capability that gives definitive answers to queries about a target collection of systems. An ASoT should make information discoverable, enable controlled information sharing, and maintain traceability across time and organizations. The challenges to establishing an ASoT include limited standards adoption by tool vendors, entrenched workflows, and data rights management needs. The systems engineering community can overcome these challenges by keeping ASoT needs at the forefront when planning engineering activities, investing in open and flexible standards for information sharing, and leveraging emerging connectivity tools and model-based systems engineering methods.

Keywords
digital engineering, authoritative source of truth, information management, model-based systems engineering

1.0 Introduction

US Department of Defense (DoD) procurement authorities are shifting to a paradigm in which there will always be a "credible threat of re-compete," by enabling the acquiring agency to own enough of the system architecture so that they can change vendors without a complete restart. Success depends on describing the system as separable building blocks. Emerging technologies, such as the congressionally mandated Modular Open Systems Approach, the Future Avionics Capability Environment (FACE™) Technical Standard, and Model-Based Systems Engineering (MBSE), provide key support while introducing new challenges. Whereas authorities once accepted only paper documents, they must now accept a variety of machine-generated artifacts. Whereas authorities once worked with a single intellectual property owner, they now must navigate multiple owners and data rights. To meet these challenges, the DoD calls on its programs to establish an Authoritative Source of Truth (ASoT) that will embody core capabilities such as information traceability, access controls, and provenance (DoD Digital Engineering Strategy, p8. See https://www.acq.osd.mil/se/docs/2018-DES.pdf).

Recently the US Army, as part of its Joint Multi-Role Mission Systems Architecture Demonstration *Capstone exercise*, tasked Adventium Labs to elicit, refine, and exercise requirements for an ASoT. The objectives of this study were to (1) define requirements for an ASoT at a sufficient level of detail as to enable its acquisition and use in support of future DoD model-

based system developments and (2) provide proof-of-concept demonstrations that the requirements could be satisfied using available technologies. This paper summarizes our results from that study.

The study revealed that the true value of the ASoT lies in its capture of *relationships* between system artifacts. While we may imagine the ASoT to be a *single repository with a single owner* that holds everything that the DoD needs to build the operationally approved system, in reality the ASoT will be a *program-specific collection* of component repositories *under the control of multiple stakeholders* that uses a mix of standardized, custom, and manual interfaces along with stakeholder-specific knowledge and processes, all operating under manual control and oversight, to manage builds of the system. Although we might hope that the contents of the ASoT derive from *discrete, standalone* build processes, those contents will derive from time-sensitive selections from vendor-proprietary product lines, and the DoD must specify in advance the details that it will require to re-compete those contents. The study also revealed that although building an ASoT is technically feasible, much work remains to communicate its proper use among all of the stakeholders.

In Section 2, we briefly recount our investigative process. In Section 3, we summarize our recommendations for procuring and assembling an ASoT. In Section 4, we provide references to additional resources (including the long form report of our study).

2.0 Our Process

The Capstone exercise focused the method and goals of our investigation. The Capstone exercise brought together major aerospace organizations (*Capstone performers*) to collaborate, develop and exchange models and software, and "put some miles" on the digital engineering tools and standards that have been gaining momentum during the past decade. The performers also received model-based Government Furnished Information (GFI) to inform their designs. In the context of the Capstone exercise, we conducted a broad conceptual exploration via user stories, refined those user stories to requirements with input from our Army customer, and conducted feasibility demonstrations driven by the DoD's prioritization of the requirements.

We elicited user stories from interviews with DoD stakeholders and Capstone performers, and from surveys of existing research. From these interviews and a review of prior research on ASoT, we collected 170 user stories describing ASoT use in twenty-five stakeholder domains. To distill requirements from these user stories, we refined our terminology enough for the requirements to be actionable. We collected and refined a collection of terms, all of which we provide in our long-form report. For example, we created a simple definition of an ASoT that reflects its value as a repository of system artifacts and relationships.

An Authoritative Source of Truth is a capability that gives definitive answers to queries about a target collection of systems.

We also identified a simple term to represent the atomic contents of an ASoT.

A digital artifact is a specific, unique, and immutable piece of information. A digital artifact has a fixed length and fixed internal structure.

As shown in Figure 1, an ASoT is a capability (composed of a combination of tools, people, processes, and rules) that gives definitive answers (backed up by business rules for the relevant organization) to queries (requests for information) about a target family of systems. The answer to a query comes in the form of digital artifacts.

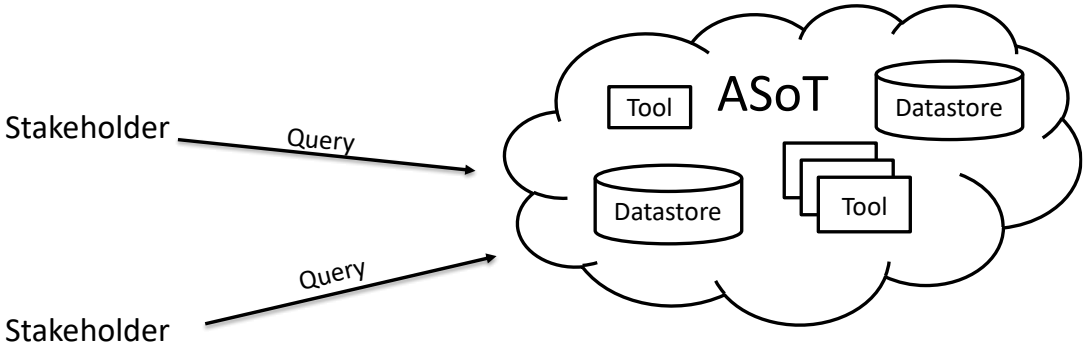

Figure 1: Authoritative Source of Truth in context

3.0 ASoT Requirements

From these user stories and these terms, we derived 123 use cases, from which we derived 103 requirements (you can find a link to these at the conclusion of this article). The requirements enumerated ASoT support across fourteen capability categories: access control for digital artifacts, authoritative state definition, autonomous operation of the ASoT itself, certification of fielded systems, collaboration across ASoTs and stakeholders, configuration control for digital artifacts, custom views of current state, metadata collection, queries, re-compete of digital artifacts, resilient operation of the ASoT itself, traceability of digital artifacts, tradeoff analysis between design alternatives, and workflow definition. We shared these requirements Army stakeholders and Capstone performers, and we incorporated their feedback. The long form of our report includes the Capstone performer feedback and the Army's prioritization of the user stories. The Army identified fifteen high priority user stories, with the most critical in the areas of access control, authoritative state, and traceability. Table 1 provides descriptions of these three categories (we provide descriptions of the other categories are in the full report).

Table 1 Descriptions of Critical Priority Requirements Categories with Select Examples

Requirements Category	**Description**	**Example Requirements (With Reference Number)**
Access Control (User Story 2702)	The ASoT must restrict access to stakeholder intellectual property according to typical security policies, restricting both regular users and ASoT administrators. The ASoT must revoke access when required, and stakeholders must be able to verify the access permissions for their own artifacts.	3468: The organization owning the information shall define security policy protecting digital artifacts according to their information sensitivity. 3432: The ASoT shall implement security policy protecting digital artifacts according to their information sensitivity.

Requirements Category	Description	Example Requirements (With Reference Number)
Authoritative State (User Story 2595)	The ASoT must support virtual integration of digital artifacts. The Government Program Manager (PM) for the system of interest defines what is authoritative for that system, but the PM may not own or control all the artifacts so designated. Artifacts may be owned or controlled by other Government PMs or outside suppliers, each with their own ASoT to manage the artifact. As a result, the ASoT for this PM may be a distributed collection of ASoTs that this PM designates authoritative at a given point in time. Regardless of the composition, the PM views its ASoT as a single, centralized repository that documents the design authorized for virtual integration along with evidence generated by approved analysis tools that the design obeys its constraints and that the design reflects an as-built system that will pass certification and the corresponding analysis results.	3452: The ASoT shall provide a version control system for storing and managing digital artifacts. 3463: The ASoT shall provide a means to associate one or more certifications with a specific version of a model artifact.
Traceability (User Story 2545)	To support certification/qualification, the ASoT must generate evidence that the system analyzed is the system as built. While a change control system provides benefits, a typical change control system may not track all required relationships. A change control system tracks individual artifacts, but the ASoT should also be capable of tracking the processes that produce those artifacts and the resulting analyses of those artifacts. The ASoT needs to track the use of government template models by performers and track the tools that produced analysis results. The ASoT must track functional and performance specifications and relate similar but distinct artifacts. The ASoT should inform stakeholders automatically of actions affecting artifacts they own or control. The ASoT must repeat analysis of evolving artifacts and be able to compare different analyses of the same artifact over time. Finally, the ASoT must support discovery of artifacts through these traceability links.	3459: The ASoT shall provide a means to associate a set of analysis results with specific versions of analysis tools. 3460: The ASoT shall maintain a registry of approved modeling and analysis tools, supporting different versions thereof. 3496: The ASoT shall notify the owner of digital artifacts of changes in automated analysis results for those artifacts.

The requirements also provided the objectives for three demonstrations. Each demonstration showed an assortment of tools and technologies targeting selected ASoT requirements. Demonstration one focused on requirements management. Demonstration two focused on analysis and change propagation. Demonstration three focused on traceability and defining a digital thread across multiple repositories. Figure 2 summarizes the tools applied for each demonstration.

Technology	Purpose	Requirements Elicitation	Demonstration One	Demonstration Two	Demonstration Three
DOORS NG	Requirements Management				
Django	Web Framework				
MagicDraw	SysML Modeling				
GitLab	Version Control				
Teamwork Cloud	SysML Version Control				
Syndeia	Artifact Synchronization				
OSLC	Model Interoperability				
OSATE	AADL Modeling and Analysis				
CAMET	Model Analysis				
Jenkins	Continuous Virtual Integration				
OpenMBEE	Model Management and Reporting				
ARAS	Product Lifecycle Management				
Neo4J	Graph Database				

A filled box indicates we used the technology in the activity.

Figure 2: Tools used for various aspects of ASoT demonstrations

We conducted our demonstrations using an open-source FireSat SysML (From Friedenthal and Oster, http://sysml-models.com/spacecraft/models.html) model as a starting point, from which we built and expanded a systems engineering scenario. Our Army customer indicated that their highest priorities for demonstration were security and traceability. We defined notional stakeholders and used the tools shown in Figure 2 to demonstrate methods for conducting engineering activities among multiple stakeholders, with a specific emphasis on security and traceability capabilities of the tools. For example, we demonstrated traceability from requirements in DOORS NG to MagicDraw to Architecture Analysis and Design Language models in OSATE.

We found that the capabilities to meet ASoT requirements are available in commercial and open-source tools, but that the integration of tools from multiple vendors into workflows required non-trivial effort. For example, Open Services for Lifecycle Collaboration (OSLC) is a standard that provides mechanisms for integration of multiple tools, but vendor adoption of OSLC is not uniform.

These demonstrations provided a reference point from which to establish generalized recommendations for DoD and industry stakeholders who will own, assemble, or use an ASoT. Although we did not have time or budget to exercise all of the ASoT requirements, we were able to establish an understanding of existing tool capabilities such we can make the following recommendations with confidence that they are feasible.

4.0 Recommendations for ASoT Acquisition and Assembly

We draw our recommendations from the results of our demonstrations and from the same source material used to generate the ASoT requirements: user stories, interviews with industry and US

government subject matter experts, surveys on existing practice, and prior research. At the acquisition planning stage, the DoD should identify documents that may need tailoring to include ASoT procurement for a program. Internal government documents, such as the System Engineering Plan (SEP), should address engineering tools and data delivery methods including products and licenses required for the ASoT. The technical review section of the SEP should address how information such how stakeholders will use models in the ASoT for review and document generation. The DoD should include the requirements for the use of an ASoT in a program during the Request for Proposal (RFP) planning stages.

Our recommendations fall into three categories: things to acquire and store in an ASoT, things to communicate to other stakeholders who will access that ASoT, and considerations for assembling an ASoT. We examined our sources for situations in which, in order for the DoD to achieve its objectives, the DoD must acquire something from its suppliers to store in its own ASoT.

What to Acquire

When acquiring digital or physical resources, procurement staff should address the following needs:

- Acquire the digital artifacts the DoD needs to approve and recompete the fielded system. "Knowing what you know" was a recurring theme in our discussions with stakeholders; data does no good if you cannot find it or do not have the rights to use it. Digital artifacts that the DoD requires to recompete the system should exist within an ASoT that is under the DoD's control. Mark the digital artifacts approved for integration, and associate with each digital artifact the evidence that justifies that approval. Track the system throughout its lifecycle to identify the as-approved, as-built, as-maintained, and as-destroyed versions of the system. Acquire models to represent legacy components.
- Acquire the data rights for each digital artifact that the DoD stores in the ASoT. Data rights were a major concern for both industry and Government stakeholders. Government needs to procure sufficient data rights to provide flexibility, while also protecting the intellectual property performers. Consider technical data, computer software, and computer software documentation data rights and communicate the DoD's desired rights in the solicitation for each procurement based on the TD and CS strategy according to Defense Federal Acquisition Regulations Supplement (DFARS) 207.106 in the Acquisition Planning Phase of the procurement. The Statement of Work and CDRL should identify negotiated data rights for each digital artifact to be delivered in the ASoT.
- Acquire required metadata for each digital artifact needed in order to support access control, search, approval, and recompete. Develop and adhere to a standard for the metadata collected. The ASoT requirements call out collecting artifact expiration dates, country-of-origin, country-of-delivery, information criticality, non-functional requirements such as manufacturing constraints, and cost and scheduling metrics. The ASoT requirements also call out evidence to demonstrate the provenance of digital artifacts, such as the tools used to build or generate the artifact, the contract guidance used to produce the artifact, marking and licensing information (even from previous contracts), template models used to produce the artifact, and analysis results and certification results associated with specific versions of the artifact.

What to Communicate

When engaging with stakeholders about a new or ongoing DoD procurement activity, the owners of the ASoT should communicate the following expectations:

- Communicate the approved tools that the DoD will require stakeholders to use. Communicate these selections in the solicitation and/or Statement of Work. The ASoT requirements call out the need for a registry of approved modeling and analysis tools and the need to store the model analysis results in a systematic way that supports examination by subject matter experts.

- Communicate the types of digital artifacts that the ASoT will manage. The ASoT requirements provide examples such as models associated with legacy components, DoD template models, models developed under the performance of this contract, and government-furnished information.
- Communicate data rights and distribution marking policy for all types of digital artifacts that the ASoT will manage. Communicate the granularity with which markings are to be applied within diverse types of artifacts. For example, policy might call for data rights markings applied at the level of blocks in a SysML model.
- Communicate the approved representations for each type of digital artifact. Adopt and adhere to a set of approved representations (languages, formats) to facilitate interoperability between different ASoTs and to simplify the recompete of any digital artifact. During our demonstrations we found that contemporary tools can manage and relate different data representations, but to configure and maintain these tools requires engineering effort. For example, we were able to automate synchronization between a requirements database and a SysML model, but configuring the network connections, authentication, and customized settings required for each tool required engineering effort .
- Communicate the security policies that will enforce authorized access to digital artifacts stored in the ASoT. Stakeholders contributing digital artifacts to the ASoT should understand how the ASoT will protect those artifacts. The ASoT requirements call for security policies addressing, for example, information sensitivity, contractual rights, and organizational role.
- Communicate the change management system within the ASoT that will manage digital artifacts. The ASoT requirements call for a change management system, including each stakeholder's role therein, that includes issue tracking and resolution, comparing and merging different versions of an artifact, and staging proposed changes for approval before submission.
- Communicate the planned execution of DoD-selected operations over digital artifacts. The ASoT requirements include calls for the ASoT to query and visualize artifact associations, to schedule automatic execution of user-defined analysis over artifacts, to notify the artifact owner of changes, and to facilitate translation of artifacts to alternate representations or languages. During the demonstrations on this study, as well as in the Joint Multi-Role Mission System Demonstration as a whole, we found that early communication of planned analysis is critical to ensuring that digital artifacts contain the necessary information in the necessary format for analysis (See our prior work on inter-organization virtual integration: https://www.sae.org/publications/technical-papers/content/2018-01-1944/).
- Communicate the interfaces approved for access to other stakeholder ASoTs, such as OSLC. Our tool survey revealed that of the two common approaches for tool integration (either build a custom interface or build to a common standard), building to a common standard is more scalable and better supports future capabilities.

What to Assemble

When constructing an ASoT or maintaining an existing ASoT, the ASoT owner should embrace the following guidelines:

- When purchasing tools to assemble an ASoT, consider the costs and risks of changing tools in the future. Consider whether individual components in an ASoT are individually replaceable. Tools that support standardized, interoperable data representations and interfaces provide flexibility and enable the “credible threat of re-compete” for the ASoT itself.
- Establish a consistent approach towards the definition of equivalency relationships within the Model Based Engineering Environment. Specifically, a rigorous process must be in place to establish equivalency relationships, and to modify or remove equivalency

relationships when associated artifacts change, undergo versioning, or are removed. Without a consistent process, equivalency relationships can become confused, corrupted, or lost, leading to unreliable traceability throughout the ASoT implementation.

- Invest in open standards. To meet engineering objectives an organization may need to use multiple tool environments. For example, an organization might use MagicDraw for a modeling environment, IBM DOORS for requirements management, and IBM Rational Change Management for change management. Any significant engineering effort generates a vast amount of data, with data overlapping in representation and storage. An ASoT should integrate accumulated data so that query operations can traverse data relationships. For example, an organization may wish to integrate MagicDraw and DOORS by enabling access to DOORS information from the MagicDraw tool environment. OSLC is one open standard approach to achieve such tool integration. In demonstration two we demonstrated use of Intercax Syndeia to transfer requirements between DOORS and MagicDraw.

5.0 Conclusions

The major systems procurement environment is moving away from siloed, sole-source systems to systems composed of modular components from multiple organizations. The artifacts associated with these systems are similarly evolving to provide increased modularity and portability. To manage these design artifacts, we need a capability to provide definitive answers to queries about the systems. This capability comes from an authoritative source of truth. We created a set of requirements for an authoritative source of truth, then demonstrated approaches to meeting those requirements. We generated guidance ASoT users and stakeholders, such as procuring systems with the authoritative source of truth in mind, being mindful of artifact identity, and investing in open standards for connectivity between tools.

The long form report for this study (which includes the ASoT requirements in appendix A) is available at https://www.adventiumlabs.com/publication/authoritative-source-truth-study

About the Authors

Tyler Smith has over ten years of experience that covers data modeling, software integration engineering, and user interface design. Tyler is leading the Army-funded Future Vertical Lift support effort, for which Adventium Labs is providing Model Based Engineering expertise, and FRIGATE, a NASA-funded effort to generate failure recovery plans from traditional engineering models. Tyler led the Army-funded ASoT study evaluating and demonstrating capabilities for analyzing design artifacts across multiple tools and organizations. He also led the Navy-funded SLICED project for software behavior integration analysis.

Charles Payne has over thirty years' experience performing computer security research at industry and government laboratories. He is currently the technical lead of development teams producing cybersecurity analysis tools supporting the US Army's Model-Based Systems Engineering (MBSE) activity for future mission systems. These tools reduce the cost and effort to qualify systems against US Department of Defense (DoD) cybersecurity standards, including the Risk Management Framework (DoDI 8510.01) and Cross Domain Policy (DoDI 8540.01).

John Shackleton has over twenty-five years of engineering experience, specializing in real-time embedded systems, model-based engineering, and cybersecurity. Since 2013 he has served as the principal investigator for several Adventium Labs research projects. John is currently leading the effort on the DARPA Cyber Assured System Engineering (CASE) program, subcontracted to Collins Aerospace, to develop an automated AADL-based build environment for unmanned vehicle platforms. Additionally, John was the technical lead for the Adventium ASoT study, responsible for developing a series of prototype demonstrations that highlight particular ASoT requirements.