2016 Conference on Systems Engineering Research

# Digital System Models: An investigation of the non-technical challenges and research needs

Jack B. Reid and Donna H. Rhodes*

*Systems Engineering Advancement Research Initiative, Massachusetts Insttute of Technology, E38-572, 77 Mass. Ave, Cambridge, MA, 02139*

**Abstract**

Models are increasingly used to drive major acquisition and design decisions, yet the diverse set of model developers, analysts, and decision makers are faced with many challenges in transitioning to a model-centric paradigm. As part of a larger research program on interactive model-centric systems engineering, this paper focuses on the *Digital System Model* in context of the larger topic of the digital framework including Digital Thread and Digital Twin. With a goal of contributing to the continued understanding of problems and concerns, this paper presents findings from the investigation of the non-technical aspects, specifically intellectual property and knowledge assessment concerns. Accordingly, the respective research needs are identified and discussed.



*Keywords*: model-centric engineering; digital twin; digital thread; digital system model; non-technical; intellectual property

## 1. Introduction

The US Department of Defense (DoD) has begun development of a digital framework under which it and its industry partners can operate in a model-centric environment. This framework, is comprised of the Digital Thread, Digital Twin, and Digital System Model (collectively referred to in this paper as a digital framework), is perhaps the most ambitious and the highest potential application of model-based engineering (MBE) to date. Under this digital framework, information will be shared quickly, systems will be designed holistically without losing detailed information, and the entire acquisition process may be greatly accelerated.

While clear, though surmountable, technical challenges exist in the creation of this digital framework, such as computing power and model fidelity, this paper will examine some issues that have not been thoroughly examined

* Corresponding author. Tel.: +1-617-324-0473; fax: +1-617-253-3641.
*E-mail address:* rhodes@mit.edu

in previous literature on the topic, specifically issues of intellectual property (IP) and knowledge assessment (KA). IP in this context refers to any piece of information owned or held in some way by a person or organization. In the defense industry, this includes patents, software (or algorithms more generally), material data, business approaches, trade secrets, etc. A key characteristic of IP is that, while information can be easily shared, value exists in information asymmetries (i.e. possessing information or IP that others do not). Since the construction of such a digital framework fundamentally requires the integration of IP from multiple sources, issues of valuation, compensation, and protection of IP arise. KA refers to the assignment of validity to any particular piece of information or expertise. This can be a technical process, such as double-checking statistical methods used to evaluate the results of an experiment, or a more social process, such as deciding which news source to trust. In the context of this paper, KA issues include "buy-in" (i.e. trust) both by technical staff directly creating the models and by decision-makers in the acquisition and operation processes, as well as inter-model validity assessment in the cases of multiple models operating in the same domain (e.g. two crack-growth modeling methods).

This paper focuses on the non-technical challenges of DSM within the larger topic of the digital framework with a focus on US DoD implementation. The goal of this paper is not to resolve the IP and KA issues but rather to clearly state them in a manner promoting development of solutions and to recommend some specific avenues of approach in resolving these issues.

## 2. Background

### *2.1. Digital Thread/Digital Twin*

The Digital Thread (DTh) is a proposed framework for integrating technical data, costs, predictions, and other accumulated knowledge over the course of design, development, and operation of a system. It is intended to provide ready access to usable information for decision makers during the design process. It includes tools such as tradespace analysis and visualization tools. The term "digital thread" is not a standard; for example, Lockheed Martin Corporation has used the term Digital Tapestry[1] instead. The DoD defines Digital Thread as:
*"An extensible, configurable and component enterprise-level analytical framework that seamlessly expedites the controlled interplay of authoritative technical data, software, information, and knowledge in the enterprise data-information-knowledge systems, based on the Digital System Model template, to inform decision makers throughout a system's life cycle by providing the capability to access, integrate and transform disparate data into actionable information"*[2].

A Digital Twin (DTw) is an integrated model of an as-built product including physics, fatigue, lifecycle, sensor information, performance simulations, etc. It is intended to reflect all manufacturing defects and be continually updated to include wear-and-tear sustained while in use. The goal is to more effectively and safely manage the individual product as well as to facilitate investigations of potential design or operational changes on the health of the system. The DoD defines Digital Twin more specifically as
*"An integrated multiphysics, multiscale, probabilistic simulation of an as-built system, enabled by Digital Thread, that uses the best available models, sensor information, and input data to mirror and predict activities/performance over the life of its corresponding physical twin"* [2].

### *2.2. Digital System Model*

The Digital System Model (DSM) is essentially the proposed product of MBE[3]. It is the integrated model of all technical data that is the general case out of which individual Digital Twins will be constructed, and is the technical grounding that the decision-making analytics of the Digital Thread refers to. The DoD defines DSM as:
*"A digital representation of a defense system, generated by all stakeholders that integrates the authoritative technical data and associated artifacts which define all aspects of the system for the specific activities throughout the system lifecycle."*[2]

### *2.3. Digital Framework*

The digital framework (comprised of DTh, DTw and DSM) has many potential benefits for the DoD acquisition process, including:

- Increased reuse of technical data and models from one project to another, as well as from one stage of a project to another stage of the same project (reduces stove-piping)[4]
- More rapid and cheaper cycling of design concepts in a form of virtual prototyping[3]
- Better analysis and comprehension of complicated systems[3]
- Reversal of the trend of outsourcing technical knowledge from the DoD to contractors and industry partners[5]

This digital framework is not purely hypothetical at present. The DoD and various private firms have actively begun developing and implementing the digital framework or portions of it. For example, the DoD's Computational Research and Engineering Acquisition Tools and Environments (CREATE) program has developed several modelling tools for the design phase[6]. Lockheed Martin used the same 3D solid models of the F-35 Lightning II for engineering design, manufacturing, tooling, and development of training and maintenance materials[7]. The United States Air Force (USAF) is currently testing elements of digital framework on four different acquisition programs[5]. NASA is working on developing Digital Twins for a microelectromechanical system[8].

Other non-defense examples exist as well, such as GE's development of Digital Twins of wind farms[9] and Singapore's partnership with Dassault Systèmes is creating a Digital Twin of the city of Singapore as a whole[10]. While not directly related, the interest by other spheres in DSM and DTw highlights their potential usefulness and the fact that technical challenges posed in their development are believed to be surmountable.

### *2.4. Non-Technical Challenges*

The technical challenges involved in creation of DSM are well understood (many since before DSM itself existed as a distinct concept[11]) and are currently being worked on by various parties in government[12], industry[1, 13], and academia[14]. However, while IP issues have occasionally been acknowledged in discussions of DSM[11,14], they appear not to have been directly addressed (with the exception of cybersecurity). Similarly, while KA issues have been examined by some researchers previously[15], they have thus far failed to be considered as priorities by many parties.

These non-technical challenges should not be downplayed or neglected. While overcoming the technical challenges addresses DSM power and capability, if left unaddressed, IP and KA issues could substantially reduce the applied effectiveness of DSM. Working to identify and address such issues may proactively prevent DSM from being at risk of becoming an expensive, powerful, but unused tool in DoD's acquisition and operations portfolio.

This paper provides an overview of some possible IP and KA considerations and their relevance on the digital framework, and DSM in particular (Sections 3 and 4, respectively), before discussing some potential structures of DSM that could address these concerns (Section 5). Not intended as an exhaustive list of possibilities, these structures offer a starting point for considering how these non-technical issues can be navigated without sacrificing the benefits of DSM.

## 3. Intellectual Property

In the modern era, IP is often as least as valuable as physical capital. This is particularly true in technology-centric industries, including defense. The advantages that the US has over many other countries is not merely in terms of physical or human labor resources, but also in terms of intellectual capital, including both the skill levels of the employees and the value of their intellectual output[16]. As a result, the US has developed many robust mechanisms for protecting intellectual property. Some are enforced by the government, such as patents, copyrights, and trademarks. Others are privately enforced, such as non-disclosure agreements (NDAs). Trade secrets have both government and private enforcement mechanisms.

DSM itself is incredibly valuable IP. As the integration of all "authoritative data and associated artifacts" possession of the DSM could allow for full understanding of the system and its individual subsystems. Many aspects of manufacture and assembly would likely be either directly included in or could be indirectly inferred from the DSM. The simulation and design assessment capabilities of DSM and the digital framework as a whole significantly decrease the difficulty in understanding the system. These aspects are an integral part of the potential benefits of DSM, but this strength is also a critical area of concern with regards to cybersecurity. Where previously, an attacker would have to steal hundreds or thousands of documents from dozens of organizations and then sort through these documents in order to understand the system, with DSM, the attacker could have a single target to go after, a target

that is designed for easy learning. Additionally, since the intention of DSM is for the same model to be used throughout the acquisition process, an attacker could potentially introduce malicious changes into the model during the manufacture stage that would become instantiated in the actual product. Cybersecurity is not a novel concern to the DoD, however, and the cybersecurity implications of DSM have been well understood for several years[11,17].

Beyond cybersecurity, DSM must have buy-in from its various collaborators. KA issues will be discussed in a later section (Section 4) but another key issue here is the sharing of IP among competitive firms. If one firm owns the system being designed, from start to finish, then DSM would be a relatively simple matter with regards to IP. If the same firm also operated the product, than the development of Digital Twins would likewise be a straightforward addition. This is not the case in the defense realm. The DoD sets requirements and is the operator of the end product. Multiple teams of firms then bid on the project. Even after one team has been selected, this team will often use other firms as suppliers. These teams are not fixed groups; on one project two defense contractors may be cooperating, while on another simultaneous project they may be competitive rivals. As a result, these firms may be unwilling to share the detailed IP required by DSM. One approach to addressing this issue in the past has been through a combination of non-disclosure agreements (NDAs) and a design process where subsystem interfaces are rigidly defined but the actual subsystems themselves are largely treated as black boxes[18]. This allows for one firm to maintain control over their IP, while delivering only the final product to the larger working group. Overcoming the design limitations that this approach introduces is a major goal of DSM, which seeks to more holistically model the system, and thus new methods of addressing IP concerns will be required.

### *3.1. Patents*

Patents have some potential usefulness in encouraging the creation of DSM. Jointly developed technologies for simulation and model integration methods could be protected under patents shared by the developers. Under the Cooperative Research Act and its amendment, the Standards Development Organization Advancement Act, cooperative research towards developing a DSM standard would potentially be protected from antitrust litigation, as it is a research area of national interest[19]. This is a ready extension of activities that the Digital Manufacturing and Design Innovation Institute (DMDII) is already pursuing[13].

It should be noted that the use cases of patents in the defense industry are somewhat constrained in this context. First, all patents must be publically published by the US Patent and Trademark Office (USPTO), which is clearly contrary to the classified nature of many defense technologies. Second, the cooperative development style described above only works for shared technologies, which applies primarily to the development of the DSM framework. With regards to the systems and subsystems being modeled, many other technologies will be privately held by an individual firm. While some of these technologies could be protected under patent law, many valuable forms of IP, such as material properties, are either not patentable or not worth being patented. Overall, patents will be useful in the process of developing the DSM framework, but less so in the actual application of DSM in specific cases.

### *3.2. Copyright*

Copyright has limited application in the context of DSM. While specific presentation of facts, such as experimental results or material properties, are subject to copyright, the facts themselves are not, and thus a restatement in a different format is enough to circumvent copyright. As a result, copyright in general is not relied upon for protecting such information. Similarly, while computer programs, such as modeling software, are copyrightable, the fundamental basis of them, such as specific mathematical methods, are not. This results in variation in the usefulness of copyright as it pertains to software. In cases where the specific software package is itself valuable, such as Microsoft Word, copyright is a sufficient tool of protection. In others where the value is not in the software package but in the technical underpinnings, such as a proprietary modeling program, copyright may not sufficiently guard the IP. Furthermore, while copyright might protect the modeling software itself, it would not protect the models made of products, which are valuable in their own right.

### *3.3. Trade Secrets*

Currently, technology and methods not patented or copyrighted are typically protected via trade secrets. While trade secrets enjoy some legal protections[20], these protections are contingent on the IP being kept secret. Unless the

DoD is the sole holder of the DSM, in order for the DSM to effectively operate, information will need to be shared among firms. One of the more common methods for handling inter-firm sharing of trade secrets is the NDA. While useful, NDAs have their drawbacks when it comes to DSM. For one, they are time-consumptive to complete, which could be an issue if they need to be continually updated during an iterative design process. Additionally, the level of detail of information being shared under DSM is quite high. Firms may not feel that NDAs are substantial enough to protect this information, particularly as the difficulties in discovering violations of NDAs might be difficult or impossible, limiting enforceability of such contracts. Excessive use of NDAs could limit the use of knowledge generated by one project in another project, one of the proposed goals of DSM.

### *3.4. Comparisons*

While some IP issues are unique to DSM, many are not. Other industries and projects that have dealt with these problems may provide insight through either similarity or contrast. In this section, two such comparisons are briefly described.

#### *3.4.1. Standards Organizations*

Standards organizations exist in many industries. Some of these are private groups, such as W3C or IEEE, while others are governmental, such as ANSI or ISO. Depending on the group and the specific standard, compliance may be either voluntary or mandatory, but either way, a common reason for the existence of standards is interoperability of products between firms. While other reasons for standards exist, including health and safety, these are less relevant to the topic of DSM. In general, the development of interoperability standards is motivated by the firms themselves, seeking to eliminate competition in certain dimensions (such as size of customer-base and location of market) and facilitate competition based on the products themselves. In order to avoid violation of antitrust laws, these standards are typically open, meaning that any firm may develop products under the standard. If there is protected IP, such as patents involved in the complying with a standard, then this IP must be licensed under fair, reasonable, and non-discriminatory (FRAND) terms. Additionally, these standards are typically formalized through a consensus method, though the exact definition of consensus varies from one standards organization to another.

In the DSM context, there is little incentive for the industry firms to develop interoperability standards in their models as the size of their customer base is fixed at one, the DoD. Thus interoperability will not allow an expansion of market. The firms may develop their own, limited, proprietary version of DSM in order to develop better products and thus better compete[7], but they will not likely reach out to other firms without external incentives. The power held by being the sole customer, though, does allow the DoD significant leeway in providing those external incentives. If the DoD defines specific interoperability requirements of modeling software or even requires specific modeling software to use, these requirements will be followed by the industry.

It should be noted that as the DoD would the motivating force behind the standardization effort, the DoD is not bound by any consensus method of DSM development, thought it may wish to do so in order to make use of industry expertise and in general to promote goodwill with the industry. Additionally, due to the aforementioned exemptions in antitrust laws (Section 3.1), it may be possible that the IP used to develop DSM does not need to be licensed under FRAND terms. This would mean additional options are open to the DoD regarding the structure of the DSM, as will be discussed in Section 5.

#### *3.4.2. Federal Drug Administration's Sentinel Initiative*

Beginning in 2008, the Federal Drug Administration (FDA) developed the Sentinel Initiative, a new method of active surveillance (in this context surveillance refers to continued monitoring of the efficacy and side effects of medical products post-approval)[21]. Instead of primarily relying upon passive surveillance (e.g. unsolicited reports from healthcare providers, from consumers, and from medical product manufacturers), the FDA sought the capability to actively query medical record data sets to answer safety questions. While medical records are not IP in the same sense as what has been discussed previously, they are considered protected information under such laws as the Health Insurance Portability and Accountability Act (HIPAA). As a result the current holders of the data sets, including healthcare providers (such as hospitals) and health insurance firms, are legally unable to provide these data sets to other parties, including the FDA or academic researchers. The Sentinel Initiative circumvents this

restriction by operating on a distributed system. In this system, data sets never leave their current location. The FDA sends out a specific query to all data partners (those possessors of medical records who are part of the Sentinel Initiative). This query is then processed by each data partner separately, the results returned in aggregate to the FDA without identifying information. In this way the FDA can assess whether drug X is causing side effect Y without violating the privacy of any patients.

In the DSM context, while firms are not legally required to guard their IP, their natural unwillingness to share valuable information accomplishes a similar effect to the HIPAA restrictions. In this way, the Sentinel Initiative poses a potential workaround to this problem. It is possible that, from a firm-to-firm perspective, the modeling software and the models generated with that software may be treated as black boxes with each firm only have access to inputs and outputs of the simulations of the others.

## 4. Knowledge Assessment

Knowledge assessment (KA) is defined in this paper as the assignment of validity to any particular piece of information or expertise. This paper is predominantly concerned with the social aspects of KA, though technical processes, such as verifying a model against experimental data, can also be involved.

### *4.1. Generating Buy-In*

Buy-in can be defined as a combination of trust and willingness in a tool, as well as the ability to use it. This is a non-trivial matter. It is all too easy in any organization for some newly developed tool to sit unused and unmaintained if those who should use it lack the skillset, willingness, or trust for it. Lack of buy-in to a new initiative can a significant and detrimental impact on the enterprise as a whole but can be avoided[22].

Developing the appropriate skillset requires investment in training, reference materials, and experience. Trust and willingness are not as straightforward to achieve. On a technical side, establishing trust requires details, examples, and authority. This means that DSM users should have access to data on technical underpinnings and assumptions for the various models, as well as proof of validation in the form of examples (these can also serve as useful reference materials for developing expertise). This does not necessarily need to be immediately presented to every user at all times, but should be accessible by those who desire it, and at varying levels of detail for different use-cases. Some of this information can be elided in certain cases by referencing standard validation certifications, though these certifications must themselves be trusted by the user and are thus unlikely to be available during the initial implementation of a new tool. The DoD has a framework in place that could be used to catalog this information and make it accessible to users: the DoD Metadata Registry and the Modeling & Simulation Catalog[11].

Beyond providing technical validation data or examples, a key component of generating buy-in is visualization. Visualization is not a mere aesthetic choice of the DSM designers, but rather an important aspect that impacts not only how DSM will be received and used, but also what decisions are reached. Previous research has showed that changing how data or models are displayed can significantly affect risk aversion/acceptance[23], ability to come to a negotiated agreement between stakeholders[24], willingness to use a tool[25], and ability to apply presented knowledge[26]. As a result, attention must be paid to how DSM is presented. This does not necessarily mean that a universal visualization standard should be developed for DSM (though it could), as industry partners may be better served by using different visualization schemes in-house than those used by the DoD. If there is no standard visualization method, however, differences should be documented and made clear, as these could affect decision-making and lead to conflicts in assessments of model results. It should be noted that the importance of visualization applies not only to DSM itself, but also to the reference materials made available to the users for training, as previous research has shown that even the layout of brochures can have significant impact on information gained[27]. As a result, multiple manuals covering the same model may be necessary if different types of users will be interacting with the model.

### *4.2. Model Comparisons/Validity*

If a heterogeneous model structure is chosen (explained in Section 5), as is currently preferred by the DoD, an issue of model comparisons arises. If during the bidding competition, two firms provide DSMs of their preliminary design, but are using different modeling software within each DSM, there may be some difficulty in comparing the

simulation results of the two DSMs. This is not necessarily a new issue to the DoD, as claims of competing firms already need to be evaluated in the current acquisition procedure, but it should be acknowledged that this problem will not vanish under the new digital framework.

As will be discussed in Section 5, one potential method of diffusing IP disputes is for each individual model in DSM to be treated as a black box by all participants except for the owner of the component and the DoD. This however introduces evaluation issues that may hamper the design process. Specifically, it falls upon the DoD to ensure compatibility of calculation methods between the models as the firms will be unable to analyze each other's models themselves. This will result in bugs being harder to identify and could result in erroneous model results, jeopardizing both the technical validity of DSM and the trust that the firms have in it as well, reducing buy-in.

## 5. Potential DSM Structures

With these issues in mind, it is worthwhile to consider the structure of DSM along two different dimensions. The first is how the modeling software packages are developed and the second is how the modeling software packages are used. As stated earlier, these options are not intended to be an exhaustive list, but should provide grounding for consideration of IP and KA issues in the design of DSM.

### *5.1. Model Package Development*

In this first dimension, the primary relevant issues are the IP of the modeling software packages (but not the products being modeled) and KA of model comparisons. Three general options exist. The first, and most simple option, is that the DoD develops its own modeling packages for each part of the DSM and then mandates that industry partners use these packages. This could be an extension, though a highly ambitious one, of the CREATE program[6]. This homogenous structure would eliminate any IP disputes over the modeling packages themselves and eliminate any KA issues of resolving inter-model differences. Furthermore, this would alleviate fears of losing access to DSMs of older systems since the completed DSM would not be reliant on any privately-held software. Doing this, however, would fail to take advantage of the large amount of intellectual capital present in the private defense industry and would require the DoD to continually maintain and improve these software packages.

The second option would be for the DoD to standardize the model interface akin to the typical standards development method discussed earlier. This heterogeneous structure would allow each firm to create its own modeling packages (or license those of others as it chose). This option does not directly resolve any IP-sharing issue (that depends on the model usage dimension discussed in section 5.2) nor does it resolve the model validity issues. Unless the software packages are permanently licensed or outright purchased, this option raises the possibility of the DoD not having perpetual access to all components of the DSM, especially if a firm goes out of business or fails to maintain its own modeling packages. It should be mentioned that this is currently the structure favored by the DoD, due to its combination of modularity and openness[28].

The third option is a hybrid of the first two, being privately-developed like the second option, but homogenous like the first. Here the industry partners would be relied upon to generate the modeling packages and these packages would be required to interface with one another, but the DoD would select specific modeling packages to be used for each portion of the DSM, likely in some sort of periodic bidding process (an acquisition project in its own right). The DoD would not just buy or license the modeling software for itself, but also for each other industry partner, otherwise the owner of the selected software package would have effective monopoly power over the other members of the industry. This option does not address the perpetual access issue any more than the second option, but it does resolve the inter-model comparison issue while still relying on the industry to generate and improve modeling packages.

These options, along with their pros and cons, are summarized in Table 1.

Table 1. Summary of Model Package Development Structures

| | Pros | Cons |
|---|---|---|
| **DoD Developed** | Reduces IP disputes | Does not utilize industry expertise |
| | Can maintain access | Requires DoD to maintain and update |
| | Eliminate inter-model comparisons | |
| **Heterogeneous, Privately-Developed** | Fully leverages competitive industry | Does not resolve IP disputes directly |
| | Minimizes DoD work | Requires inter-model comparison |
| | | Potential lack of continued access |
| **Homogenous, Privately-Developed** | Reduces IP disputes | Introduces miniature monopolies |
| | Partially leverages competitive industry | Potential lack of continued access |
| | Reduces DoD work | Does not fully leverage industry expertise |
| | Eliminates inter-model comparisons | Does not minimize DoD work |

### *5.2. Model Use*

The second dimension is, once the individual modeling packages are selected, how do they work together in practice to form the DSM? Once again, three general options exist, two integrated and one distributed, though different variations of each option exist.

The first option is that the complete DSM is held by one party. This could either by the DoD for the entire system lifecycle or it could be the lead industry partner during the design process before transferring to the DoD afterwards. This method could potentially reduce cybersecurity concerns as the DSM would not necessarily need to be connected to any network or the internet. If the DSM is held by the lead industry partner, however, it fails to address the IP-sharing issues. Regardless of who holds the complete DSM, this option may reduce the benefits of the DSM but inhibiting the design process, as it may be difficult and time-consuming for one central authority to keep the DSM updated as well as to continually run simulations and distribute the results to the other industry partners.

The second option is to have multiple copies of the complete DSM, each held by the different firms and organizations involved in the product development process. This option addresses some of the design inhibition concerns of the first option by allowing various firms to run their own simulations. This comes at the cost of introducing additional cybersecurity concerns in whatever syncing process is used between the various copies. Furthermore, as has been discussed by other researchers[14], the DSM is going to be a massive model, in terms of computational power necessary to run simulations with it. It is fully possible that only a select few industry partners would have the computing capability to run the full DSM themselves. In the case of particularly complicated systems, it is possible that only the DoD themselves would have such capability. This may limit the benefits of this option in comparison to the first option, though the industry partners would still likely be able to run the DSM either in part or at lower resolutions, while relying on the DoD for the higher resolution, full system simulations.

The third option is for each firm to maintain control over the models they create and have the DSM exist as a sort of distributed network, similar to the FDA's Sentinel Initiative. Cybersecurity is once again of high concern with such an arrangement and the distributed system may slow down simulation run times, particularly if multiple parties simulate the system at the same time. This option could provide for more robust protections of IP of the industry partners. It is likely that if this structure was chosen, it would only exist prior to hand-off to the DoD, as the DoD would like to maintain the ability to run its own simulations without relying on an entire network of other parties.

Each of these options, which are summarized in Table 2, could be implemented with various degrees of IP protections of the modeling software and the models themselves. In either distributed or integrated form, models and their associated software could be handed off as black boxes working in the kind of framework described in the previous section. This would help alleviate concerns over sharing IP with other industry members but would come at the cost of placing the burden of assessing inter-model compatibility and model comparisons on the DoD, with whom, presumably, full details on the software and models would be shared so these assessments could be made.

Table 2. Summary of Model Use Structures

| | Pros | Cons |
|---|---|---|
| **Centralized – Single Copy** | Reduces IP disputes | Difficulty in updated |
| | Reduces security risk | Hampers iterative design |
| **Centralized – Multiple Copies** | Allows for iterative design | Few firms can host full DSM |
| | | Increases security risk |
| | | Does not address IP disputes |
| **Distributed** | Reduces IP disputes | Increases Cybersecurity Issues |
| | Allows for iterative design | Requires transition to centralized during hand-off to DoD |
| | | Potentially technically difficult |
| | | Increases simulation-run times |
| | | Increases security risk |

## 6. Research Needs

There has been some uncertainty regarding DSM due to the lack of clear distinction between DSM and DTh in previous literature[14]. As a result, it may be worthwhile for future official explanations of the concepts to be more specific about their differences, and perhaps include examples of what is a part of each. Alternately, it may be possible to combine the terms under one title if the concepts referred to are not worth differentiating.

Previous authors have suggested that DSM is contrary to, rather than an extension of, more traditional MBE[14]. If this is the case, additional issues of knowledge assessment by the systems engineering community as a whole would need to be evaluated as well. However, the assertion was not elaborated upon and may, in fact, stem from the aforementioned uncertainty of definitions rather than an actual opposition.

Further investigation by legal experts is needed regarding the potential exception of DSM development from antitrust laws. If the IP used to develop DSM does not need to be licensed under FRAND terms, then additional options are open to the DoD for the structure of the DSM. Regardless of the legality of such options, pursuing a developmental structure that is not under FRAND terms may result in political and/or industry pushback.

Visualization schema and standardization must be considered and intentionally designed throughout the development of the digital framework. This may require comparative testing of multiple display styles or even novel research if existing methods of visualization are insufficient for the systems being designed and managed by DoD.

DoD must serve several roles: customer (thereby supplying financial incentive), the standards enforcer (regulatory incentive), and neutral mediator (serving as non-competing party with whom information can be shared).

## 7. Conclusions

Many assessments of DSM's potential benefits to the acquisition and operations processes appear to assume that the IP and KA issues discussed in this paper would be perfectly resolved, though these same assessments often did not provide means of achieving such resolutions. While these issues are not insurmountable, they require no less attention than the various technical challenges facing DSM. These issues will not resolve themselves and some, such as the user buy-in issue, could scuttle the DSM entirely, even if the technical challenges are all overcome. This is not to be pessimistic, however, as this paper has outlined some viable paths forwards in investigating these issues and finding strategies for achieving the goal of next generation model-centric engineering. The authors hope that this paper will lead to additional investigation into these issues so that they may be overcome moving forward.

## Acknowledgements

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Systems Engineering Research Center (SERC) under Contract HQ0034-13-D-0004. SERC is a federally funded

University Affiliated Research Center managed by Stevens Institute of Technology. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Department of Defense.

## References

1.Lockheed Martin, Digital Tapestry. Available: http://www.lockheedmartin.com/us/what-we-do/emerging/advanced-manufacturing/digital-tapestry.html (accessed November 20, 2015)
2. DoD, "Glossary: Defense Acquisition Acronyms and Terms," US Department of Defense, Defense Acquisition University, Learning Capabilities Integration Center, Center for Acquisition and Program Management, 2015.
3. P. Zimmerman, "MBSE in the Department of Defense," OuSD Systems Engineering, DoD, 2015.
4. P. Zimmerman, "A Framework for Developing a Digital System Model Taxonomy," in *18th Annual NDIA Systems Engineering Conference*, Springfield, VA, 2015,
5. G. Warwick, USAF Selects Lead Programs for 'Digital Twin' Initiative. *Aviation Week & Space Technology*, Penton Corporate. http://aviationweek.com/technology/usaf-selects-lead-programs-digital-twin-initiative, Jan 26, 2015.
6. E. M. Kraft, "HPCMP CREATE TM-AV and the Air Force Digital Thread," presented at the SciTech, Kissimmee, FL, 2015.
7. Lockheed Martin, The Digital Thread Key to F35 Joint Strike Fighter Affordability. Available: https://www.onlineamd.com/article/amd-080910-f-35-joint-strike-fighter-digital-thread, accessed Nov 20, 2015
8. E. Glaessgen and D. Stargel, "The Digital Twin paradigm for future NASA and US Air Force vehicles," in *53rd Struct. Dyn. Mater. Conf. Special Session: Digital Twin, Honolulu, HI, US*, 2012. pp. 1-14.
9. T. Kellner. Wind in the Cloud? How the Digital Wind Farm Will Make Wind Power 20 Percent More Efficient. General Electric. http://www.gereports.com/post/119300678660/wind-in-the-cloud-how-the-digital-wind-farm-will/ accessed Nov 20, 2015.
10. G. Goh, *Building Singapore's 'digital twin'*, Digital News Asia. Sep 15, 2015.
11. NDIA, "Final Report of Model Based Engineering (MBE) Subcommittee," National Defense Industrial Association, 2011.
12. A. Feeney, "Digital Thread for Smart Manufacturing," Engineering Laboratory-Systems Integration Division-Systems Engineering Group, US National Institute of Standards and Technology, 2014.
13. M. A. Aisenberg, D. Davis, and T. D. Kehoe, "Intellectual Property Rights for Digital Design and Manufacturing: Issues and Recommendations," The MITRE Corporation, 2014.
14. T. D. West and A. Pyster, "Untangling the Digital Thread: The Challenge and Promise of Model-Based Engineering in Defense Acquisition," *INSIGHT*, vol. 18, pp. 45-55, 2015.
15. D. Rhodes and A. Ross, "Interactive Model-Centric Systems Engineering (IMCSE) Pathfinder Workshop Report," Systems Engineering Research Center, Systems Engineering Advancement Research Initiative, 2015.
16. S. Smith, "Science and Technology Intellectual Capital: A Critical US Asset," vol. 59, AE&T. Command, USAF, 2010.
17. M. McGrath, "Protecting the Digital Thread," in *Global Supply Chain Summit*, Rockville, MD, 2014, NDIA
18. "Systems Engineering Guide for Systems of Systems," S. a. S. Engineering, Department of Defense, 2008.
19. *Standards Development Organization and Advancement Act of 2004*, U. S. Congress, 2004.
20. "Trade Secret," in *WEX*, ed. Ithaca, NY: Legal Information Institute, Cornell Law School.
21. "The Sentinel Initiative," Office of Surveillane and Epidemiology, Federal Drug Administration, 2010.
22. K. Thomson, L. de Chernatony, L. Arganbright, and S. Khan, "The Buy-in Benchmark: How Staff Understanding and Commitment Impact Brand and Business Performance," *Journal of Marketing Management*, vol. 15, pp. 819-835, 1999/11/01 1999.
23. S. Park and L. Rothrock, "Systematic analysis of framing bias in missile defense: Implications toward visualization design," *European Journal of Operational Research*, vol. 182, pp. 1383-1398, 11/1/ 2007.
24. M. E. Fitzgerald and A. M. Ross, "Effects of Enhanced Multi-party Tradespace Visualization on a Two-person Negotiation," *Procedia Computer Science*, vol. 44, pp. 466-475, 2015.
25. K. Wodzicki, E. Schwämmlein, U. Cress, and J. Kimmerle, "Does the Type of Anonymity Matter? The Impact of Visualization on Information Sharing in Online Groups," *Cyberpsychology, Behavior, and Social Networking*, vol. 14, pp. 157-160, 2011/03/01 2010.
26. A. L. Alexander, T. Brunyé, J. Sidman, and S. A. Weil, "From gaming to training: A review of studies on fidelity, immersion, presence, and buy-in and their effects on transfer in pc-based simulations and games," *DARWARS Training Impact Group*, vol. 5, pp. 1-14, 2005.
27. W. G. Morgan Baruch Fischhoff, A. Bostrom, L. Lave, and C. Atman, "ES&T Features. Communicating Risk to the Public. First, Learn what people know and believe," *Environmental Science & Technology*, vol. 26, pp. 2048-2056, 1992/11/01 1992.
28. P. Zimmerman, "Modularity and Open Systems: Meaningful Distinctions," in *18th Annual NDIA Systems Engineering Conference*, Springfield, VA, 2015,