Carnegie Mellon University
Software Engineering Institute

CRITERIA FOR EVALUATING A SOFTWARE SYSTEMS MODEL

Sholom Cohen

John McGregor

January 2025

Introduction

This study paper addresses questions frequently asked by organizations transitioning to digital engineering. These organizations are involved in the acquisition or development of large-scale systems that integrate hardware, software, and human-executed subsystems. Their questions pertain to the development, analysis, acquisition, review, and validation of models for these systems and delivering digital artifacts. These artifacts form a “digital thread” – an interconnected chain of models that covers all lifecycle phases. The digital thread serves as basis for system analysis, implementation, integration, verification, validation, accreditation and deployment of product systems. The organizations that face the challenges of transition include government acquisition entities, prime contractors, suppliers, and qualification and accreditation authorities.

Digital engineering for physical aspects of systems utilizes computer-aided design, engineering, and manufacturing tools. Use of such digital tools has demonstrated significant value across all industries for many years. Achieving similar success in systems where hardware-software integration is predominant, known as cyber-physical systems (CPS), remains challenging. The development of such systems has faced difficulties in creating and effectively using model-based engineering artifacts. The specific questions we hear include:

- Why do we receive models from suppliers that don’t really address our acquisition needs?
- How do we create and deliver models that satisfy our business drivers?
- How do we create models for CPS that provide analytic results in the same way that models of purely physical systems support analysis?
- How can we use models to support early lifecycle decision-making or tradeoffs in the areas of functionality, safety and security?

In addition, we find many organizations questioning what models to create, who should create them, when in the lifecycle modeling is appropriate, and how to use models in support of milestone reviews.

This report does not examine modeling content that defines a system product. Many modeling languages, tools, and methods exist to provide that content. The topic we address here is more basic – what criteria apply to analyze any model in terms of questions about the system product under development. When these models are under review, analysis focuses on whether the models satisfy specific use cases of stakeholders for the system product. Those use cases focus on either production of the models or use of those models for delivering the product.

Study Structure

Bottom Line Up Front (BLUF)

Government organizations and contractors alike perform extensive modeling efforts as a basis for fielding integrated hardware-software system products. Though modeling approaches have a multi-decade history, the results still fall short of expectations – customers of the models that are delivered find them hard to use, models are often descriptive of system detail but lack analytic potential, models over-emphasize detail, and models cannot be used to support tradeoff or early lifecycle decisions.

Many current models and the modeling approaches used to create them are not sufficient to serve as usable specifications or designs. Where the government produces a collection of models – the model set – to communicate needs to potential vendors or where contractors and suppliers deliver model sets that respond to those needs, the modeling products are assessed as incomplete. Gaps or inconsistencies in model content from government result in products that inadequately satisfy government needs or in products that exhibit misinterpretation of those needs. Contractors and suppliers deliver models that cannot answer the acquirer's questions in terms of functionality, key system attributes, and risk reduction. While models could start with an explicit statement as to model intent and scope, they often lack that very basic content.

This report proposes a set of criteria that, when satisfied, address stakeholder needs, improve existing model-based practices, introduce modeling to address analytic needs, support modeling across the lifecycle of acquisition and development, and advance techniques for supporting model reuse.

Driving question

Scenarios in use of models help form the basic criteria that modeling for CPS must address. From the government perspective the scenario is expressed as follows:

> **Government Scenario***: "As an acquisition organization, we need to acquire a new CPS. We will produce models that contain the acquisition requirements and provide them to a contractor and its suppliers. The primary use case for these models is for developing both refined specification and design models for the CPS. Our intent is to issue those models as a means of contracting with an industry supplier to decompose the requirements and demonstrate a progression of refined models that lead to implementation, integration and deployment of our CPS products."*

For the contractors and suppliers, the formative scenario is expressed as:

> **Contractor Scenario***: "Our organization exists to deliver products to our customers that satisfy their needs and meet their schedule and performance requirements within a set budget. We develop models as a means of*
>
> 1. *demonstrating our understanding of customer needs*
> 2. *showing our progress over the course of development in meeting those needs*
> 3. *providing early lifecycle analysis and tradeoffs*
> 4. *satisfying capabilities*
> 5. *establishing a modeling foundation early in the lifecycle that can be used by customers to review our work and internally for refining specification models into design models ready for analysis, implementation, integration, verification, validation, accreditation and deployment of system products.*

The criteria we need should address the following:

1. how to assess the adequacy of government acquisition models to assure they provide requirements with adequate specification to potential suppliers of needed CPS
2. whether contractors and suppliers are using their engineering capability to model actual CPS products that satisfy these requirements.

In the criteria that follow, we need to establish two sets of use cases for models

1. *Digital thread use cases* define ways that data from the model set must be used. Actors in these use cases include the acquisition authority, modelers, contractors, qualifiers, and other stakeholders of the system product that is planned for and created. The use cases describe how the models themselves will be used in acquisition, for Request for Proposal (RFP) issuance, to conduct tradeoffs and analysis, for system qualification, during reviews, and other actions.
2. *System product use cases* for the system product. Actors in system product use cases are the users of the system product that is ultimately fielded. These use cases may focus on system startup, nominal system use, failure mode actions, and system shutdown.

There will be overlap in actors between these two sets of use cases, but the activities should be modeled as separate use cases. Both sets can proceed through modeling, developing, and operations for verification, validation and accreditation (VV&A). Each set has its own criteria that the respective model sets must satisfy. The criteria for digital thread use cases assess their ability to support acquisition, development and materiel release activities. The criteria for assessing system product models must evaluate content with respect to the product capabilities. Table 1 summarizes the different aspects of each model category and provides an example validation.

Table 1. Aspects of each category of model for digital engineering assessment

Model Criteria Categories	Digital Thread Use Cases	System Product Use Cases
Actors	Acquirers, modelers, contractors, qualifiers	Users of system product, maintainers, developers of systems that must interoperate
Activities	Model is used in RFP Model is used to convey specifications/design Model is used to understand customer need Model is used to support qualification and VV&A	Decompose and allocate requirements to subsystems or components Trace refinements back to source Design system elements Develop test plans and procedures
Concerns	Level of detail and design decisions in specification models. Appropriate coverage of hardware resources, qualities, evaluation mechanisms	System product addresses customer needs. Analysis to determine satisfaction of constraints
Verification	Create model Evaluate compliance with regulation Conceptual description Imposed constraints	Model of system product directed to testing with respect to all test cases and procedures.

Model Criteria Categories	Digital Thread Use Cases	System Product Use Cases
Validation	Create model Use in subset of modeling activities Evaluate and improve models for meeting user needs	Evolve models to implementation and integration Create minimum viable product, execute and test Refine MVP to MVCR
Accreditation	Create model Determine if sufficient information or data is in model to support certification criteria.	Use model as representative of system to support future physical certification.

Criteria for Assessment of a Model

Both government and contractors produce models to document understanding of the needed CPS. These models may be for use internally or by others for a variety of development needs. It is these needs that drive the activities of modeling use cases, that is, how the models will be used in a continuing fashion by the model developer and by others for understanding, analysis, or refinement.

Models should cover aspects needed by a variety of stakeholders in the development of the CPS. For example, the model should include:

- explicit connections to other parts of the model, such as hardware resources, and between multiple models.
- quality attribute (QA) aspects to elaborate the meaning of any QA. If configurability is an attribute, the model must reference the areas needed for configuration, likely in software, and at what time configuration can occur – during development, at build time, at load time, during execution, etc. – or whether by integration as on board or off board
- constraints that must be evaluated for qualification of the CPS including latency, connectivity, bandwidth limitations, processor limitations, logging options, or security needs.

The following criteria concentrate on the modeling content we expect to see in any government or contractor specification model. From that perspective, models from suppliers and contractors document design decisions while specification models from government generally do not include such decisions. Specification models define information needs in abstract terms. Design models refine these abstractions into data design, whether messages for interchange of data or data structures to satisfy computing processing, memory and networking requirements.

The criteria also establish use cases for the model. Analysis that applies these criteria, should establish scope for use of the model, for example, to be used to assess the correctness of the current model and whether it is internally consistent. To assess a specification model in general, we expect to see specific content in the model including:

1. A statement of scope that describes the system product being modeled
2. A clear statement of purpose and intent behind the model
3. The ecosystem of users including acquirers, modelers, model users, as well as the digital environment
4. Questions the model should answer
5. Diagrams needed to define the specification
6. A workflow or activity diagram of model flow across the value stream associated with the ecosystem
7. Use cases for the model (vs. system product use cases)
8. Requirements for products defined by or that will be built from the model

These aspects are defined in the "enabling environment" under a modular open systems approach (MOSA): supporting requirements, acquisition strategies, and business practices. Table 2 summarizes the criteria and applies them in the context of a government specification model. For a contractor design model, the example model content would be applying the criteria to satisfy both elaboration of requirements from the specification model and development of the design model, itself.

Table 2. Description of content to be captured in a specification model

Expected content of a Specification Model	Instructions for Model Content
1. Scope of system product	Define the scope of the system product to be delivered. This may be scoped as a subsystem or component of a full system product and model must define this. Define any non-functional needs (safety, security, performance, standards) that model should include
2. Purpose and intent of the specification model	Use cases for the model. Examples: 1. Acquisition authority provides requirements for a supplier to develop the system product. 2. Qualification authority has information needed to assess future certifiability and gaps.
3. Ecosystem of specification model users	Define roles, responsibilities, and what level of expertise expected from: industry contractor, subsystem supplier, acquisition authority, qualification authority
4. Questions the specification model should answer	What are the product system requirements that must be satisfied by a supplier? What are the design constraints that a conformant CPS must satisfy in terms of resources, timing, scheduling, network access, connectivity? What are the criteria to assess conformance to the specification?
5. Diagrams needed to define the component specification	Block diagram to decompose acquisition item in terms of systems, subsystems or components. Requirements allocated to decomposed blocks Activity diagram showing interactions between user and system or between system product and external systems

Expected content of a Specification Model	Instructions for Model Content
6. Workflow	Acquirer develops specification model of system product and provides that model in RFP Acquirer receives and reviews refined models from contractors proposing to build the system product Contractor develops and delivers models of the system product for review by acquirer and qualification authority Contractor revises and refines models to implementation, integration, and deployment
7. Use cases for the models	Understand and validate requirements Produce the refined requirements Elaborate specification models to design Analyze model content for satisfaction of attribute constraints
8. Requirements for system product to be built and of models for the product	Detailed throughout the model via structure, behavior, data abstractions, system product attributes Model attributes such as readability, usability, traceability, reusability if required

Study Approach

This section applies the criteria to evaluate the utility of models for a CPS. For this study, the models include those to satisfy use cases of both the government and contractor scenarios. We first need to understand the intent and goals of models derived from the scenarios.

Government Scenario: we understand that the intent of this specification model is to specify requirements needed for a contractor to deliver a CPS. The government should produce models that contain the acquisition requirements in terms of product scope and provide them to a contractor and its suppliers. Table 2 further elaborates the content we expect to see in the government specification model. The primary use case for these models is for developing both refined specification and design models for the CPS. This information should be contained in the model, or the model must contain links to related government artifacts that spell out this detail.

Contractor Scenario: we understand the contractor intent as providing products to its customers. For the scenarios in this report, the contractor should satisfy the needs of its government customer based on the government's specification model. The elaboration of that specification model into refined and derived requirements. Contractors also provide design including models of function, behavior, and data design. Combined with analysis for constraint satisfaction and addressing of qualification needs, these models and non-model artifacts provide confidence to the government, that the contractor can meet its schedule and all performance requirements within a set budget. The government should assess all models that are developed to assure that they:

1. establish a modeling foundation early in the lifecycle
2. demonstrate that the contractor understands the government needs

3. show our progress over the course of development in meeting those needs
4. can provide early lifecycle tradeoffs and analysis for satisfying required capabilities

The model criteria in Table 2 can be used by government as review criteria to satisfy specific milestone reviews. They can also be used internally by the contractor to assure that models developed can be used for refinement from specification models into design models ready for development, implementation, integration, configuration audit, VV&A, and deployment of deployed system products.

This model content is essential to understand the intent and goals for applying the models, both those from the government (specification) and those from the contractor (design). These analyses could be combined into the structure of Table 2. The content of the table can then be modeled to clarify the specifics that are present in the delivered model or that must be captured and used to satisfy model use cases under each scenario. Note that these criteria are not based on extensive review of the system product content contained in the models from either government or contractor. The intent of the review defined by this study is limited to addressing model and modeler needs for delivery and exchange of models. Separate studies are required to elaborate and define system product modeling content for specification, design, behavior, data analysis, etc.

Let's now turn to a concrete acquisition scenario. From our experience in product development, we expect an acquisition scenario to be as follows:

> *The program manager (PM) of a ground-based fighting vehicle platform needs a mission computing environment. The environment for the platform must satisfy product-specific functional requirements within various system constraints (SWaP, latency, bandwidth capacity, safety, security). The PM issues a specification model of the computing environment as an RFP to industry and expects contractors to propose solutions that address the specification in model form. The supplier conforming to the specification delivers a response in model format that demonstrates its ability to deliver a product that satisfy the PM's needs. The PM and supplier work together to arrive at models and model content that precisely satisfy the needs of the computing environment for the ground-based fighting vehicle.*

The government specification model should contain content to satisfy this acquisition scenario. Assuming SysML V1 modeling, the specification model should show a block definition diagram to establish the context of the computing environment and functionality under acquisition. It should also show use case diagrams of the ground-based fighting vehicle. But as the criteria establish, the government model should also include content that reflects the stakeholders of the model, the use cases of the model itself – understand the system under acquisition, review the model, develop qualification criteria of the system – and where these stakeholders are use case actors.

Even before bringing computing environment specifics into the specification model, the government can define its plan for elaborating that model. Again, the structure of Table 2 offers a form for capturing that data. If the criteria are applied after modeling has commenced or even completed, the table format provides the evaluation support for refinements of the model. These refinements assure that models address downstream needs. The contractor tasks address a similar set of criteria for creating its models. The contractor executes a planning activity to determine how to best address the modeling criteria in response to an RFP, during development, in planning for reviews, and in applying the models to implement and integrate the computing environment.

Modeling Behavior Context

The government, in the above scenario, applies a modeling technique to construct a model-based product specification for the ground-based fighting vehicle system product. The specification is provided to all entities intending to bid on the acquisition of the product. The specification model can be addressed by a supplier who already has a family of vehicle products. The supplier can then bring one of those products into conformance with the government specification. Other suppliers may propose delivery of a standalone product.

For the purposes of this context discussion there are several models of interest:

> P_{spec} – the model of the government's specification for the computing environment product
>
> $P_{proposed}$ – a model of the contractor's proposed solution or solutions
>
> P_{actual} – the model of an actual solution

Each user of one of these models will evaluate the initial government specification based on their own experience and interests. The experience and interests may be qualified by the following organizational characteristics

- The P_{spec} need not contain certain information if all the potential users of the model possess that information and have a shared understanding.
- Completeness, consistency, and correctness are all evaluated relative to that shared understanding.
- Members of a single team or organization likely have a common or shared understanding of the information in their own products that are similar to those to be derived from the P_{spec} but that organizational context is not shared among all potential users

Members of the team creating the P_{spec} (the government specification model developer) may think the model is complete. However, the users may interpret the P_{spec} in a variety of ways. The degree to which context and understanding differs between the model creators and model users will affect the interpretation. The way in which that understanding varies within an individual organization is another reason why teams handed the P_{spec} may interpret the spec in different ways. They may not even understand the P_{spec} if underlying assumptions vary between the creator and a specific user of the P_{spec}.

The specification must clearly address the criteria established under model assessment above. Without a clear understanding of how the model is to be used in the workflow from model specification and requirements (functional and non-functional) to design, implementation and integration, suppliers cannot create conformant products. Also, weapon system PMs who need a conformant solution will not understand how to express their needs to obtain, integrate, and use a supplier's solution.

Figure 1 represents the creation of the government specification model and its use across the ecosystem for the vehicle computing environment. In the figure (ModelingSME-PMO swimlane), the workflow begins with creation of a specification model template. This swimlane also includes an evaluation activity to assure that the models address the modeling use cases, and, during product development, that system product models satisfy product use cases, requirements, and design. A systems engineer (SystemsEngineer-PMO swimlane) uses the specification model to apply the range of computing environment features to establish the P_{spec} computing environment. The computing environment specification model is provided as part of an RFP and a contractor creates the $P_{proposed}$ to define how the supplier will create the computing environment (SystemsEngineer-Contractor Modeler swimlane). This capability is the P_{actual}. This computing environment design model is the basis for implementing and for integration into the PM's ground vehicle platform. It is used by the PM acquiring a conformant computing environment (SystemsEngineer-Contractor Developer swimlane) to apply the design model, implement the CPS for the computing environment, and integrate on the platform.

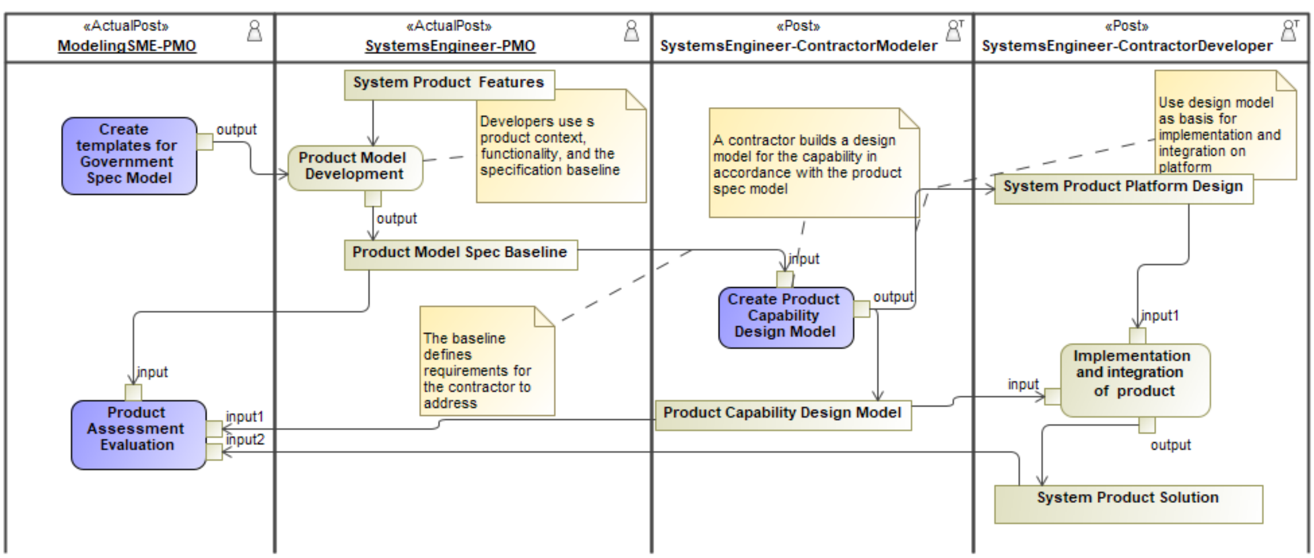

Figure 1. Flow of ecosystem exchanges from government specification model to Specific Product

Use Cases for the Model

Use cases for the model are directed at use of the model content not at use of the system product. These modeling use cases answer questions such as: If I use the model, what should I expect to derive from it? The answer may be another model, a system, a process, or other artifacts. This category of use cases differs from product system use cases that are concerned with the executable system, its users, and the result of performing that use case.

There are several situations in which the type of modeling captured in the specification model is useful.

UC1 – the PM wants to issue an RFP. Performing this use case builds a model (the P_{spec}) to provide an unambiguous way of communication between the PM and the potential vendors

UC2 – the PM wants to use the P_{spec} as a means of evaluating a model (the $P_{proposed}$). This use case establishes interactions among the ecosystem players who accept the government specification model, derive additional models, prototypes, tools, cost estimates, development team descriptions or other content that is submitted as part of the response to the RFP.

UC3 – the PM wants to evaluate a delivered product. Running the use case allows the acquirer to check conformance to the technical specification (P_{actual}) delivered by the vendor which includes functional and behavioral elements.

Table 3. Role of Model Depicted in Figure 1 and Derived Table 2

Expected content of a Specification Model	Example Model Content
1. Scope of system product	"Reconfigurable hardware resources" "CPS to deliver ground fighting vehicle maneuver capabilities"
2. Purpose and intent of the specification model	Provide acquisition requirements for a Supplier to develop a CPS computing environment for the ground-based fighting vehicle
3. Ecosystem of specification model users	Ground vehicle contractor, computing subsystem supplier, acquisition authority, qualification authority
4. Questions the specification model should answer	What are the requirements that must be satisfied by a supplier of CPS that satisfies the ground vehicle computing requirements? What are the design constraints that a conformant CPS must satisfy?
5. Diagrams needed to define specification	Template to guide modeling for specification baseline Block diagram of decomposition for acquisition item – systems and subsystems or components. Activity diagram showing interactions between user and system or between CPS and external systems

Expected content of a Specification Model	Example Model Content
6. Workflow	Acquirer provides specification of CPS in RFP Acquirer receives and reviews refined models from contractors proposing to build the CPS Contractor delivers models of the CPS during development for review by acquirer and qualification authority Contractor revises and refines models to implementation, integration, and deployment
7. Use cases for the models	Understand and validate ground vehicle computing requirements Produce the refined requirements Elaborate specification models to design Analyze model content for satisfaction of attribute constraints
8. Requirements for system product to be built and of models for the product	Examples: Block diagrams to establish original requirements and capture derived requirements and data abstractions, activity diagrams to show information and control flow across computing elements Model of non-functional requirements include safety and timing. Providing data needed to perform analyses to assess conformance to requirements

Exploratory Questions and Suggestions

After this initial analysis of the current P_{spec} for the computing environment, we have a few questions and some suggestions.

1. In the P_{spec} there is an implicit assumption that terms are either explicitly defined in the model or are considered widely understood. In a specification model, would it be helpful to state the minimum experience assumptions such as “entry-level system engineer or experienced system architect?”
2. A specification model may have numerous places where information is missing. There could be several reasons why. The model could be annotated with the reason why the information is not in the model. The information may not be available until later, or until some other piece of information is available. Annotating the model with the reason would help users of the model know how to react.
3. An attribute may be bound to a specific value or may be unbound. The model should clearly communicate if or when an unbound attribute will be bound.
4. The SysML language allows for multiple design hierarchies within a model. The node in the model where two or more hierarchies split off should be annotated.

Summary

Based on our study, we expect that the government specification model will provide information essential to the definition of resources that are configurable with respect to hardware and software. We would like to see additional information at both sides of the model to define the ecosystem around the model, use cases for the model, and the kinds of product solutions must be capable of addressing the contents of the specification model. Also, we expect to see in the RFP a thorough model review and examples to assure that requirements are specified and that design decisions or statements about the intended solutions are minimal.

The contractor models derive from the government models to capture design decisions in the areas of decomposed design elements (e.g., derived requirements) and interface elements for connections to/from the platform. The contractor models build on key data abstractions or data architecture in the specification model to define abstract data types, system messages, and communication protocols.

Legal Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM25-0207

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu
Email: info@sei.cmu.edu