Model Based Mission Assurance & Flight Worthiness Workshop

Outbrief of Content and Results

Norman Lao
Robert Stevens
Alexander Chang
Alec Gil

September 14th, 2021

Approved for public release. OTR-2021-00978.

Your Hosts

- MBMA/FW Workshop Co-Leads
  - *Robert Stevens, Director, Model Based Systems Engineering Office*
  - *Norman Lao, Director, Acq. Risk and Reliability Engineering Department*
- Session Recorder
  - *Alec Gil, Associate Member of Technical Staff, Space Architecture Department*
- Systems Engineering Forum Chair
  - *Alexander Chang, Senior Member of Technical Staff, Space Architecture Department*

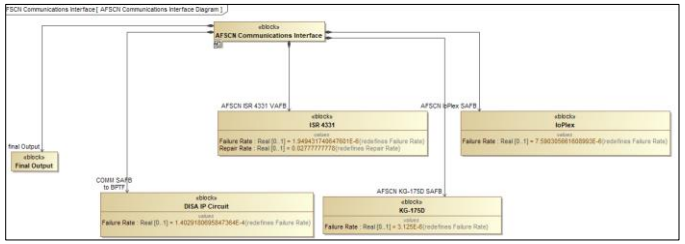
MBMA/FW Summary

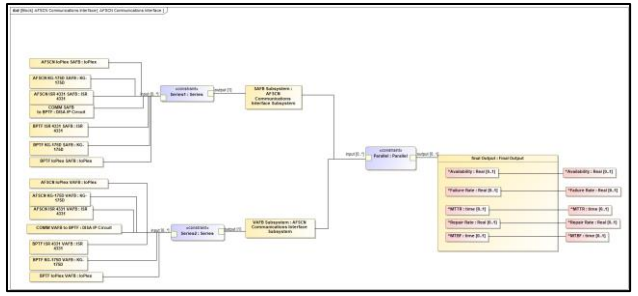
- The Systems Engineering Forum (SEF) hosted a virtual workshop for government and Aerospace members to discuss Model-Based Mission Assurance & Flight Worthiness on August 17, 2021
- Represented groups: NASA, SMC, AFMC, MDA, AFNWC, and Aerospace
- Workshop Format
  - *Presentations*
    - SysML Libraries and Profiles for Model Based Mission Assurance (Myron Hecht / Hetav Patel - Aerospace)
    - MBSE Support for Airworthiness (Keith Siders – AFMC)
    - MBMA in the context of NASA's Digital Transformation Program (Anthony DiVenti, Steven Cornford – NASA)
    - SMC and Space Flight Worthiness Criteria (Jay Landis – USSF)
  - *Discussion*
  - *Findings*

SysML Libraries and Profiles for Model Based Mission Assurance

Myron Hecht & Hetav Patel – The Aerospace Corporation

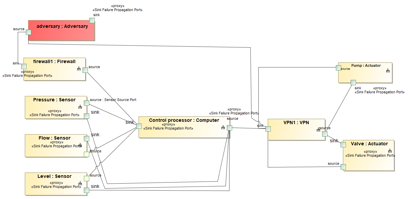
- Models for Mission Assurance
  - *Reliability and Availability*
  - *FMEA*



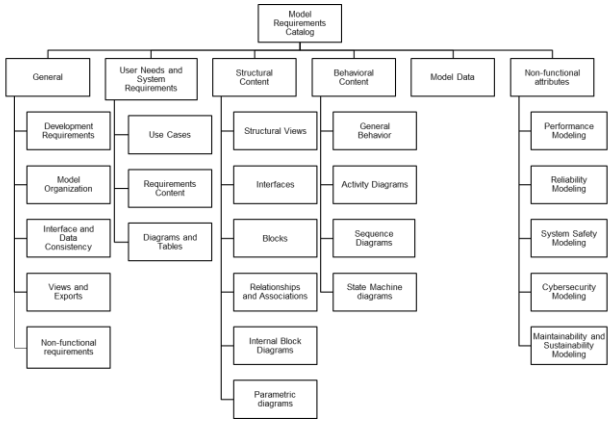


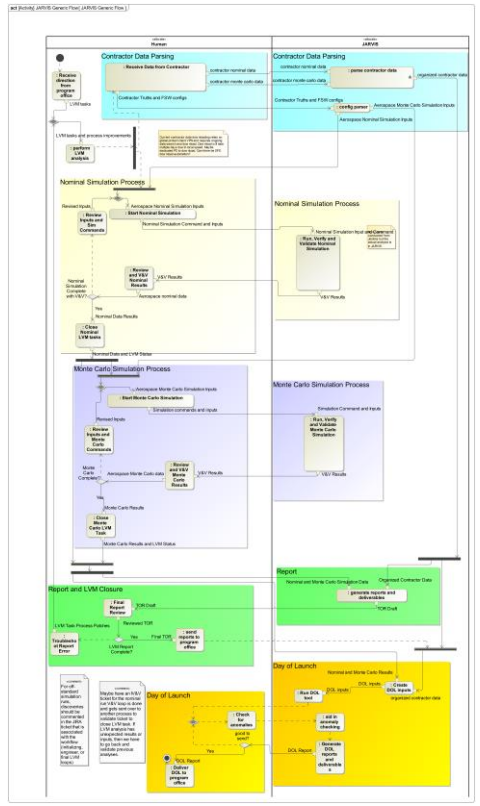
- Assuring the Digital Engineering Process
  - *Mission Assurance Activity Stereotypes*
  - *Risk Management Stereotypes*
  - *Modeling Mission Assurance Workflows*

3. Defining the propagation paths with a System Internal Block Diagram



- Assuring the Models
  - *Need for Model Verification and Validation*
  - *Manual and Automated Verification and Validation*





Model Based Mission Assurance is Essential for Digital Engineering

MBSE Support for Airworthiness

Keith Siders - AFLCMC/EZSI
AFLCMC… Providing the Warfighter's Edge

- ***General Approach to Certifications***
- ***Acquisition System Data Package (ASDP)***
- ***Airworthiness SysML Profile***
- ***SysML 2.0 – Things to Come***
- ***Future Vision***

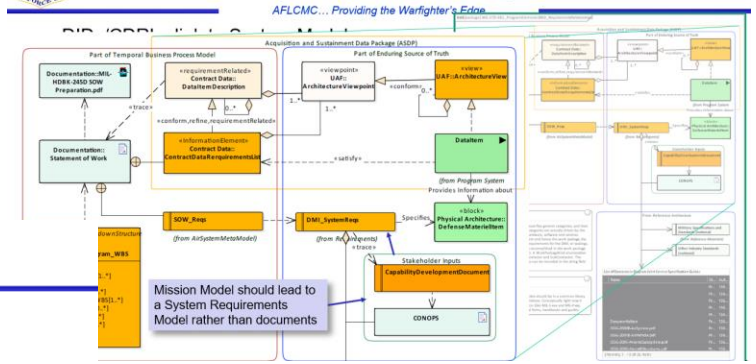
General approach to certifications

AFLCMC… Providing the Warfighter's Edge

- All certifications are for assessing ***risk***
  - Non-compliance does not automatically mean redesign, rebuild, retest, etc.
  - Only if risk of non-compliance is too great
  - Non-compliance can be waivered after assessment
- MIL-STD-461/464 EEE and TEMPEST
  - Test limits are generally:
    - constraints for emissions,
    - performance requirements for susceptibility
  - Tests are standardized, setup and procedure
- Cyber Security – NAVAIR RMF support in Cameo
  - NIST controls -> criteria(?) -> requirements
  - Note: Navy SET site is hard to get to over VPN
  - It can only be accessed from a .mil domain
  - Link is available upon request to .mil domain participants
- Airworthiness via MIL-HDBK-516C
  - Specifies attributes of the system to meet criteria
  - Consider NAVAIR cyber requirements derivation process
    - Can similar be applied to AW criteria?

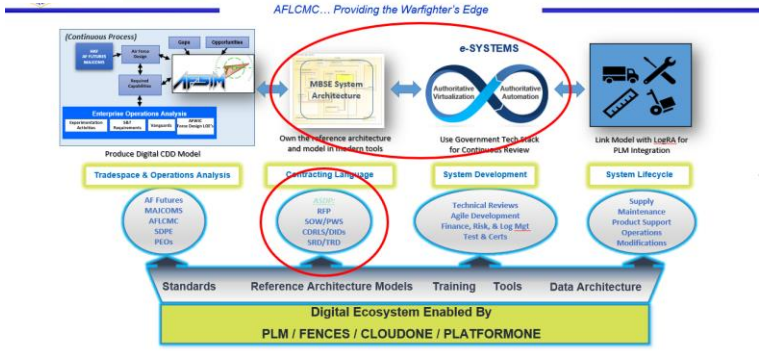
ASDP Ties Acquisition Model to System Model

AFLCMC… Providing the Warfighter's Edge



Digital Ecosystem – GRA in Action

AFLCMC… Providing the Warfighter's Edge

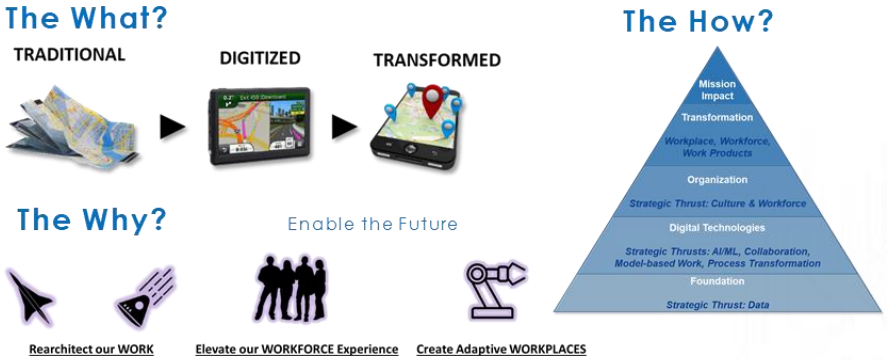


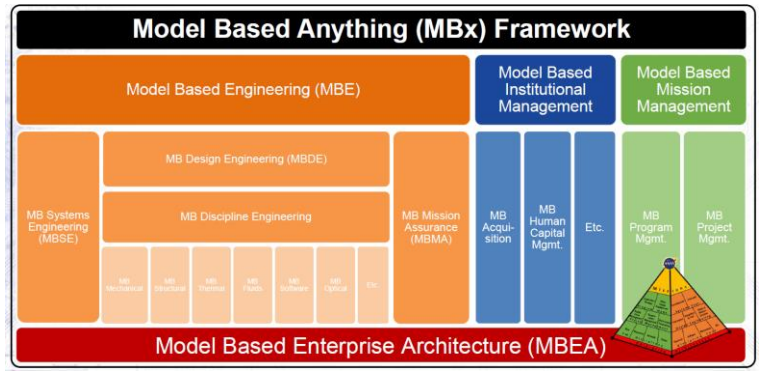
MBMA in the context of NASA's Digital Transformation

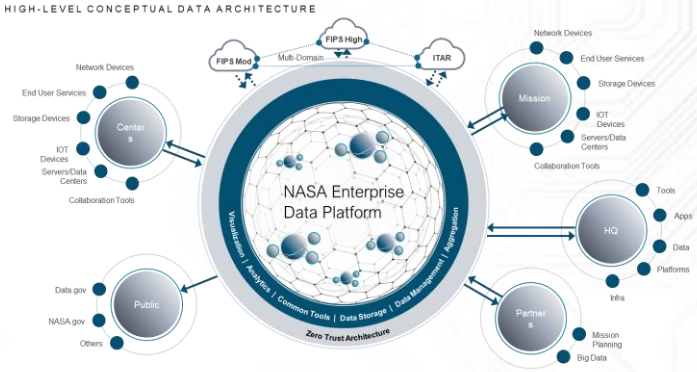
Anthony Diventi (NASA HQ) and Steven Cornford (NASA JPL)

Agenda:

1. NASA DT Program Overview
2. NASA Data Foundation – F.A.I.R./F.A.I.R.U.S.T
3. What is MBx and MBMA
4. Why MBMA







(Findable, Accessible, Interoperable, Reusable, Understandable, Secure, and Trustworthy)

Model-Based Mission Assurance (MBMA): SMA's complement to Model Based Systems Engineering, Model-Based Mission Management (MBMM), and Model-Based Institutional Management; is focused on digitally transforming delivery of fundamental SMA functions, such as

- Assuring Safety and Mission Success through oversite and insight in the acquisition, development and operation of NASA missions
- Providing for delivery of technical products and processes to qualitatively and quantitatively characterize risks for NASA missions covering the safety, reliability and quality of hardware, software, and human systems integration over the life cycle
- Supporting decision making in the acceptance of risks on NASA missions; though development and adoption of advanced mission assurance capabilities that continually enable more efficient, effective, and agile safety and mission assurance of NASA's mission as part of an integrated, model-based, enterprise environment.

SMC and Space Flight Worthiness Criteria

Mr. Jay A. Landis – SMC/ECEM

- SFWC governance provided in two documents:
  - *SMCG 1202, Space Flight Worthiness Criteria (SFWC), 7 October 2009.*
  - *Space Flight Worthiness Criteria (SFWC) Planning, Verification, and Certification Guide, Aerospace Report No. TOR-2012(1315)-5, 10 August 2012.*
- NSSL uses different, but equivalent, process to certify SFWC
- SFWC is a self-assessment by program offices with assistance from SMC/ECEM for certification to SMC/CC at Flight Readiness Review
- SFWC is a lifecycle process from acquisition through launch
- Digital Engineering already in use to satisfy aspects of SFWC

Operational Safety Criteria

Defined by SMC as: The condition of having acceptable risk to life, health, property, and environment caused by a system or end-item when employing that system or end-item in an operational environment. This requires the identification of hazards, assessment of risk, determination mitigating measures, and acceptance of residual risk.

Operational Suitability Criteria

Defined by SMC as: The degree to which a system or end-item can be placed satisfactorily in field use, with consideration given to availability, compatibility, transportability, interoperability, reliability, wartime use rates, maintainability, full-dimension protection, operational safety, human factors, architectural and infrastructure compliance, manpower supportability, logistics supportability, natural environmental effects and impacts, and documentation and training requirements. (Note: In SMC's application the system could be a satellite, launch vehicle, or critical ground system. In addition, consideration would include launch rates and operational software.)

Operational Effectiveness Criteria

Defined by SMC as: The overall degree of mission accomplishment of a system or end-item used by representative personnel in the environment planned or expected (e.g., natural, electronic, threat) for operational employment of the system or end-item considering organization, doctrine, tactics, information assurance, force protection, survivability, vulnerability, and threat (including countermeasures; initial nuclear weapons effects; and nuclear, biological, and chemical contamination threats).

Mission Certification

Defined by SMC as: the final certification process for all mission critical elements, including the launch vehicle and spacecraft, that ensures that the integrated system has been properly tested and processed so that the entire system will perform its required functions and is ready for launch.

SFWC = Space Flight Worthiness Criteria
NSSL = National Security Space Launch

Workshop Goals

1. *Define Model-Based Mission Assurance and Flight Worthiness (MBMA/FW)*
2. *Define what it means when we say that mission assurance and flight worthiness (MA/FW) are "model based"*
3. *Identify goals and benefits of MBMA/FW*
4. *Identify opportunities and barriers to incorporating model-based practices in MA/FW*
5. *Recommend pathfinders to those pursuing MBMA/FW*

Discussion

1. Define Model Based Mission Assurance/Flight Worthiness

- How do you define model-based mission assurance and flight worthiness (MA/FW)?
  - Disciplined view of **integrated** models
  - FW is a subset of MA, MA follows disciplined engineering principles. FW are task that need to have confidence of being flight worthy. AFMC is heavy design aspect.
  - Adding a **structured** aspect to definition in terms of process / approach. **Traceability**.
  - **NASA Standard 7009** for validating models
  - Produce understood and common products quickly, efficiently, and with the potential for automation.
- Is MBMA/FW a subset of MBSE?
  - *Subset of MBE*
  - *Consensus to be determined*
    - Some view MBMA and MBSE as related, but separate portions of MBE
    - Some view MBMA as a portion of MBSE
    - Highly dependent on how MBMA is defined
- Proposed Definition

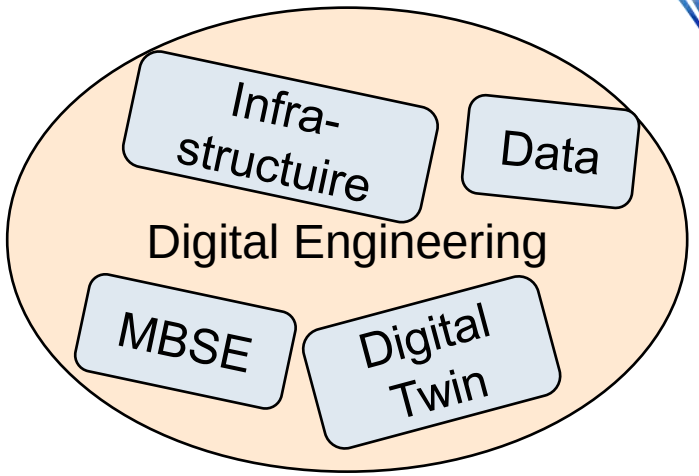
Disciplined integration of analytical and descriptive models to manage risk, quality, and safety throughout the system lifecycle

Discussion

2. Define what it means to say MBMA/FW is "model-based"

Primer questions

- *What is "model based"? … Examples?*
  - ***Connectivity and integration** of the model.*
  - *Connectivity can represent different things (e.g., level of connectivity, restricted views, etc.)*
  - *Connectivity doesn't have to mean to connect everything all the time.*
  - ***Mil Handbook 516c** for airworthiness. Various process for air vehicle definition and planning. **Safety critical functions** are those that if not done correctly will be catastrophic or critical failure. Can sometimes be related to MA/FW(AW).*
  - ***Configuration and data management**, understanding where the data is coming from. (Having **ASOT** for data and models.)*
  - ***[Counter Example]** SAPHIRE (reliability) program, did not connect to anything and lots of human interaction that it represents the opposite of model based.*



- *Do you use MA/FW guidelines, instructions, or reference documents? How would you "modelize" them?*
  - ***Yes, guidelines (etc.) are available***
  - *Example of "modelized" guideline = MIL Handbook 516c implementation in AFRL*

Discussion

3. Identify goals and benefits of MBMA/FW

Primer Question

- *What would be some benefits/goals of MA/FW being model based vs. document based?*
  - *Quality*
  - *Speed through automation*
  - *Earlier metrics to analyze along the way*
  - *Handling increased complexity*
  - *Enhanced Rigor*
  - *Explicitly incorporating Lessons Learned*
  - *Traceability*
  - *Gov. reference to compare with contractor products*
  - *Cost (may be indirect)*

Discussion

4. Identify opportunities/barriers to incorporating model-based practices in MA/FW

- *What are obstacles to implementing change to established processes?*
- *Any unique barriers for model-based practices?*
- *What are factors that could help incorporation of model-based practices?*

Barriers to Adoption	Potential Solutions
Connectivity & Integration *Ex. Physically disperse locations, Classifications, Intellectual Property*	Cloud Solutions (for dispersed locations) Security mechanisms for corporations to store IP on the same server (Intellectual Property)
Investment cost given the unknown Return on Investment (ROI)	Using Internal Research & Development / Corporate funding to develop core capabilities and reference models. Develop metrics to measure success (to address ROI).
How to overcome **cultural inertia**?	**(Bottom-Up)** Promoting MBSE as a System Engineering service. *Ex. Have the model generate commonly understood artifacts such as Reliability* **(Top-Down)** Grab leadership support early on. *Ex. Government owning the technical baseline.* **Provide Training and Awareness:** Defense Acquisition University (DAU), Leadership Videos, Forums & Events, easy to use web-based guides
Perceived Risk: longer time in design phase yields higher risk of being cancelled.	Informing decision makers on the positive implications of a robust design phase as related to I&T so that the critical path is not impacted. *Ex. May be able to reduce I&T schedule, minimize prep time for milestone reviews.*
Difficulty sharing models across the whole span of stakeholders easily (model in a vacuum). MA requires interaction beyond modelers and System Engineers	Strategically understanding users and developers' accessibility needs. *Ex. NASA's FAIRUST Approach (Findable, Accessible, Interoperable, Reusable, Understandable, Secure, Trustworthy)*
Lack of Government Reference Models (Descriptive)	Develop Reference Architecture Models
Lack of Standards	Develop model, data, and architecture standards needed for automation. Metrics for success or fidelity.

Discussion

5. Recommend collaborations/pathfinders to those pursuing MBMA/FW

Primer questions

- *What can we learn from current pathfinders?*

Government's focus should be predominantly in the area of MBSE using SysML models	Government needs an efficient and automated mechanism for relating MBE to MBSE (ie. Run a high-fidelity physics simulation and have the results update a SysML model)
Develop a data architecture for your system or domain	Develop a reference architecture (SysML model) for your system or domain
Establish what data the government needs to own	Train your people on the tools ASAP
Pick a set of digital tools (SysML, PLM, Analytics)	Integrate the tools
Need to establish a framework for how the model and tools interact (e.g. SysML plugins)	Before you attempt using MBSE on complicated air and flight worthiness processes, you should establish a data architecture and SysML model of your system.
Establish a collaborative environment via Cloud (on/off prem)	

- *Guidelines or Style Guides for the Community:*
  - *MIL-HDBK-516c*
  - *Draft SMC (SSC) MBSE Style Guide*
  - *NASA-STD-7009a Change1*

Findings

1. Define Model-Based Mission Assurance and Flight Worthiness
   - *Disciplined integration and connectivity of models to manage and trace risk, quality, and safety throughout the system lifecycle.*
   - *A discipline of MBE, but different from MBSE*
2. Define what it means when we say that MA/FW are “model based”
   - *The products people want are sourced from models that are configuration managed and credible.*
   - *The products people want are made faster, better, more consistently.*
3. Identify goals and benefits of MBMA/FW
   - *Quality, Speed through automation, Greater trade exploration (by product of speed), Identify early metrics, Handling increased complexity, Enhanced rigor, Explicit Incorporation of Lessons Learned, Traceability, Framework for a Gov’t Reference (e.g. GRA), Reduced recurring cost*
4. Identify opportunities and barriers to incorporating model-based practices in MA/FW
   - *Barriers (as opportunities): Cultural Inertia, Accessible guidelines(books) / trainings, Funding for proving concepts, Model accessibility between stakeholders, Connectivity between enclaves (classification, proprietary, KTR/Gov, tool enclaves, etc.)*
5. Recommend potential collaborations/pathfinders to those pursuing MBMA/FW
   - *Pathfinders and prototypes have been confirmed among all groups*
   - *NASA sees collaboration opportunities creating an SMAP (Safety & Mission Assurance Plan) auto-generation capability*
   - *AFMC has developed a model-based certification process that may be leveraged by others and refining USG-industry MA roles*
   - *Future collaboration to incorporate contractors / industry*

Questions?

Backup

What is a Model Anyways?

Analytical and Descriptive Models – Paraphrased from SEBoK

- **Analytical models** provide quantitative answers to questions regarding performance or other nonfunctional requirements
  - *CAD model, thermal model, structural model, energy balance model, reliability model, etc.*
- **Descriptive models** describe what the system is or does
  - *System **structure** (composition, interconnection, and interfaces)*
  - *System **behavior** (functions and functional flow, control logic)*
  - *System **requirements** and their traceability relationships*
  - *System **parametric** relationships and constraints*
  - *For example, DODAF architecture descriptions are based on descriptive models*
- In the absence of formalized descriptive models, systems engineers rely on their own ***mental models*** to make sense of the system
  - *Everyone's mental model is different, incomplete, and inconsistent*

Traditional SE uses lots of analytical models but relies too heavily on static documents for system description

Definitions

National Security Space

- **Mission Assurance:** The disciplined application of proven scientific, engineering, quality, and program management principles toward the goal of achieving mission success[1]
- **Mission Success:** The achievement by an acquired system (or system of systems) to singularly or in combination meet not only specified performance requirements but also the expectations of the users and operators in terms of safety, operability, suitability and supportability[2]

1 2009 Mission Assurance Summit Strategic Intent.
2 Mission Assurance Guide, TOR-2007(8546)-6018, Rev B. Note: in contrast, acquisition success can be defined in terms of performance, cost, and schedule

Analytical, Descriptive, System Models

Systems Engineering Body of Knowledge (SEBoK)

- *Analytical Model:*
  - *An **analytical model** describes mathematical relationships, such as differential equations that support quantifiable analysis about the system parameters. Analytical models can be further classified into dynamic and static models. Dynamic models describe the time-varying state of a system, whereas static models perform computations that do not represent the time-varying state of a system. A dynamic model may represent the performance of a system, such as the aircraft position, velocity, acceleration, and fuel consumption over time. A static model may represent the mass properties estimate or reliability prediction of a system or component.*
- *Descriptive Model:*
  - *A **descriptive model** describes logical relationships, such as the system's whole-part relationship that defines its parts tree, the interconnection between its parts, the functions that its components perform, or the test cases that are used to verify the system requirements. Typical descriptive models may include those that describe the functional or physical architecture of a system, or the three-dimensional geometric representation of a system.*
- *System Model:*
  - ***System models** can be hybrid models that are both descriptive and analytical. They often span several modeling domains that must be integrated to ensure a consistent and cohesive system representation. As such, the system model must provide both general-purpose system constructs and domain-specific constructs that are shared across modeling domains. A system model may comprise multiple views to support planning, requirements, design, analysis, and verification.*