Model Based System Engineering (MBSE) Applied to Program Oversight and Complex System of Systems Analysis

10-30-2014

Agenda

- Introduction
  - MBSE, UML & SysML – mature approach with broad base of practitioners
- MBSE & the Acquisition Lifecycle
  - Better Buying Power, transparency and MBSE
  - Management / Engineering use of MBSE data for program evaluation
  - Program data organization for cost / schedule / performance risk mitigation
- Program Model & Cyber Risk Example
  - Leverage MBSE's structure to describe emerging program risk
- Wrap Up

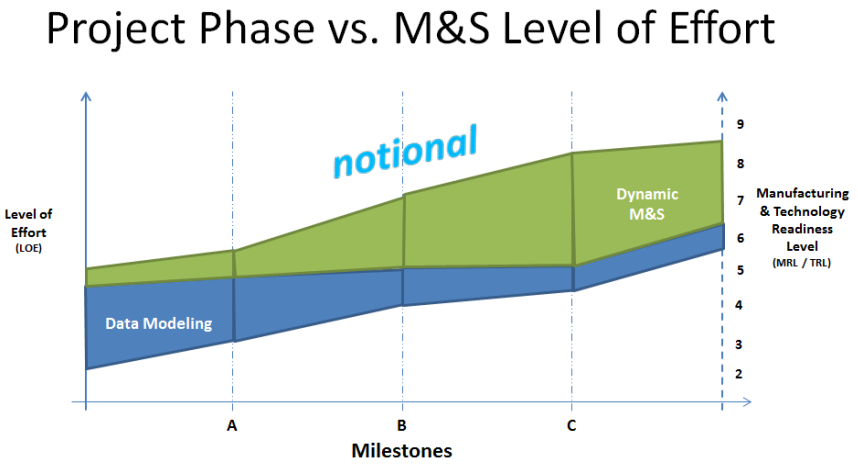
Introduction

- MBSE is able to describe physical processes, along with their attributes, for evaluating acquisition program cost / schedule / performance (CSP)
- MBSE builds on successful techniques from the software engineering community for structuring systems data
- MBSE provides a method to organize data to function / purpose over a program's lifecycle
- Modeling and Simulation (M&S) leverage MBSE data to provide analytical insight on system behavior across an acquisition's lifecycle

DoD's Acquisition Approach – Data Challenged

Acquisition management characterized by – *Ad hoc program data pulls, simple cost / schedule / performance (CSP) stoplights, document centric data, incomplete data for analysis, lack of digital data, data incompatibility with complex tools for assessing performance* (GAO, 2013).

- DoD program assessment, via cost and schedule (CS) propagates up / across programs
  - Cost and schedule are enumerated from reported data
  - Earned Value Management (EVM) widely accepted for tracking cost as a function of work performed
- Data scalability an issue, especially for Performance(P) data
  - Meetings currently the key method for hierarchically communicating data
  - Abstraction is a challenge in packaging engineering performance data for management inspection
  - New Technologies (e.g., Cyber Risks) add additional complexity to program development
- The use of MBSE is still with the technology folks (e.g., DISA's JIE architects)
  - costs of conducting MBSE not well understood
  - overlap with architecture approaches (e.g., DoDAF) being determined

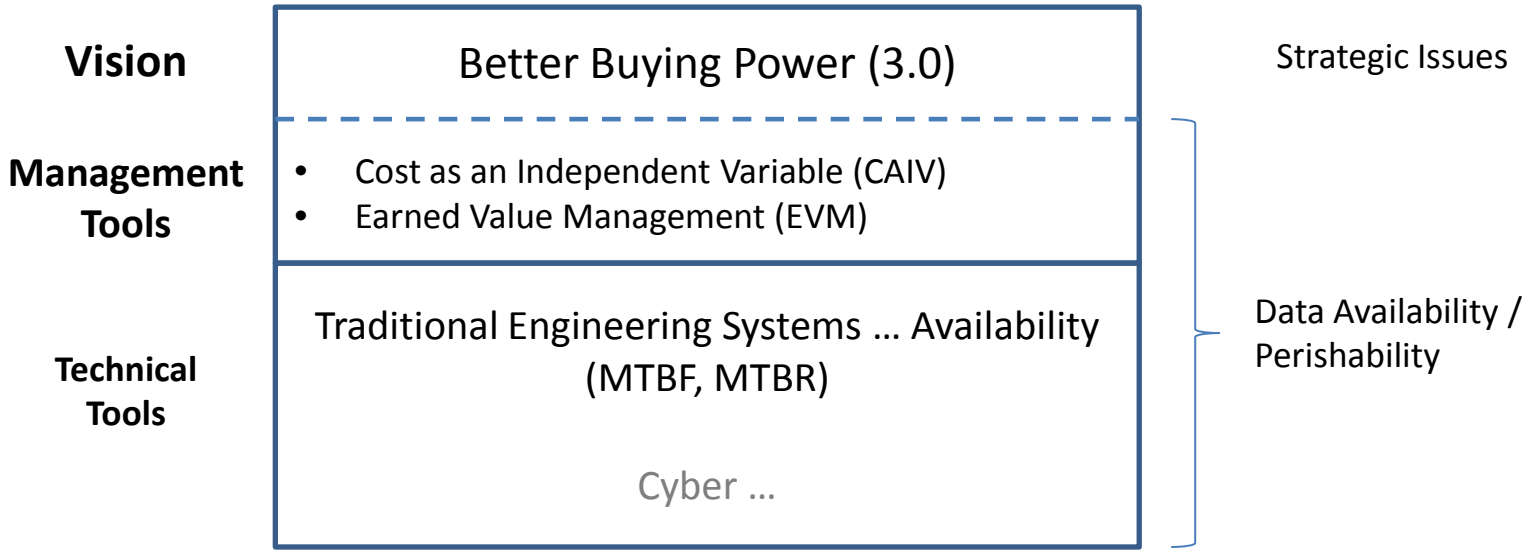


- Data modeling has higher level of effort (LOE) up front, as project comes together
- Systems model results in project data being available throughout the system's lifecycle

MBSE provides taxonomy to organize program acquisition management data

Enterprise Acquisition

(Architecture of System Tools)

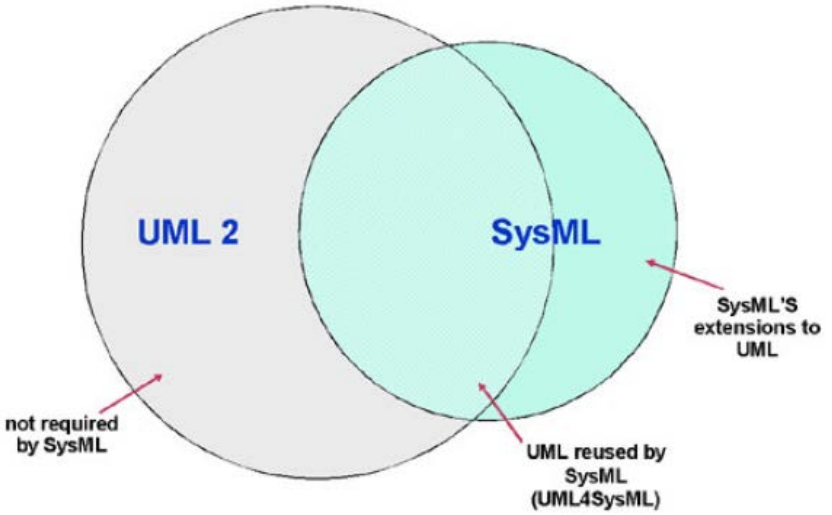


- "Better Buying Power" adds rigor to acquisition (e.g., developing Acquisition Body of Knowledge (BOK))
- Data availability an ongoing issue for standard approaches (e.g., CAIV, EVM, Availability)
- Emerging issues (e.g., cyber …) add additional risk to the acquisition process

MBSE can reduce program acquisition risk for each level of decision maker

Model Based Systems Engineering
(UML 2 & SysML)

- MBSE
  - derives from the software development community - Object Management Group ’s (OMG) Universal Modeling Language (UML) specialization for hardware is called the systems modeling language, SysML
  - provides a structure to define, characterize, and use the data required for DoD program decision making (CSP), in a systematic and repeatable manner (data to decision)
  - determines essential elements of data to support an assessment or decision (i.e., Top down not bottom up)
  - supports organizing data to describe activity threads
    - workflows of interest - performance / risk / cost
    - assessments / decisions with appropriate fidelity / accuracy at each level
  - Applicable to testing, VV&A, program oversight and assessment



- SysML (OMG Standard) heavily leverages UML 2 (software engineering standard)
- SysML’s goal is to provide a standardized language for system engineering

MBSE shows promise for DoD programs oversight / decision-making

MBSE – Top Down Approach

(System Entity Structure)

The System Entity Structure (SES) is designed as a labeled tree with attached variable types that satisfy the following axioms:

uniformity: Any two nodes which have the same labels have identical attached variable types and isomorphic subtrees

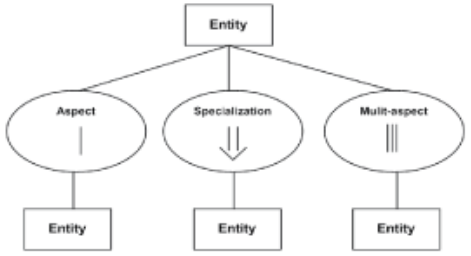
strict hierarchy: No label appears more than once down any path of the tree

alternating mode: Each node has a mode which is either entity, aspect, or specialization

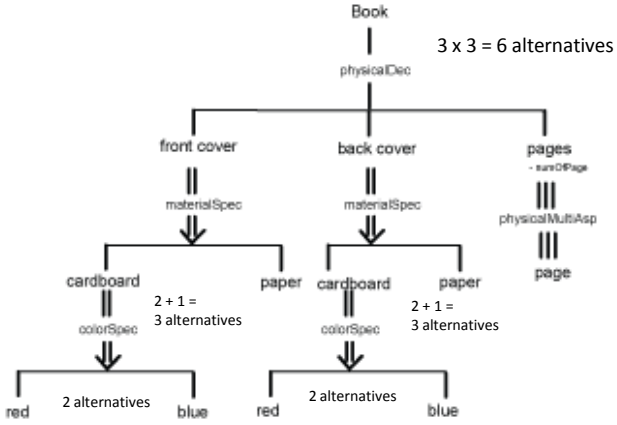
- the mode of the root is entity
- if the mode of a node is entity then the modes of its successors are aspect or specialization
- if the mode of a node is aspect or specialization, then the modes of its children are entity

attached variables: No two variable types attached to the same item have the same name

inheritance: every entity in a specialization inherits all the variables, aspects and specializations from the parent of the specialization



SES & Labeled Tree Components



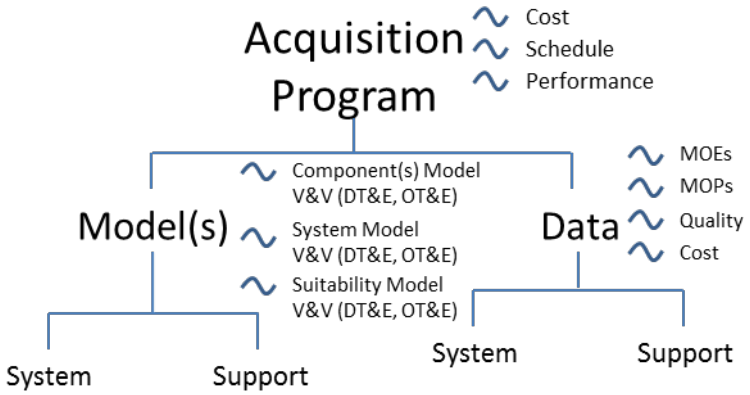
SES & Book Example

No. Alternatives ~ $x_i\ n_{si}$

MBSE & Evaluation Roll Up Methods

MBSE is an industry standard methodology currently used for developing systems (e.g., the DoD's JIE)

- leverages well-known academic approaches for packaging data (e.g., semantic networks …)
- provides a consistent design / storage approach for later recall by evaluation functions

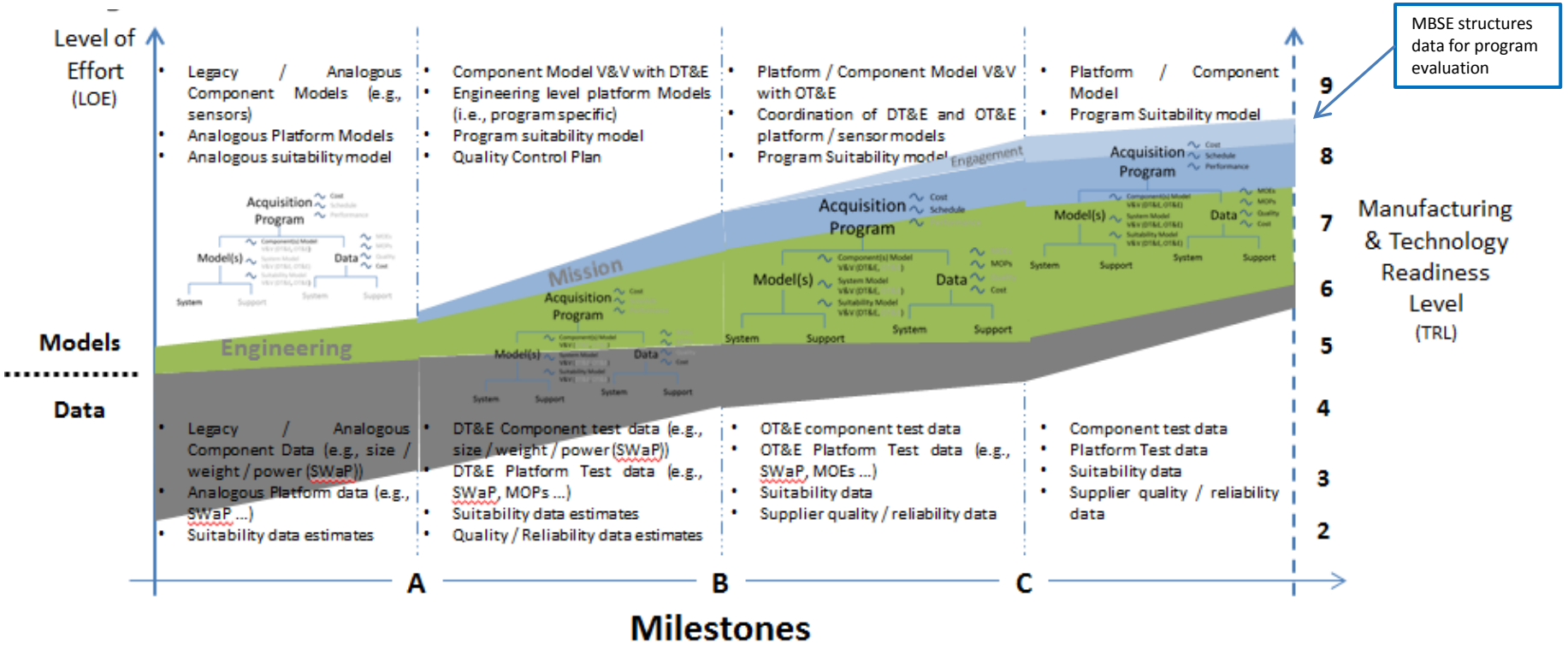


Enterprise Graph consists of models and data descriptions

- Tree Structure example is currently an "AND" graph
  - Acquisition Program = Model(s) AND Data
- Each entity has its own attributes (i.e.,
  - designated with " ~ " – e.g., Cost / Schedule / Performance

MBSE's structured approach provides data at each level of system decomposition

MBSE & the Acquisition Lifecycle

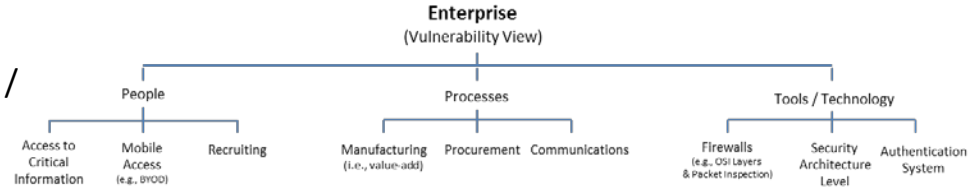


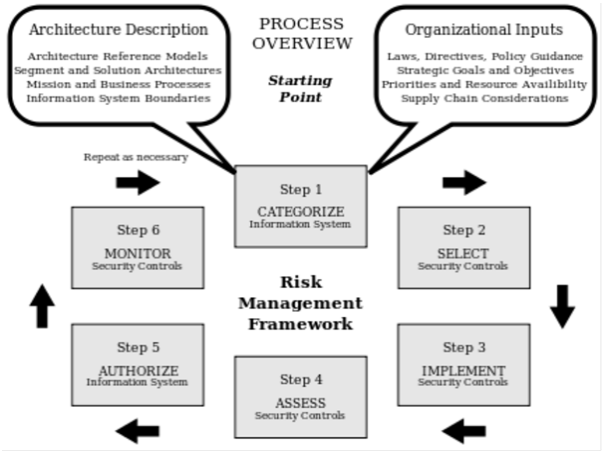
- Model resolution changes over the various phases of a system's acquisition life cycle

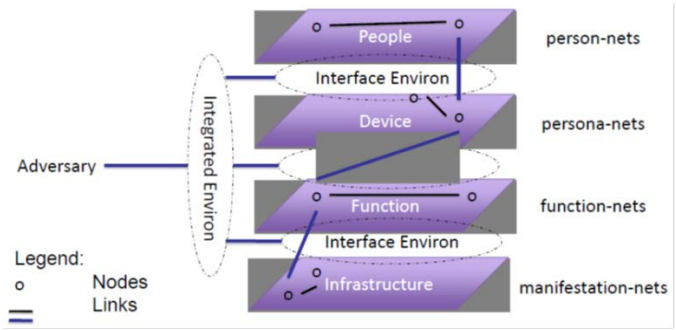
- MBSE provides a method for decreasing (C,S,P) risk across the project lifecycle

Program Model & Cyber Threat Description

- Currently, it's a challenge to represent any platform / sensor / system's attack surfaces
- Multiple "planes" used to visualize the threat terrain's attack surfaces
- Processes are the conventional human / machine based approach for decomposing the issue
- People, processes and tools that compose the enterprise, via surveys and interviews, are the data used to develop the system's entity-relationship model, called a System Entity Structure (SES)







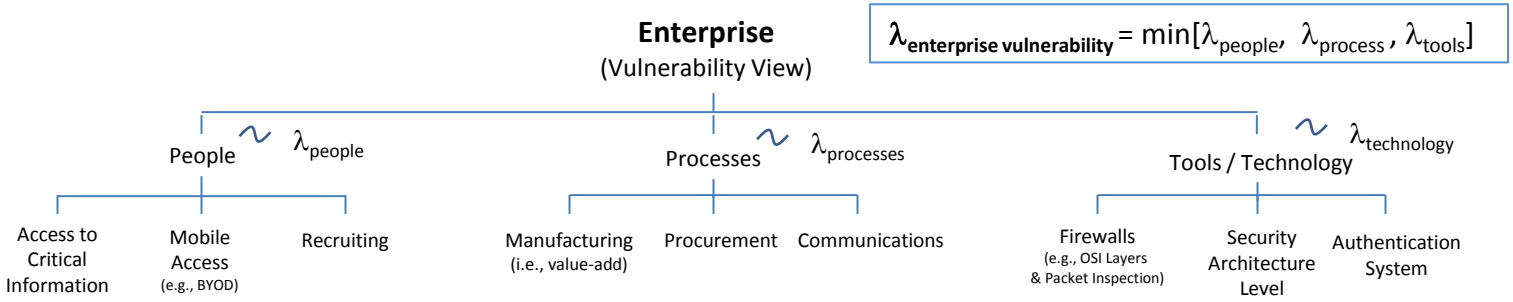
[1] http://www.itl.nist.gov/div898/handbook/apr/section1/apr161.htm

Program Model & Parameterization

(organize respective failure rate estimates)

Enterprise "As Is" Graph Description to organize disparate People / Processes / Tools descriptions

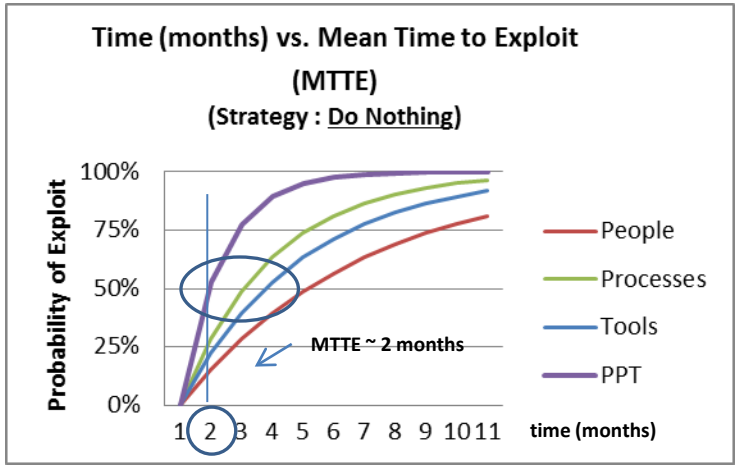
- Tree Structure example is currently an "AND" graph, where each of the decomposed entities has its own failure rate, that is used to contribute to the overall failure rate for each key node of the Enterprise (e.g., people, processes and tools)
- Decompositions can also include "OR" specialization nodes, where alternative people, process or technology implementations are available
- Graph Structure is formally called a System Entity Structure (Zeigler, 1984); used to describe an enterprise for evaluation (Couretas, 1998)



$\lambda_{people} = \lambda_{crit\ info\ access}$ AND $\lambda_{mobile\ access}$ AND $\lambda_{recruiting}$

- λ is the failure rate for the respective domain (e.g., people, process, tool) or one of its components
- Exponential distribution results in "additive" combination of failure rates over the heterogeneous data for the respective domains

“As Is” Risk Estimation

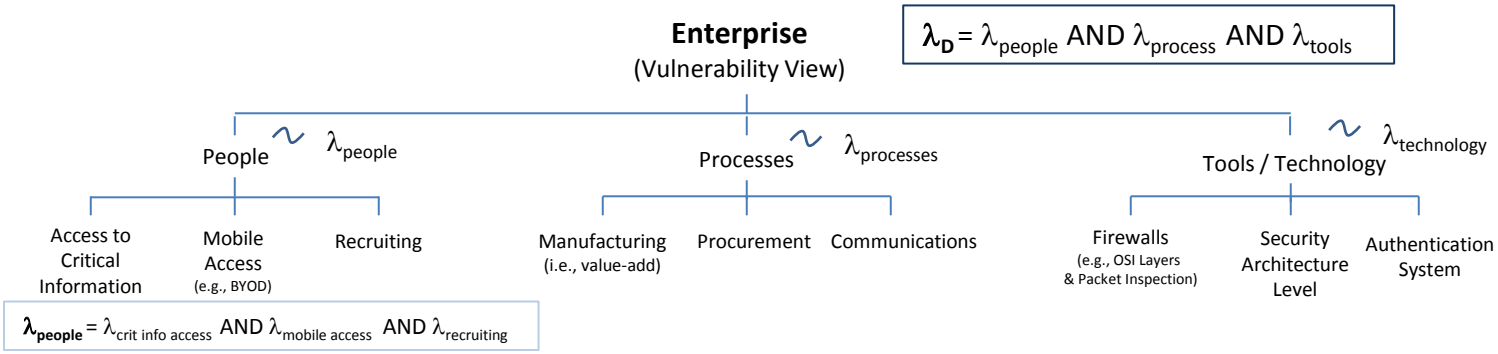


$MTTE \sim 1 - e^{-\lambda_{vulnerability} * t}$

- 50% is critical marker
- Example Enterprise currently has a 2 month Mean Time to Exploit (MTTE)

Exponential Distribution provides a rough approximation to Enterprise security failure. Advantages include -

- Get the conversation started about enterprise security structure (i.e., System Entity Structure (SES) of Enterprise)
- Initial cut at Enterprise risk model (i.e., more accurate approaches available as data quality increases)

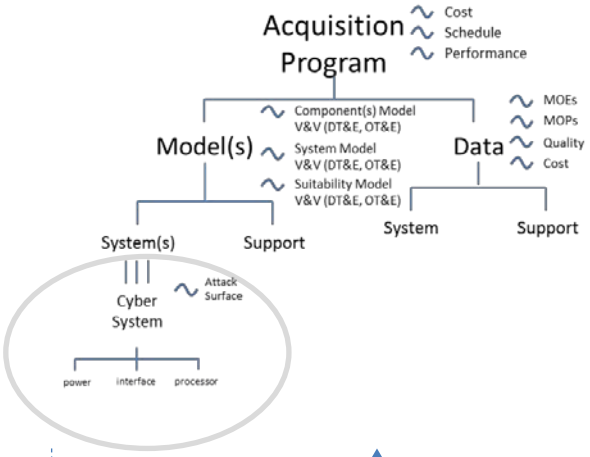


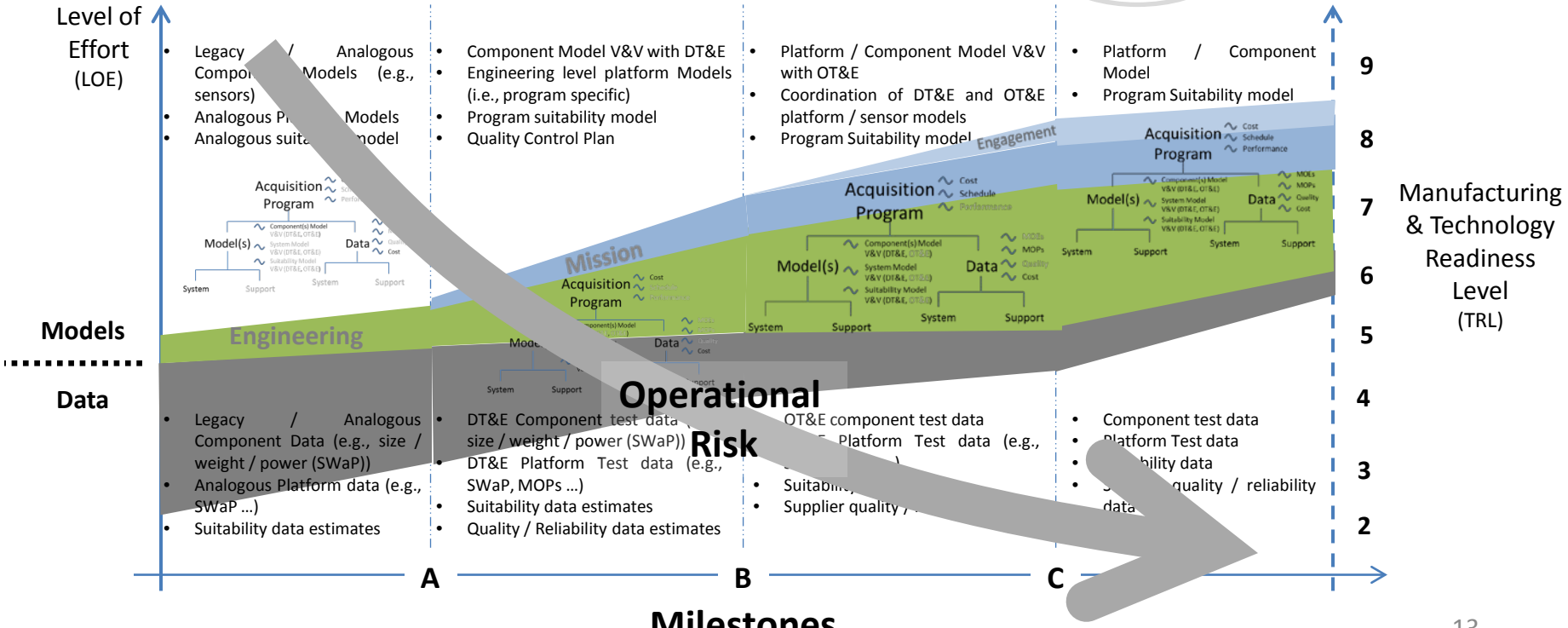
Mean Time to Exploit (MTTE) is an overall estimate of an Enterprise’s Cyber Security Risk

Program Data & Risk Description via MBSE

(Cyber & the Acquisition Lifecycle)

- Operational Risk decreased by building out the program's taxonomic description across during the progression of the acquisition
- MBSE structure extensible to account for cyber issues
  - System models serve as "attack surface" descriptions





Wrap Up

- MBSE leads to long-term traceability, via data, that minimizes current and emerging program acquisition risk
- MBSE derives from the software development community – the Object Management Group ’s (OMG) Universal Modeling Language (UML) specialization for hardware
- MBSE provides a taxonomy able to organize program acquisition management data
- MBSE’s systems level description provides extensible framework for the description of current and emerging technologies and their threats

MBSE shows promise for DoD program oversight / decision-making