Model Based System Safety
and
Emerging Systems of Systems

A presentation to the Tennessee Valley Chapter of the System Safety Society, and local System Engineering and Software Engineering Guests

October 21, 2015

Barry Hendrix

Principal Software Safety Engineer

APT Research, Inc.

Model Based System Safety and Emerging Systems of Systems

Systems of Systems (SOS) in DoD are information intensive with complex software functionality and highly integrated systems for interoperability and optimization to enhance performance in future battlefield scenarios.

Employing Effective System Safety for any SOS can be a challenge in the current “emerging” System Engineering and Software Engineering environment.

Systems of Systems and System Safety (30K ft. View)

- Times and technology are changing and so must system safety and other engineering domains.
  - Tri-Service F-35 JSF (Lightning) II is the most expensive and most complex software intensive safety-critical system in development.
    - The F-35 ($390B Projected for ~2500 aircraft) has plowed the way for many MBSE and software safety processes, it addition to other emerging Protection Technologies (Cyber Security, Software Security, IA, Anti-tamper)
  - **F-35 and others have an Umbrella "Technical Integrity" domain to ensure Chief Engineers are responsible for** all aspects of System Engineering, System Safety, Human Systems Integration, R&M, Security, Functionality, performance.

System Safety…What next?

- System Safety in past 50 years has evolved with technology from old federated systems to integrated systems to sensor fused systems, and from basic hazard analyses of hardware to highly complex software intensive systems-of-systems with various degrees of autonomy that command, control and monitor many safety-critical functions:

  - 1967: Hazard-based > Risk-based > + 1980s Requirements-based > + 1990s Functional-based> + 2000s LOR Criteria-based > + now and Future more emphasis on Model-based…..

Evolving/Emerging SOS are just now learning how to implement MBSE, MBSS, and Technical Integrity

- C4ISR and more are Tri-Services coordinating for the current and future battlefield
  - USN/USMC centric Cooperative Engagement Capability has been in place for some time.
  - NAVSEA and NAVAIR and Carrier Task Force SOS are in place and work well. Future F-35 and UCLASS will be more complex.
  - USAF has manned bombers, tactical fighters, UAVs and SOS are working, but still evolving. Long Range Bomber on the horizon…selection soon
  - MDA has mature SOS – C2BMC, more.
  - US Army Integrated Battlefield Command System (IBCS) plug and play, any weapon, anytime will be matured in years to come Patriot, PAC 3, more to come.
  - IFPC- Inc 2 Multi Mission Launcher (MML) currently under development using more non-traditional Agile software and Model Based System Engineering.

Command and Control System Safety

- C2 (Command and Control) – software intensive safety-critical functions and safeguards are designed to prevent top level catastrophic events such as Fratricide, Inadvertent Launch…more
  - Some Typical S-C Messages are:
    - Safe Commands
    - Engagement Termination Command
    - Cease Radiate Command
    - State Mode Command
    - Launcher Control Command
    - Missile Launch Command
    - Many functions are safety-critical, much more are mission critical (don’t confuse)

Systems of Systems and System Safety

- Traditional system safety may not be adequate for emerging and evolving SOS and paradigm shifts…different “Mental Models” needed to adapt
  - Multiple Contactors/Agencies, National Teams – Meshing Cultures/Methods
  - Highly Integrated, Sensor Fused, High Complexity
  - Proliferation of UAVs/AUS and autonomous systems, even driverless cars…are they robots??
  - Software Intensive with many Complex Interactions require new software safety methods
  - Model Based System Engineering (MBSE) is becoming the Norm on C2 and other emerging Information Centric SOS
  - Agile software development and less formal methods and must be geared to include software safety more so than in past when used in rapid prototyping
  - Total Risk Determination and Summation will require more effort
  - Safety Cases may be needed to collect all aspects and objective safety evidence

Systems of Systems and System Safety

- Model Based Systems Engineering (MBSE) requires a different system safety concept, application and effort because of :
  - Less traditional artifacts centric, less English Prose, More Graphical/Visual Notations
  - Can show Functional and Physical Architecture, integration and Interface
  - UML and SysML languages, System Architecturally Based, Model Must be Validated
  - More models (Functions, Use Cases, Structural Diagrams, Activity Diagrams, Sequence Diagrams, Executable States Charts, Architectural System, Functional Behavioral Verification, Complete Requirements Traceability, Handoff to Defined Systems
  - Autocode Generation, Greater Level of Abstractions, Traditional CM must change with model
  - Extracting Objective Evidence Needed for a Safety Cases

Some Popular Models

- **IBM Rational Rhapsody**, a modeling environment based on UML, Rhapsody is a visual development environment for systems engineers and software developers creating real-time or embedded systems and software.
- Rational Rhapsody uses graphical models to generate software applications in various languages including C, C++, Ada, Java and C#.
- Rational Rhapsody helps diverse teams collaborate to understand and elaborate requirements, abstract complexity visually using industry standard languages (UML, SysML, AUTOSAR, DoDAF, MODAF, UPDM), validate functionality early in development, and automate delivery of high quality products. Large complex programs (F-35 uses Rhapsody)

Module Base System Engineering (MBSE)

- Advantages over paper and artifacts centric engineering documentation
    - Creates one standard model for visualization
    - Greatly reduces interpretation of English prose and narrative requirements
    - Everyone is in same ballpark, in same songbook and on the same page
    - Same concept as “a picture (graph or functional diagram) is worth a thousand words”

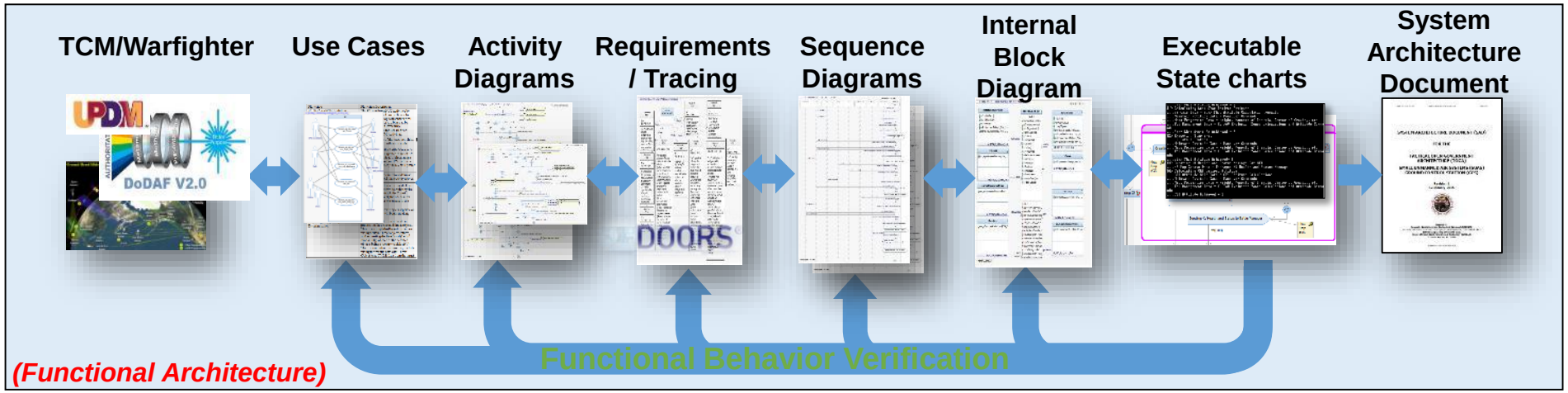
MBSE Can Help Refine the Granularity

- Example: Requirement Ambiguity and Correct Interpretation in English prose. “Thou shalt “Secure that Building”…
  - USAF interprets… **take out a lease on it**
  - USN interprets… **put a lock on it**
  - USA interprets…….**surround it**
  - **USMC …kicks in the door, rushes inside, clears it**

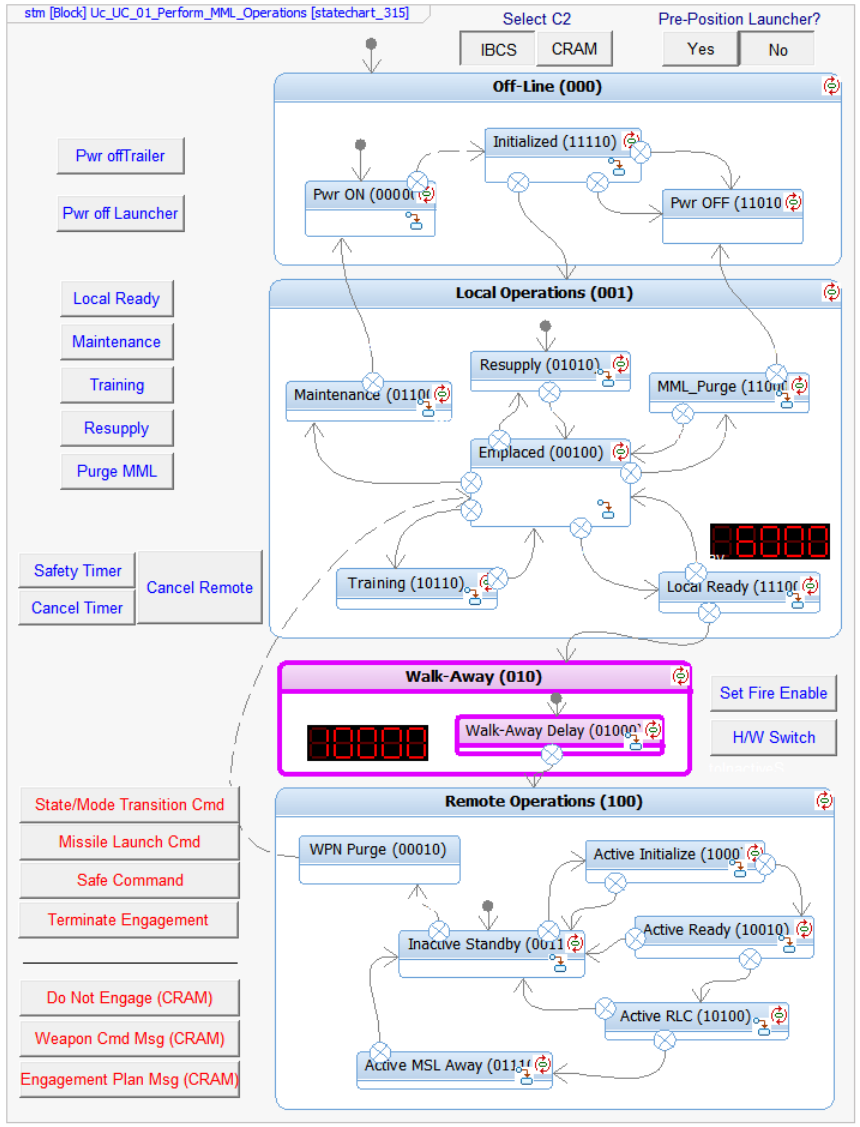
MBSE Output Useful for a Safety Case

Example of MBSE in place today by SED CoMBAT Team Process

Behavioral Allocations can then be handed off to Software Developers



MBSE – Typical Executable State Behavioral Diagram



Systems of Systems and System Safety

- Methods are evolving, but level of abstraction requires system safety to ensure objective safety evidence is obtainable from the Model
  - Ensuring software safety analysis of each Use Case for Safety-critical Functional; behavior – labor intensive as inputs to DOORs
  - Ensuring safety-significant attributes are flagged, tagged throughout model means software safety must keep up with evolving model at every stage
  - Use Cases, S-C Functionality, S-C requirements Assessment, safety test case allocation, safety verification and yielding OBJECTIVE SAFETY EVIDENCE (and Hazard Closure Evidence).
  - LOR (design assurance to give confidence) may be a mute point in some cases from a safety perspective, but more Special Safety Tests will be required:
    - Off Nominal Tests (ONT), Failure Modes Effects Tests (FMETs), Failure Immunity Tests (FITs) to refute safety arguments to validate Safety Cases.
  - Safety Cases with Refuted Arguments will be required as current SARs are inadequate as current written for Model Based System Safety

SOS with MBSE Needs Special Safety Tasks

- LOR (still required separately) is simply software design assurance, design assurance levels (DALs) and may in some cases be a “mute point” with MBSE (rigor built in model), but Special Safety Tests will be required beyond LOR:
  - Fault Trees are Often inadequate
    - Modern Models need to show Faults manifest to Errors and under what conditions cause Failures
  - Nominal (non-failure) must be modeled to Off Nominal Tests (ONT) ,
  - Failure Modes Effects Tests (FMETs),
  - Failure Immunity Tests (FITs) to refute safety arguments to validate Safety Cases.
- Safety Cases with Refuted Arguments as evidence of claims will be required for MBSE Programs
  - Current SARs are inadequate and fall far short of convincing evidence as current written
  - Objective Evidence can be extracted for Model Based System Safety
    - No need for expensive formal methods unless unique special cases to ensure safety
  - Contractors and Agencies must have a Cultural Change and an UNDERSTANDING of the need to Acceptance and Embrace Better Methods

Safety Cases and Refuting Argument

- Safety Cases with Refuted Arguments as proof/evidence of safety claims will be required for MBSE Programs, otherwise a level of uncertainty due to level of abstraction.
  - Current SARs are inadequate as currently written
  - Objective Evidence can be extracted for Model Based System Safety if properly planned and implemented
    - No need for expensive formal methods unless unique special cases to ensure safety
  - Contractors and Agencies must have a Cultural Change and an UNDERSTANDING of the need to Acceptance and Embrace Better Methods

Highly Complex Safety-Critical Systems Require More

- CASE EXAMPLE: F-35B JSF Lightning II Vehicle Management Computers (Triple Identical Systems) OFP for Flight Controls, Propulsion, Utilities and Subsystems required:
- Standard MIL-STD-882 System Safety and IEEE STD 1228 Software Safety PLUS…
  - Safety/Software Evidence Assurance Levels (SEAL)
  - Highly Integrated Sensor Fusion
  - Elaborate MBSE with Validated Model
  - Formal Methods
  - Mathematical Proofs
  - Goal Structuring Notation (GSN) a 5 year Outstanding Yield Effort
  - Safety Case Structure with Refuting Arguments

THE SAFETY EFFORT HAS PAID OFF – NO AIRCRAFT LOSSES SINCE FIRST FLIGHT DEC 15, 2006

Challenges to System Safety and Software Safety

- Ensuring MBSE transitions smoothly from traditional artifacts centric to model visualization
  - It can be done, but will require a devoted collaboration (Deming's Constancy of Purpose)
    - more direct involvement with system safety in Use Cases, tagging attributes and tracing safety-critical functions, flows, threads, and functional behaviors in safety domain for capturing objective safety evidence.

- Ensuring Agile software transformation that are less formal, cheaper and faster, also allow adaptation of a software safety process to the standards expected by customers, safety boards and certification authorities (MIL-STD-882E, AOP 52, AMCOM 385-17)
  - Requires measurement, value and risk assessments, a balance of the essentials of practical, formal, and integrated product and process development
  - Software Safety must be much more than just part of the daily "Scrum" – a Rugby Huddle

Summary

- MBSE will require more horizontal integration and collaboration
  - system safety, software system safety, systems engineering, software engineers all engaged with inputs to model, internal model functions, and outputs of the model
- MBSE can help safety engineers better understand safety-critical functionality and expected behavior when conducting FHAs and software safety analysis
- MBSE if set up correctly can yield objective safety evidence output needed for a more convincing Safety Case with Arguments
- Agile software development (and other less formal methods) will require safety engineers to be more closely aligned and involved with day to day activities, including witnessing of tests.
- Ensuring “more” formal methods and models and “less formal” development artifacts (Agile, etc.) will require leadership due diligence to keep it balanced for BOTH process and product **Technical Integrity.**

Closing Thoughts

- System Safety transition to emerging engineering methods
  - It can be done with open mindedness and transition from older traditional methods. Times, technology and environments are changing and system safety must adapt and help make it all work.
  - Cultural changes needed and management buy-in needed,
  - Convincing evidence is needed that emerging methods can be implemented within constraints
  - Ensuring the MBSE Process can work for emerging complex integrated systems of systems (SOS) for warfighters.
    - **Action: R&D Needed in this area to tweak and integrate new Model based processes and Safety Cases with traditional system safety to ensure better Objective Safety Evidence for risk reduction while ensuring Technical Integrity**
  - Recent Links on how some programs are progressing well:
  - http://usaasc.armyalt.com/#folio=60
    - Page 59, Agile Acquisition, Ranjit Singh Mann P.E., and Michael Hanners

Good Leading Edge Technical Papers

- A paper on Model Based Safety Analysis by NASA and NASA Langley
  - http://shemesh.larc.nasa.gov/fm/papers/Model-BasedSafetyAnalysis.pdf