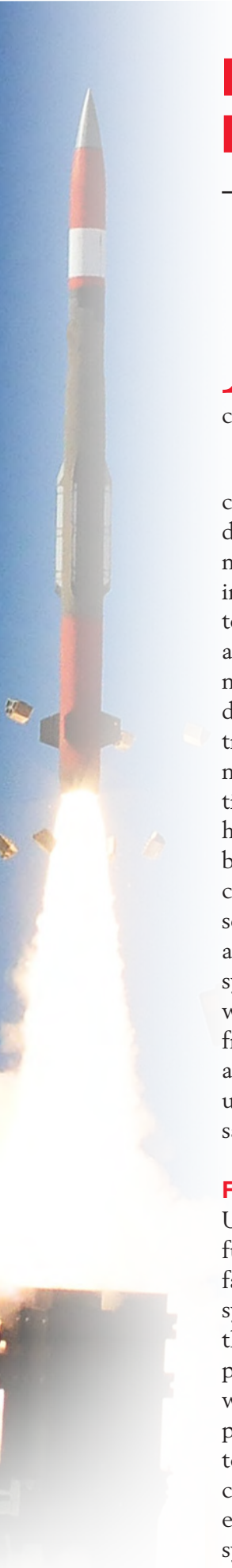


Model Based Functional Safety – How Functional Is It?

by Barry Hendrix, Thomas E. Lewis, Melissa Emery and Brian Rachele
Huntsville, Alabama and Boston, Massachusetts

As the engineering world embraces model based system engineering (MBSE), the system safety discipline needs to be an integral part of this approach. The need for model based functional safety (MBFS), as part of the established system safety and software safety process, is becoming apparent due to system complexity.

MBFS may utilize use cases, structural architecture models, activity diagrams, sequence diagrams, functional flow diagrams and state/mode models to depict safety attributes and to influence explicit safety requirements. MBSE tools suites and effective subset tools, such as ANSYS Medini, can be used effectively to model functional safety aspects of the functional decomposition of requirements with complete traceability and allocation to software. SysML may be used to depict critical functions, functional threads, safety features and expected behavior. Such augmented safety models can also be used to analyze potential off-nominal failure conditions and system behavior for various scenarios when conducting functional hazard assessments (FHA) and subsequently detailed system and software safety analyses. This paper will provide a functional example of the MBSE framework and concepts for tool use in the analysis of safety aspects and the use of attributed models and artifacts to supplement system safety documentation.

Functionality of MBSE

Using models can improve accuracy during the functional hazard analyses and can help validate fault tree analyses (FTA), as well as subsequent system safety analysis (SSA) processes because the model focuses on the architecture, the physical system and the computer system, as well as the applicable software/middleware/programmable logic devices. This paper is intended to show how valuable MBFS approaches can be for complex software-intensive integrated systems in the evaluation of safety significant systems/functions.

Safety-critical systems and safety-critical functions (SCF) must be the focus when conducting functional hazard analyses and FHAs. FHAs have become the prerequisite for software safety analyses because the behavior of the software and its system interfaces must be well understood in the safety domain. Functional safety models should focus on how the architecture and the physical system, the computer system and embedded software contributions ensure correct and predictable system behavior. On complex systems with software-intensive SCFs, MBSE functional analyses and functional safety subsets should focus on the many complex interactions in software, and functional failure and fault conditions and situations that can lead to hazards. Functional safety tasks as part of, and beyond, the FHAs and software safety analyses should be integrated into models producing safety use cases, safety activity diagrams and functional flow diagrams to influence system and explicit safety requirements, design safety features, hazard mitigation, safety verification and risk reduction actions in the design and operations leading to system certification. The use of MBSE tools at the safety level is vital to properly capture and depict safety attributes and contributions to correct system behavior.

Model Based Functional Safety

Unlike previous papers on the subject, including those prepared by A-P-T Research, Inc. [Refs. 1 and 2], that try to convince and persuade based on need and value, the precept is now advocating the essential value of MBFS as part of the established MBSE beyond acceptance into the actual use of tools. Model based

(Photo: John Hamilton, Army)

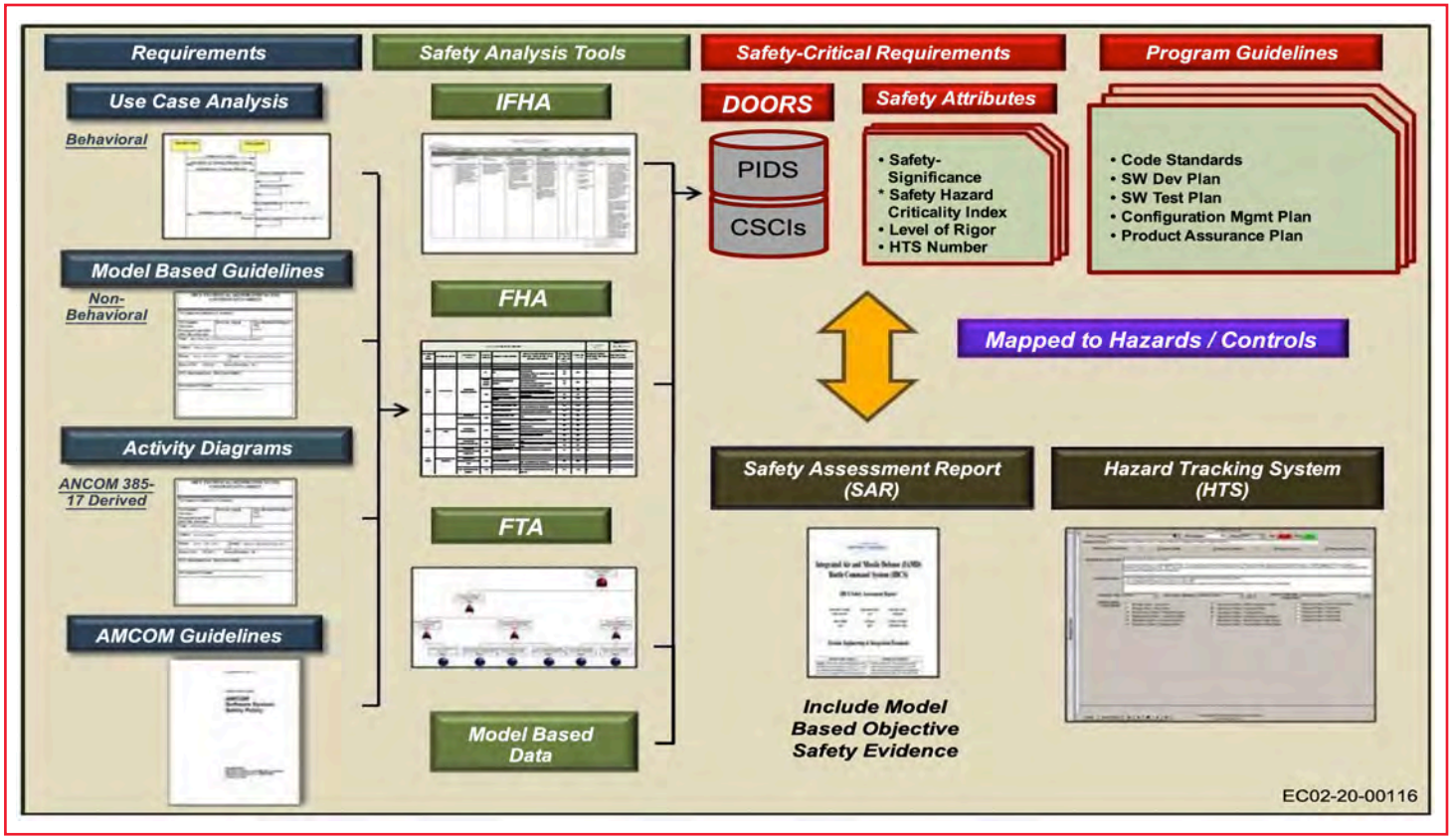


Figure 1 — Model Based Functional Safety.

tools can be used effectively to depict the facts, safety attributes, safety requirements, documentation of safety mitigations, traceability, objective safety evidence and all parts of the process.

In 2012, MIL-STD-882E promulgated task 208 Functional Hazard Analyses (FHA) [Ref. 3]. FHAs always focus on the safety-significant domain of SCFs and safety-related functions, especially those functions and behaviors of the embedded application software instruction set at the system level. FHAs have been part of the SAE ARP-4761 process since 1996 and became the central focus of system safety and software safety that has in recent years evolved into functional safety per IEC 61508 [Ref. 4]. Other standards, such as the DO-178C [Ref. 5], focused on avionics software verification, but lacked modeling tasks.

The new augmented DO-331 Model Based Development and Verification [Ref. 6] added the process for ensuring functional safety aspects are modeled as part of the integrated safety analysis process. Each standard requires a common outcome for systems to be proven with acceptable, known and documented risks. Modeling of all aspects is possible regardless of the subtle approaches and differences. Tools and processes can adapt to meet the objectives of the standard.

Safety models should be developed to make safety engineering documentation easy to read and interpret (see Figure 1). These models can be any formal constructive method to accurately depict the various aspects and attributes of functional safety. The models can be constructed to augment existing FHAs. The focus should be on modeling the system to identify hazards such that safety requirements can be allocated throughout the system. The functional decomposition of explicit safety requirements, especially derived safety requirements during the safety analysis process, can be included in the functional safety model. Highly integrated and complex software-intensive systems functions with many interactions must be broken down and depicted with functional flow charts and safety activity diagrams to ensure the system is well understood from a safety perspective. Models make this a reality.

These functional models should focus on safety behavior at the system, subsystem and software levels. MBSE models and safety subsets should integrate and support system requirements, design safety, safety analysis, safety verification and certification.

For Department of Defense (DoD) systems, models should support the Defense Architecture Framework (DoDAF) tools for depicting and documenting a system's functional and physical architectures. DoDAF defines a common approach for models describing and presenting principles, assumptions and all viewpoints (CONOPS; capability, functional, system, operational).

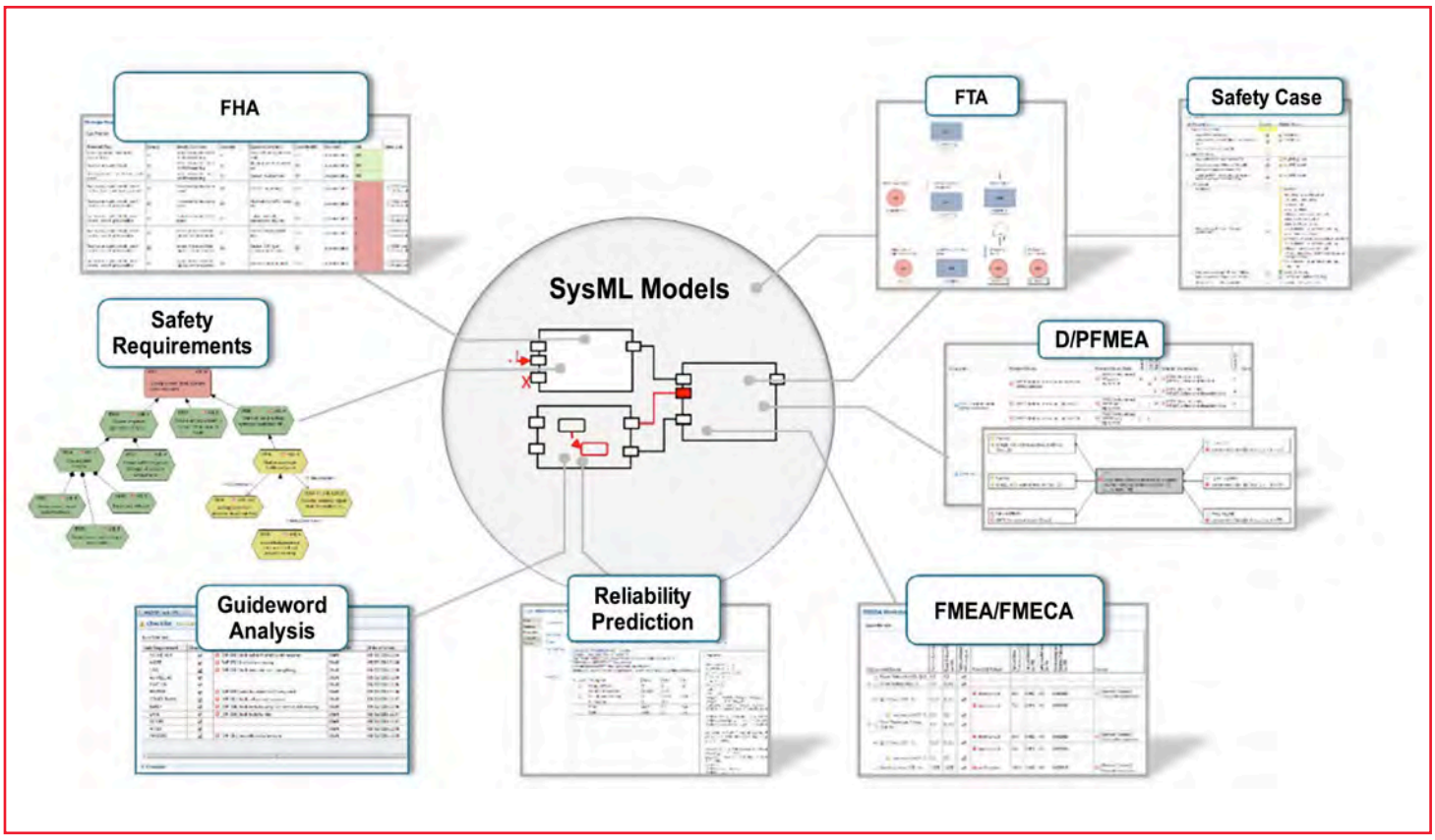


Figure 2 — Medini Toolset for Safety Analyses.

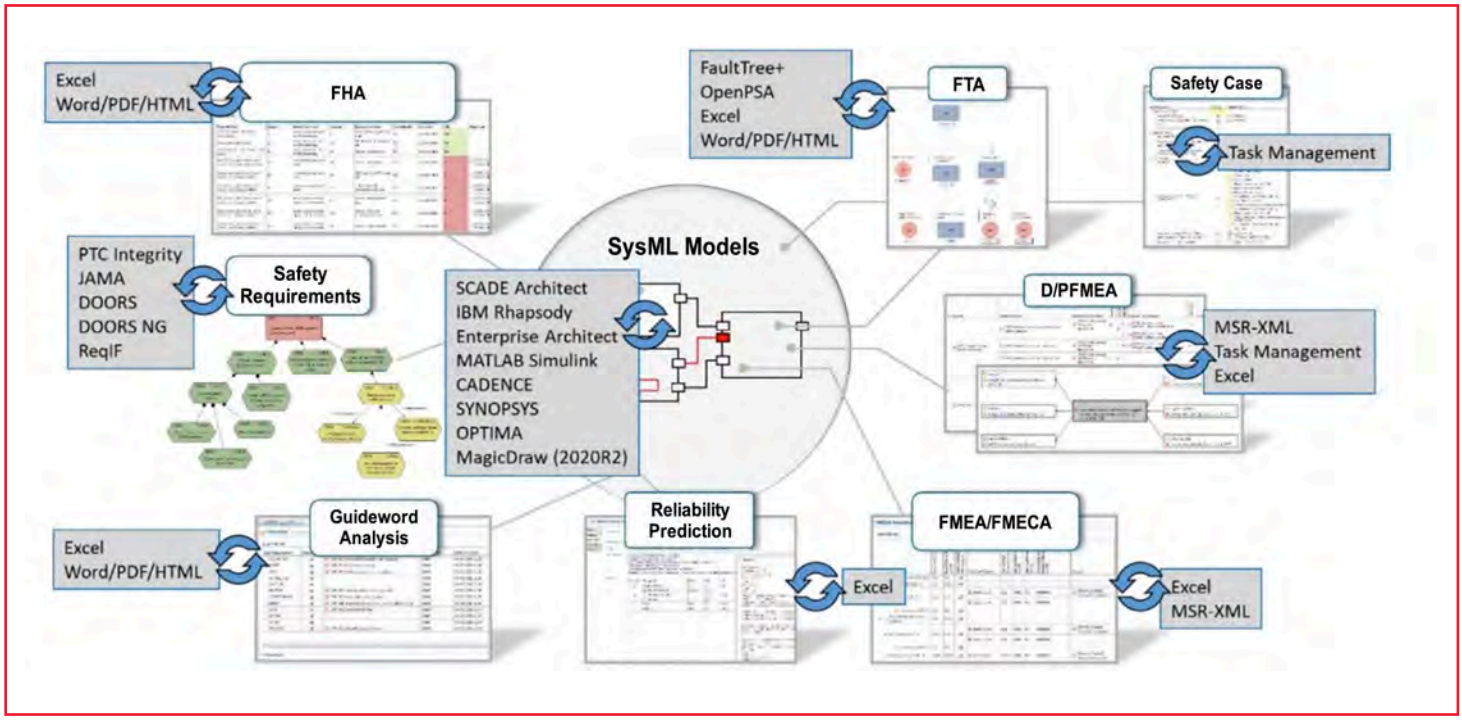


Figure 3 — Medini Toolset Compatibility with Other Software Tools/Products.

A Functional Example Using ANSYS Medini

MBSE tools have many facets that support functional safety analysis and production of safety artifacts. Figure 2 shows the SysML Models support safety analyses, and Figure 3 displays the compatibility of SysML models with other tools and software products.

Figures 4 through Figure 8 show the system architecture for an example of a missile system and MIL-STD-882E task application. The ANSYS Medini

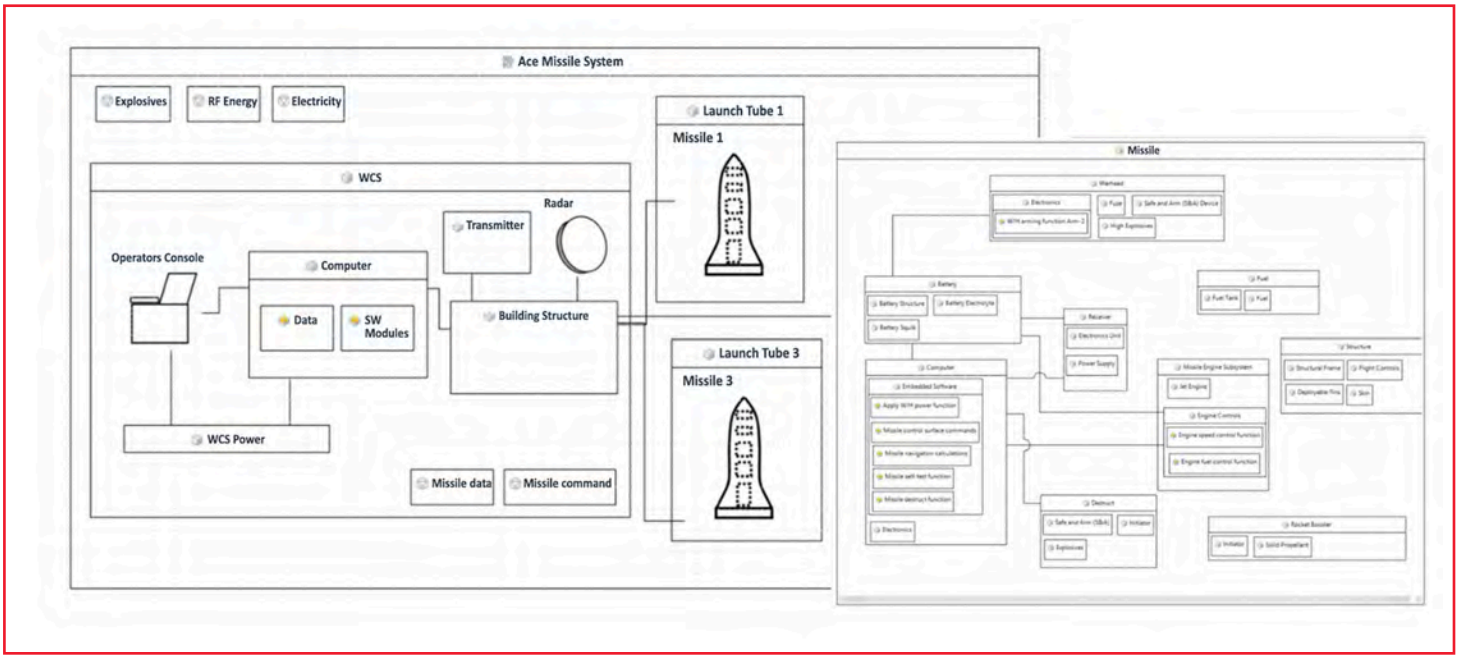


Figure 4 — Example Missile System Functionality.

ID	Item or Function	Name	Hazard Effects	Description	Comments
PHL-1	Structure	Missile body breaks up resulting in fuel leakage and ignition source causing fire	[MHP-001] Missile fire		Ground operations
PHL-2	Structure	Missile body breaks up causing missile crash	[MHP-002] Missile crash		Flight
PHL-3	Warhead	Detonation of W/H explosives from fire, bullet, shock, etc.	[MHP-003] W/H explosives detonation		Use insensitive munitions (IM)
PHL-4	Warhead	Initiation of W/H from inadvertent initiation commands	[MHP-004] Inadvertent W/H initiation		Initiation requires both arm and fire signals
PHL-5	Warhead	Missile W/H fails to initiate	[MHP-005] Dud		Unexploded ordnance (UXO) concern
PHL-6	Rocket Booster	Engine fails to start (missile crash)	[MHP-006] Incorrect Target		Unsafe missile state, fuel release
PHL-7	Rocket Booster	Engine fails during flight resulting in crash	[MHP-006] Incorrect Target		
PHL-8	Fuel	Engine fuel tank leakage and ignition source present resulting in fire	[MHP-001] Missile fire		
PHL-9	Computer	Computer inadvertently generates W/H Arm-1 and Arm-2 commands, causing W/H initiation	[MHP-004] Inadvertent W/H initiation		
PHL-10	Computer	Computer fails to generate W/H Arm-1 or Arm-2 commands	[MHP-007] Inability to initiate W/H		
PHL-11	Computer	Computer inadvertently generates missile destruct command	[MHP-010] Inadvertent missile destruct		
PHL-12	Computer	Computer fails to generate missile destruct command	[MHP-009] Inability to destruct missile		
PHL-13	Battery	Battery is inadvertently activated, providing power for W/H Arm and Fire commands	[MHP-004] Inadvertent W/H initiation		
PHL-14	Battery	Battery electrolyte leakage occurs and ignition source present resulting in fire	[MHP-001] Missile fire		
PHL-15	Destruct	Destruct system fails	[MHP-009] Inability to destruct missile		
PHL-16	Receiver	Receiver fails—no communication with missile	[MHP-009] Inability to destruct missile		
PHL-17	Receiver	Receiver fails—creates erroneous destruct command	[MHP-010] Inadvertent missile destruct		
PHL-18	Rocket Booster	Inadvertent ignition of rocket	[MHP-011] Inadvertent launch		
PHL-19	Computer	Computer inadvertently generates missile launch commands	[MHP-011] Inadvertent launch		
PHL-20	Radar	Electromagnetic radiation (EMR) injures exposed personnel	[MHP-012] Personnel RF energy injury		

PHL Analysis of Ace Missile System—System Functions Evaluation

type filter text

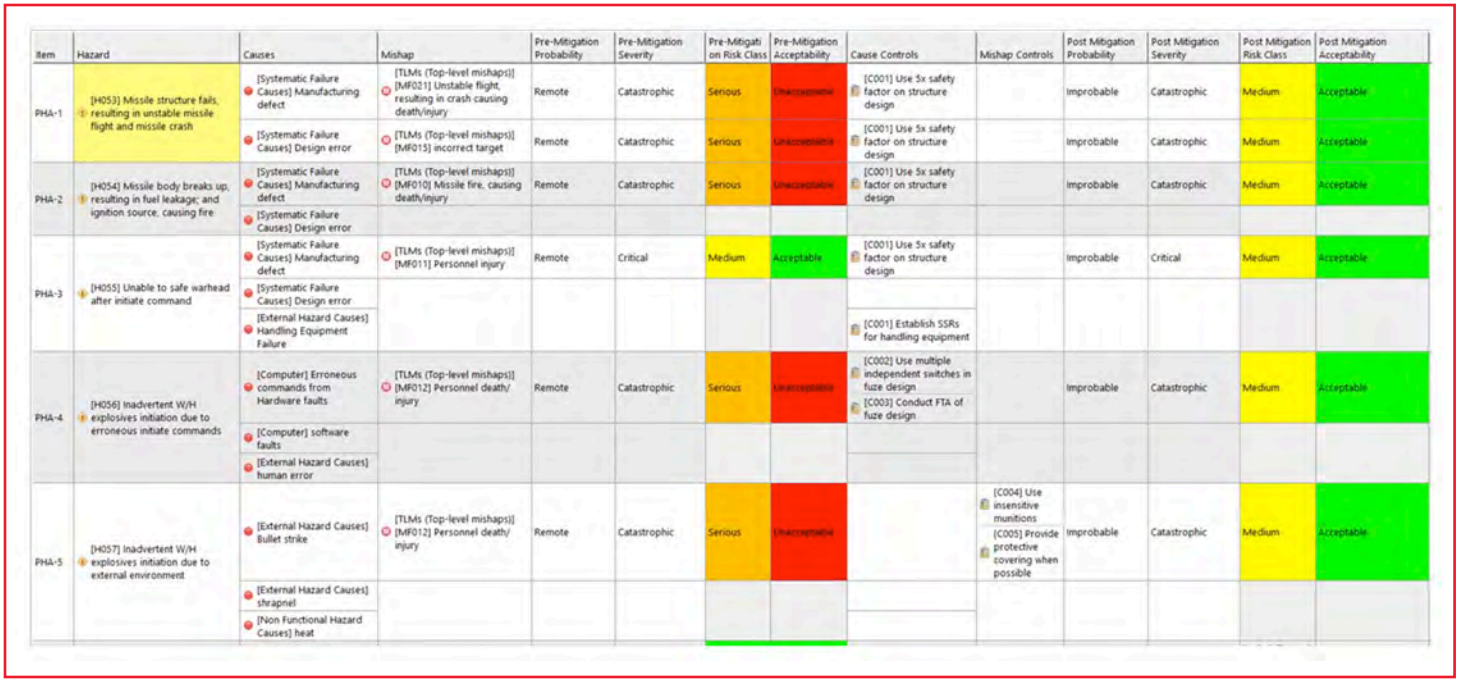
ID	Item or Function	Malfunctioning Behaviour	Hazard Effects
PHL-24	[F001] Warhead initiate	[MF002] Warhead initiate function occurs inadvertently	[MHP-004] Inadvertent W/H initiation
PHL-25	[F001] Warhead initiate	[MF003] Warhead initiate function fails to occur	[MHP-005] Dud
PHL-26	[F002] Missile launch	[MF004] Missile launch function occurs inadvertently	[MHP-011] Inadvertent launch
PHL-27	[F003] Missile self-test	[MF005] Self-test function fails, resulting in unknown missile status	[MHP-016] Unsafe missile state
PHL-28	[F004] Missile destruct	[MF006] Missile destruct function occurs inadvertently	[MHP-010] Inadvertent missile destruct
PHL-29	[F005] Missile navigation	[MF007] Errors occur in missile navigation function	[MHP-006] Incorrect Target
PHL-30	[F006] Missile guidance	[MF008] Errors occur in missile guidance function	[MHP-006] Incorrect Target
PHL-31	[F007] Communications with missile	[MF009] Communication is lost, causing inability to initiate missile destruct system	[MHP-009] Inability to destruct missile

Figure 5 — Task 201 Preliminary Hazard List.

tool can support generation and tracing of hazard analyses, failure modes, mitigation, requirements, etc.

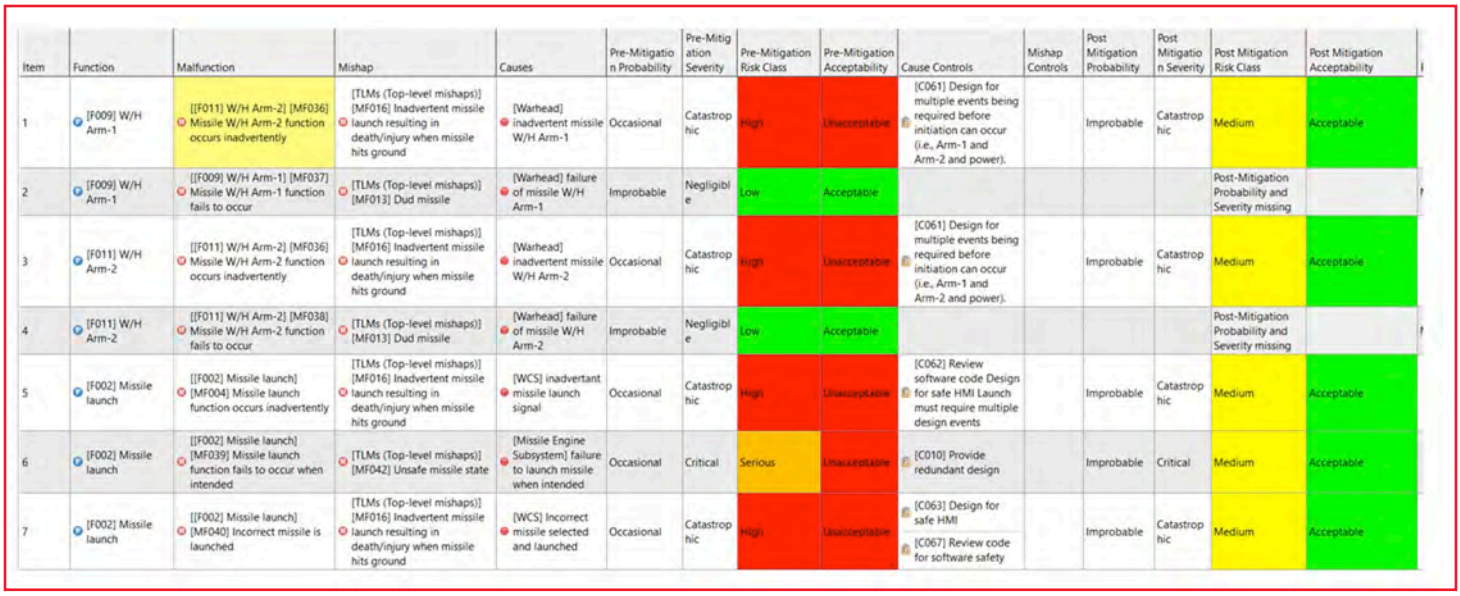
The MBSE toolset contributes to the generation of MIL-STD-882E safety artifacts as defined in the MIL-STD-882E tasks. Continuing with the missile system example in Figure 4, Figures 5 through 7 show a subset of the MIL-STD-882E task artifacts producible using the ANSYS Medini tool.

Other safety and system analyses, such as FTA, can also be implemented and tracked in the toolset (Figure 8).



Item	Hazard	Causes	Mishap	Pre-Mitigation Probability	Pre-Mitigation Severity	Pre-Mitigation Risk Class	Pre-Mitigation Acceptability	Cause Controls	Mishap Controls	Post Mitigation Probability	Post Mitigation Severity	Post Mitigation Risk Class	Post Mitigation Acceptability
PHA-1	[H053] Missile structure fails, resulting in unstable missile flight and missile crash	[Systematic Failure Causes] Manufacturing defect	[TLMs (Top-level mishaps)] [MF021] Unstable flight, resulting in crash causing death/injury	Remote	Catastrophic	Serious	Unacceptable	[C001] Use 5x safety factor on structure design		Improbable	Catastrophic	Medium	Acceptable
		[Systematic Failure Causes] Design error	[TLMs (Top-level mishaps)] [MF015] incorrect target	Remote	Catastrophic	Serious	Unacceptable	[C001] Use 5x safety factor on structure design		Improbable	Catastrophic	Medium	Acceptable
PHA-2	[H054] Missile body breaks up, resulting in fuel leakage; and ignition source, causing fire	[Systematic Failure Causes] Manufacturing defect	[TLMs (Top-level mishaps)] [MF010] Missile fire, causing death/injury	Remote	Catastrophic	Serious	Unacceptable	[C001] Use 5x safety factor on structure design		Improbable	Catastrophic	Medium	Acceptable
		[Systematic Failure Causes] Design error											
PHA-3	[H055] Unable to safe warhead after initiate command	[Systematic Failure Causes] Manufacturing defect	[TLMs (Top-level mishaps)] [MF011] Personnel injury	Remote	Critical	Medium	Acceptable	[C001] Use 5x safety factor on structure design		Improbable	Critical	Medium	Acceptable
		[Systematic Failure Causes] Design error											
		[External Hazard Causes] Handling Equipment Failure						[C001] Establish SSRs for handling equipment					
PHA-4	[H056] Inadvertent W/H explosives initiation due to erroneous initiate commands	[Computer] Erroneous commands from Hardware faults	[TLMs (Top-level mishaps)] [MF012] Personnel death/ injury	Remote	Catastrophic	Serious	Unacceptable	[C002] Use multiple independent switches in fuze design [C003] Conduct FTA of fuze design		Improbable	Catastrophic	Medium	Acceptable
		[Computer] software faults											
		[External Hazard Causes] human error											
PHA-5	[H057] Inadvertent W/H explosives initiation due to external environment	[External Hazard Causes] Bullet strike	[TLMs (Top-level mishaps)] [MF012] Personnel death/ injury	Remote	Catastrophic	Serious	Unacceptable		[C004] Use insensitive munitions [C005] Provide protective covering when possible	Improbable	Catastrophic	Medium	Acceptable
		[External Hazard Causes] shrapnel											
		[Non Functional Hazard Causes] heat											

Figure 6 — Task 202 Preliminary Hazard Analysis.



Item	Function	Malfunction	Mishap	Causes	Pre-Mitigation Probability	Pre-Mitigation Severity	Pre-Mitigation Risk Class	Pre-Mitigation Acceptability	Cause Controls	Mishap Controls	Post Mitigation Probability	Post Mitigation Severity	Post Mitigation Risk Class	Post Mitigation Acceptability
1	[F009] W/H Arm-1	[[F011] W/H Arm-2] [MF036] Missile W/H Arm-2 function occurs inadvertently	[TLMs (Top-level mishaps)] [MF016] Inadvertent missile launch resulting in death/injury when missile hits ground	[Warhead] inadvertent missile W/H Arm-1	Occasional	Catastrophic	High	Unacceptable	[C061] Design for multiple events being required before initiation can occur (i.e., Arm-1 and Arm-2 and power).		Improbable	Catastrophic	Medium	Acceptable
2	[F009] W/H Arm-1	[[F009] W/H Arm-1] [MF037] Missile W/H Arm-1 function fails to occur	[TLMs (Top-level mishaps)] [MF013] Dud missile	[Warhead] failure of missile W/H Arm-1	Improbable	Negligible	Low	Acceptable					Post-Mitigation Probability and Severity missing	
3	[F011] W/H Arm-2	[[F011] W/H Arm-2] [MF036] Missile W/H Arm-2 function occurs inadvertently	[TLMs (Top-level mishaps)] [MF016] Inadvertent missile launch resulting in death/injury when missile hits ground	[Warhead] inadvertent missile W/H Arm-2	Occasional	Catastrophic	High	Unacceptable	[C061] Design for multiple events being required before initiation can occur (i.e., Arm-1 and Arm-2 and power).		Improbable	Catastrophic	Medium	Acceptable
4	[F011] W/H Arm-2	[[F011] W/H Arm-2] [MF038] Missile W/H Arm-2 function fails to occur	[TLMs (Top-level mishaps)] [MF013] Dud missile	[Warhead] failure of missile W/H Arm-2	Improbable	Negligible	Low	Acceptable					Post-Mitigation Probability and Severity missing	
5	[F002] Missile launch	[[F002] Missile launch] [MF004] Missile launch function occurs inadvertently	[TLMs (Top-level mishaps)] [MF016] Inadvertent missile launch resulting in death/injury when missile hits ground	[WCS] inadvertant missile launch signal	Occasional	Catastrophic	High	Unacceptable	[C062] Review software code Design for safe HMI Launch must require multiple design events		Improbable	Catastrophic	Medium	Acceptable
6	[F002] Missile launch	[[F002] Missile launch] [MF039] Missile launch function fails to occur when intended	[TLMs (Top-level mishaps)] [MF042] Unsafe missile state	[Missile Engine Subsystem] failure to launch missile when intended	Occasional	Critical	Serious	Unacceptable	[C010] Provide redundant design		Improbable	Critical	Medium	Acceptable
7	[F002] Missile launch	[[F002] Missile launch] [MF040] Incorrect missile is launched	[TLMs (Top-level mishaps)] [MF016] Inadvertent missile launch resulting in death/injury when missile hits ground	[WCS] Incorrect missile selected and launched	Occasional	Catastrophic	High	Unacceptable	[C063] Design for safe HMI [C067] Review code for software safety		Improbable	Catastrophic	Medium	Acceptable

Figure 7 — Task 208 Functional Hazard Analysis.

Some Crucial Defense Top-Level Event Functions Ideal for Safety Modeling (Non-Aviation)

Civil aircraft agencies have detailed safety-critical functions, loss-of-function conventions, failure conditions and hazards for aircraft functions requiring safety analyses. However, non-aviation military often lacks standardization. The following list includes some — but not all — crucial defense top-level event functions that are ideal for safety modeling:

- Total systems integration using use cases, activity diagrams, functional flow, states/modes
- SCFs that directly impact top-level catastrophic hazards/events
- Inadvertent launch models
- Fratricide prevention models for weapons command and control
- Inadvertent movement of launchers or sensors models
- Inadvertent radiation models
- Loss of positive sustained communications of Command and Control (C2) models
- Loss of, or malfunction of, any messaging or crucial inputs to C2 models
- Hazardously misleading information on graphical user interfaces (GUIs) or displays, erroneous displays and false alerts models

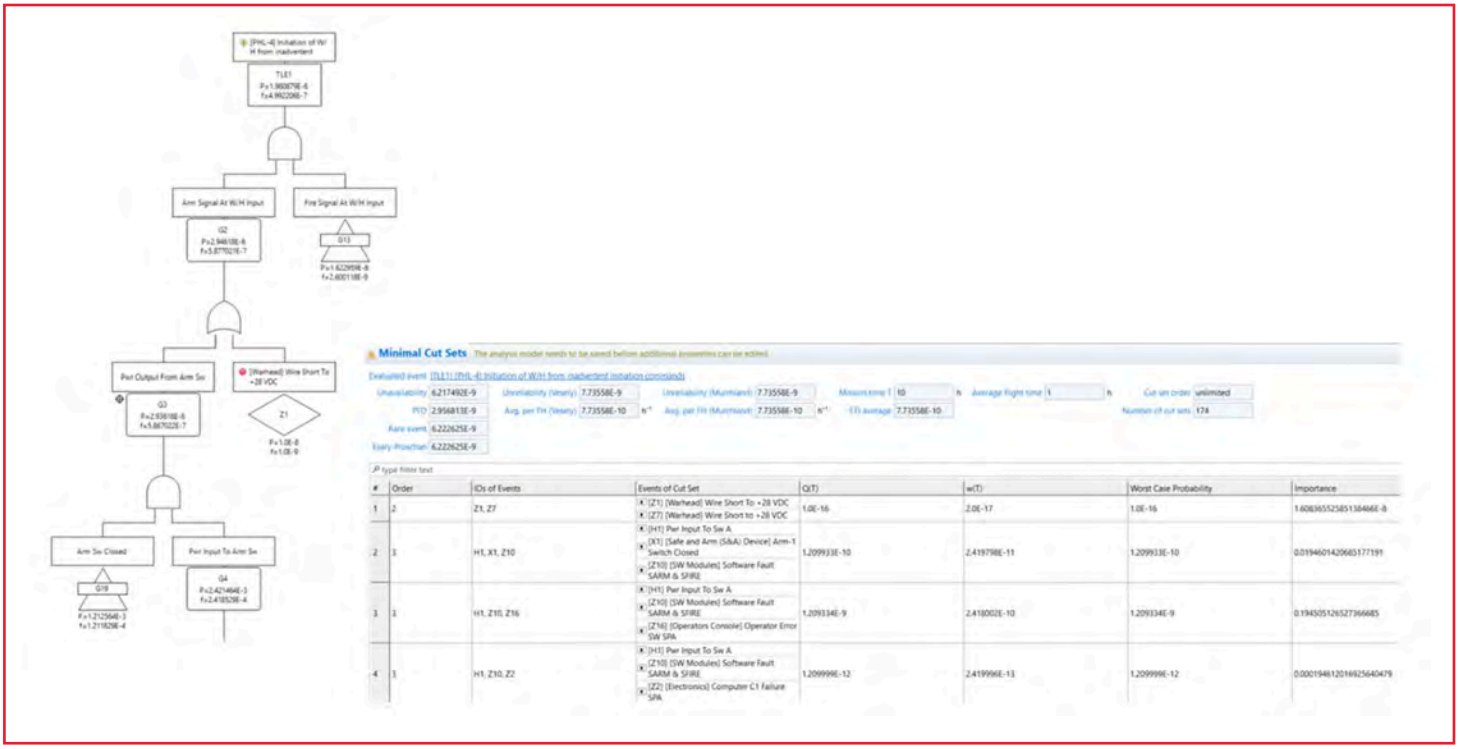


Figure 8 — Fault Tree Analysis.

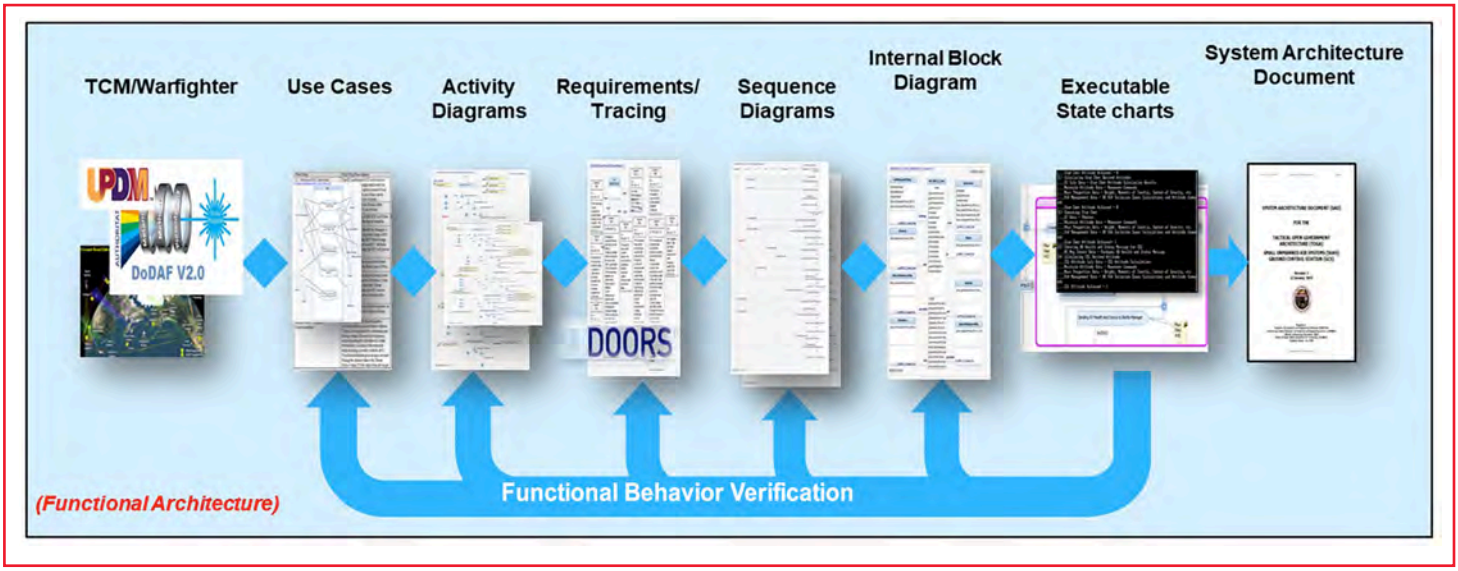


Figure 9 — Functional Safety Model Supporting Processes and Documentation.

- Software safety complex interaction and behavioral models
- Safety verification of off-nominal behavior of software-controlled SCF models
- System of system interoperability of SCF models

The DoDAF with safety preferences in Figure 9 illustrates the vital areas highly recommended to be part of the functional safety model for any military/defense system requiring system safety and software safety. Specifically, when generating a safety assessment report or safety case, this process provides the required functional architecture. DoD has made it clear in many other documents MBSE tools must have the ability to use the models for the transition from system design to software design and the complex functional decomposition of higher-level requirements in software into lower-level requirements in software and all the functional threads and paths, down to the lowest unit level functions and scripts. The ability to analyze safety activities and ensure SCFs and functional threads in software from the system level to the CSCI to CSCs to CSUs to class and types can be modeled is

part of the modern functional safety and software safety process.

Conclusion

Using MBSE toolsets, such as ANSYS Medini, provides efficient and cohesive functional safety assessments. The ability to trace, track, integrate and assess the requirements, design, and system/subsystem models provides functional and comprehensive contributions. MBSE becomes a real safety functional toolset when using an MBSE tool designed to support safety analyses and required artifacts. The ability to use modern and powerful tools as part of the safety analysis and review process greatly enhances the safety documentation showing precisely how a system behaves under credible failure conditions and hazardous situations. Capturing the comprehensive safety data with models to provide objective safety evidence is a major breakthough from previous methods where such evidence could not be depicted in precise detail.

In June 2018, the DoD Digital Engineering Strategy was promulgated by the Office of the Deputy Assistant Secretary of Defense for System Engineering [Ref. 7]. The first goal was to "formalize the development, integration and use of models to inform enterprise and program decision making." Model-centric organizations have evolved at NASA and DoD in recent years as more modeling tools and processes, lean initiatives and focused agile processes are becoming more widespread and valued. Several agencies and commands made MBSE mandatory on some new major acquisitions and the restructuring of the Army Futures Commands made a priority of the use of MBSE. Since system safety is widely viewed in DoD as a subset of system engineering, many contractors have sought ways to incorporate MBSE into their internal best practices using toolsets and process procedures. Our goal is to continue using MBSE toolsets to help make our approach efficient and completely functional.

References

1. Hendrix, B., S. Dwyer, & D. West. "Model Based Functional Safety," *Journal of System Safety*, 2018.
2. A-P-T Research, Inc. "Software *System Safety & Risk Management for Engineers" Training Courses, 2018*.
3. Department of Defense. *MIL-STD-882E Standard Practice System Safety*, 2012.
4. International Electrotechnical Commission. (n.d.). *IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.*
5. RTCA SC-205; EUROCAE WG-12. *DO-178C Software Considerations in Airborne Systems and Equipment Certification*, 2012.
6. RTCA SC-205; EUROCAE WG-12. *DO-331 Model Based Development and Verification*, 2010.
7. Office of the Deputy Assistant Secretary of Defense for System Engineering. *DoD Digital Engineering Strategy*, Retrieved from https://sercuarc.org/wp-content/uploads/2018/06/Digital-Engineering-Strategy_Approved.pdf, 2018.