# Model Based Functional Safety – How Functional Is It?

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

s 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)32 Journal of System Safety, Spring 2022



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 inter-

pret (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.

P type th	ter hext						
ID	Nem 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	3 Warhead	Initiation of W/H from inadvertent initiation commands	(MHP-004) inadvertime W/H initiation		Initiation requires both arm and fire signals		
PHL-5	3 Warhead	Missile W/H fails to initiate	(MHP-005) Dud		Unexploded ordnance (UXO) concern		
PHL-6	Rocket Booster	Engine fails to start (missile crash)	<ul> <li>[MHP-006] Incorrect Target</li> </ul>		Unsafe missile state, fuel release		
9HL-7	· Rocket Booster	Engine fails during flight resulting in crash	(MHP-006) Incorrect Target				
PHL-8	3 Fuel	Engine fuer tank leakage and ignition source present resulting in fire	(MHP-001) Missile fire	PHL Analy	sis of Ace Missile System-	-System Functions Evaluat	ion
PHL-9	(@ Computer	Computer inadvertently generates W/H Arm-1 and Arm-2 commands, causing W/H initiation	(MHP-004) Inadvertent W/H initiation	P type filter	text		
PHL-10	Computer	Computer fails to generate W/H Arm-1 or Arm-2 commands	(MHP-007) Inability to initiate W/H	ID	Item or Function	Malfunctioning Behaviour	Hazard Effects
PHL-11	Computer	Computer inadvertently generates missile destruct command	• [MHP-010] Inadvertent missile destruct		0	[MF002] Warhead initiate	[MHP-004] Inadvertent
PHL-12	Ge Computer	Computer fails to generate missile destruct command	(MHP-009) inability to destruct missile	PHL-24	[F001] Warhead initiate	unction occurs inadvertently	W/H initiation
PHL-13	Battery	Battery is inadvertently activated, providing power for W/H Arm and Fire commands	(MHP-004] Inadvertent W/H initiation	PHL-25	G [F001] Warhead initiate	[MF003] Warhead initiate function fails to occur	[MHP-005] Dud
PHL-14	Battery	Battery electrolyte leakage occurs and ignition source present resulting in fire	[MHP-001] Missile fire	PHI -26	G (E002) Missile Jaunch	MF004] Missile launch function	MHP-011] Inadvertent
PHL-15	Destruct	Destruct system fails	<ul> <li>[MHP-009] Inability to destruct missile</li> </ul>	Price CO	· Fronel missile market	occurs inadvertently	launch
PHL-16	@ Receiver	Receiver fails—no communication with missile	[MHP-009] inability to destruct missile	22.25		[MF005] Self-test function fails,	MHP-0161 Unsafe missile
PHL-17	() Receiver	Receiver fails—creates erroneous destruct command	(MHP-010) Inadvertent missile destruct	PHL-27	[F003] Missile self-test	resulting in unknown missile status	state
PHL-18	Rocket Booster	Inadvertent ignition of rocket	<ul> <li>[MHP-011] Inadvertent launch</li> </ul>			Duroofi Missile destruct	IN ALLO ALLON LOOK AND
PHL-19	Computer	Computer inadvertently generates missile launch commands	(MHP-011) inadvertent launch	PHL-28	[F004] Missile destruct	o [MF006] Missile destruct function occurs inadvertently	missile destruct
PHL-20	ve Radar	Electromagnetic radiation (EMR) injures exposed personnel	<ul> <li>[MHP-012] Personnel RF energy injury</li> </ul>	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	<ul> <li>[MHP-006] Incorrect Target</li> </ul>
				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).

tem	Hazard	Causes	Mishap	Pre-Mitigation Probability	Pre-Mitigation Severity	Pre-Mitigati on Risk Class	Pre-Mitigation Acceptability	Cause Controls	Mishap Controls	Post Mitigation Probability	Post Mitigation Severity	Post Mitigation Risk Class	Post Mitigation Acceptability
HA-1	[H053] Missile structure fails, (1) resulting in unstable missile	[Systematic Failure Causes] Manufacturing defect	[TLMs (Top-level mishaps)] [MF021] Unstable flight, resulting in crash causing death/injury	Remote	Catastrophic	Serious	LINACCAREMENT	[C001] Use 3x safety factor on structure design		Improbable	Catastrophic	Medium	Acceptable
	flight and missile crash	[Systematic Failure Causes] Design error	[TLMs (Top-level mishaps)]     [MF015] incorrect target	Remote	Catastrophic	Serious	Gracewoldela	[C001] Use 5x safety factor on structure design		Improbable	Catastrophic	Medium	Acceptable
HA-2	[H054] Missile body breaks up, resulting in fuel leakage; and	Systematic Failure Causes] Manufacturing defect	[TLMs (Top-level mishaps)] (MF010] Missile fire, causing death/injury	Remote	Catastrophic	Serious	Unacceptation	[C001] Use 5x safety factor on structure design		Improbable	Catastrophic	Medium	Acceptable
	ignition source, causing fire	<ul> <li>[Systematic Failure Causes] Design error</li> </ul>											
	100	(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
на-з	(H055) Unable to safe warhead after initiate command	<ul> <li>[Systematic Failure Causes] Design error</li> </ul>											
		<ul> <li>[External Hazard Causes]</li> <li>Handling Equipment Failure</li> </ul>						(C001) Establish SSRs for handling equipment					
	[H056] Inadvertent W/H	[Computer] Erroneous commands from Hardware faults	[TLMs (Top-level mishaps)] [MF012] Personnel death/ injury	Remote	Catastrophic	Serious	Leacceptains	[C002] Use multiple independent switches in fuze design [C003] Conduct FTA of fuze design		Improbable	Catastrophic	Medium	Acceptable
	erroneous initiate commands	[Computer] software faults						1	A Barris	i	1		
		[External Hazard Causes] human error											
9HA-5	[H057] Inadvertent W/H	<ul> <li>[External Hazard Causes] Bullet strike</li> </ul>	[TLMs (Top-level mishaps)] (IMF012] Personnel death/ injury	Remote	Catastrophic	Serious	(maccaptaica)	R	(C004) Use insensitive munitions (C005) Provide protective covering when possible	Improbable	Catastrophic	Medium	Acceptable
		<ul> <li>[External Hazard Causes] shrapnel</li> </ul>	-							1	1		
		<ul> <li>[Non Functional Hazard Causes] heat</li> </ul>											

Figure 6 — Task 202 Preliminary Hazard Analysis.

Item	Function	Malfunction	Mishap	Causes	Pre-Mitigatio n Probability	Pre-Mitig ation Severity	Pre-Mitigation Risk Class	Pre-Mitigation Acceptability	Cause Controls	Mishap Controls	Post Mitigation Probability	Post Mitigatio n Severity	Post Mitigation Risk Class	Post Mitigation Acceptability
1	• [F009] W/H Arm+1	([F011] W/H Arm-2] [MF036] O Missile W/H Arm-2 function occurs inadvertently	[TLMs (Top-level mishaps)] [MF016] Inadvertent missile [2] Iaunch resulting in death/injury when missile hits ground	[Warhead] inadvertent missile W/H Arm-1	Occasional	Catastrop hic	High	Linecorptable	[C061] Design for multiple events being required before initiation can occur (i.e., Arm-1 and Arm-2 and power).		Improbable	Catastrop hic	Medium	Acceptable
2	G [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	Negligibl e	Low	Acceptable				13	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 I aunch resulting in death/injury when missile hits ground	[Warhead] inadvertent missile W/H Arm-2	Occasional	Catastrop hic	High	Unacceptable	(C061) Design for multiple events being required before initiation can occur (i.e., Arm-1 and Arm-2 and power).		Improbable	Catastrop hic	Medium	Acceptable
•	• [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	Negligibl e	Low	Acceptable					Post-Mitigation Probability and Severity missing	
5	[F002] Missile     Iaunch	<ul> <li>[[F002] Missile launch]</li> <li>[MF004] Missile launch function occurs inadvertently</li> </ul>	[TLMs (Top-level mishaps)] [MF016] Inadvertent missile launch resulting in death/injury when missile hits ground	(WCS) inadvertant. missile launch signal	Occasional	Catastrop hic	High	Unacceptation	[C062] Review software code Design for safe HMI Launch must require multiple design events		Improbable	Catastrop hic	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	Linacceptable	CO10] 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 I launch resulting in death/injury when missile hits ground	[WCS] Incorrect missile selected and launched	Occasional	Catastrop	Han	Unacceptable	<ul> <li>[C063] Design for safe HMI</li> <li>[C067] Review code for software safety</li> </ul>	2	Improbable	Catastrop hic	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

[PHC-4] instations of W/     H from instations of W/							
TUE							
fs4.80208-7							
	· · · · · · · · · · · · · · · · · · ·						
Arm Signal At WLH Imput Fire Signal At	WHinput						
	<u></u>						
P=2.948102-6 f+5.8770216-7	7						
Pu1622 1+2.002	结绳-击 11超-夺						
1							
$\bigcirc$							
	and the state of						
Original States Tele	Minimal Cut	Sets The analysis model needs to be	a same before additional properties can be edited				
Put Output Form Arm Ser	Minimal Cut	Sets The analyse model reach to be 11/17H-0 toitution of With from made 11/4924-9 University General 7	e sand before additional prosenties parties edited where installant protected (75588-9 installant (Secretary) 775588-9	Manual Annual 19	In Justice Fight Stars 1	h Cation brane unimated	
Part Chaput From Aim Sar         Image: From Aim Sar           Image: From Aim Sar         Image: From Aim Sar	Minimal Cut Destured event IDJ Cransilation (62 PTD 23	Sets The analyse model needs to be     L111PHL-D Initiation of With from made     H17492E-9     Unversionity (Anny) 7     H9411E-9     Arg. per Tri (Vening) 7	e aand belleen accilient i ensemble carrier echel ended instalien contriandi (735586-9) (Investalishy (Marriane) (735586-1 (735586-10) % <sup>4</sup> Ang. per III (Marriane) (735586-1	6 Missoni mug 1 KS 10 M <sup>rs</sup> (1) average 7,2155	66-10	h Caster order selented	
Par Oupul Fam. Am Sar           Par Oupul Fam Sar           Par Oupul Fam. Am Sar           <	Minimal Cut Internet over 1111 Under Lettry 62 PTO 29 Fare coret 62	Sets The analyse model reach to be     11 (Pril - 4) Instances of W/H from nach     P1462E-9 Uncellapting (Arag. per file (Vesety) 7.     S6811E-9 Arag. per file (Vesety) 7.     220625E-9	e cand belline additional anominis can in extent antindi instation constands (20558-9) (similation) (Aurritanis (20558-9) (20558-9) (s <sup>a</sup> ) Ang, par III (Manmand) (205588-9	Mountaine 1 10 10 11 10 Autoop 7,7350	6 demage Tight time 1	h Ger lan trans unlimbed Number of our sets 174	
Por Corpus Frame Arm San           Image: Corpus Frame Arm Arm San           Image: Corpus Frame Arm	Minimal Cut Detend over 111 Unavelative 42 Pro 29 Fare coret, 62 Usey Research 62	Sets The analysis model's results to be 111 (FRL-E) induction of With Som, cadds 117482E-9 Unrestability (Versely) 7, 95841E-9 Arg, per Thi (Versely) 7, 220428E-9	e und hefme addianal anamme car in schol acted analon concession 20056-9 Unrelative (Aurilianis) 20056-9 6° Ang per in (Aurilianis) 220566-9 22056-10 6° Ang per in (Aurilianis) 220566-1	6 Almanni time 1 (6) 10 6° (1) average 7,7355	6 Januage Right sine 1	h Get in order unimored Number chair sets 174	
Pur Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser           Image: Conput Fram. Am Ser         Image: Conput Fram. Am Ser	Minimal Cut Detrand Sent (D) Unavaluating 62 PTD 29 Fare sent 62 Daty Product 62 P type Inter Let	Sets The analysis middle sends to be     111 (Prill-4) Initiation of With Inns, media     114482-9     Universativity (Marriy) 7,     1664112-9     Zavest-4     Zavest-4	e and helme additional anamine can be sched adapt motion concast 20086-9 University (Manharin 725566-0 225566-9 Inf Manharin 225566-0 255566-19 Inf Manharin 225566-0	0 Mauniting   60 10 N <sup>-1</sup> (1) Aurity (77)55	6 Jaamaga Tugin Sina 1	N Certain Scan weinnand Kennen of ein sens 174	
Pur Conput from Aim Ser	Minimal Cut Denand Sent (DL) Unavaluativy 62 RVD 2.9 Ann som 62 Dany Rouches 62 P spa finar text # Order	Sets The analyse model reach to be     III.074-b analyse model reach to be     III.074-b analyse of With from model     III.022431-b     Arg per thir (testry) 7     Set112-b     Os of Evens	e cand hoffma dollared provinting can be sold extend and don consolidity (20088-9 Extendency (Aumannii 200898-9 (20088-9 R* Aug pe In (Aumannii 200898-1 (20088-9 Cat Set	Massars strong   10 10 N <sup>-1</sup> (1) surrage 7.71550 (0.7)	6 Jamage Right time 1	A Get ten cross wellmood Nomen of not sen (1)4 West Care Probability	Inpofance
Per Gaged from Am Sor 9 1 1 1 1 1 1 1 1 1 1 1 1 1	Minimal Cut Detained seen III Unavailanty 42 File 29 Fair seen 42 Ray Rostan 42 Pape francisco Pape francisco Coder 1 2	Sets The analyse moder reach to be     11 (Prot -0) Instance of With Form made     11 (Prot -0) Instance of With Form made     11 (Prot -0) Instance of With Form made     11 (Prot -0) Instance of With Form     21 (Prot Forms     21, 27	a cand hollow additional provinties can in estimal extend astration controlled 725566-5 Constitutions (Aurenteen) 725566-5 (225566-10 H H H H H H H H H H H H H H H H H H H	6 Masses reg 1 (6) 6 * (1) amage 27359 (0.1) (0.2)	6 demage fight one 1 600 200-17	A Car an order unlimed Remote of a sites 174 Worst Care Profestolity 126-16	Importance 1.60(E)05523(51184662-8
Per Copper From Am Ser	Minimal Cut Desared Frent IIIL Unavelently 42 Rev 1001	Sets         The analysis moder results to be 111 (1914) - E initiation of With from nach 114 (2014)           United and the initiation of With from nach 114 (2014)         Area per fire (result) 7.           2228/23.4 /r 2228/23.4 /r         Area per fire (result) 7.           EXECUTIVE To Compare the (result) 7.         Area per fire (result) 7.           228/23.4 /r         Area per fire (result) 7.           EXECUTIVE To Compare the (result) 7.         Area per fire (result) 7.           228/23.4 /r         Area per fire (result) 7.           EXECUTIVE To Compare the (result) 7.         Area per fire (result) 7.           EXECUTIVE To Compare the (result) 7.         Area per fire (result) 7.           EXECUTIVE To Compare the (result) 7.         Area per fire (result) 7.	cond before additional ensembles can be schedul     extend additions consciencial     725566-9     Torontalianty (Augmenter)     725566-9     Forest of Cat Set     12(2) Weehead Wee Sout To -20 VICC	0 Kountmy 1 6 0 K* (Disease 7755) 007 107-16	is Jamage Right size ( 16.10) w(D) 20(-37)	h Carsen bran selenced Remote of carses 574 Worst Care Protectiny 126-16	Importance 1 400055525(3136466-8
Par Coppet Fram. Am Ser           Par Ser           Par Ser           Par Ser           Par Ser Coppet To Am Ser	Minimal Cat     Descend over IIII     Overalized y 42     Pro 2.9     Aux cord 42     Pro 4     Pro 4     Pro 4     Pro 4     Pro 4     P	Sets. The analyse moder sends to be     11 (1111-4) initiation of With from Inacion     114(82)-9     114(82)-9     114(82)-9     114(82)-9     114(82)-9     114(82)-9     114(82)-9     114(82)-9     114(82)-9     114(82)-9     114(82)-9     114(82)-9	cond before additional encountre can in edited encod additional constraints (20086-5) Unreliations (Augmenters) (20086-5) Ve <sup>+</sup> Aug per lin	0 Kountmel (6 0 e <sup>n</sup> (7) sense 2755 (0) 5 1000 1000 1000 1000 1000 1000 1000 10	86-10. 6 Annage Right size 1 w(T) 2.0(-1)7 2.4195/982-11	A Car an oran selement Remote of car sets 724 Worst Care Protocolity 1.25-16 1.2099335-10	Importance 1.4053552351136466 8 0.0154401403665377191
Per Conjust from Adm Sar         Improved (this throw Tar)           Improved (this throw Tar)         Improved (this throw Tar)           Improved (this throw Tar)         Improved (this throw Tar)           Improved (throw Tar)         Improved (this throw Tar)           Improved (throw Tar)         Improved (throw Tar)	Minimal Cut     Enduard event III     Underland vent III     Underland vent III     Underland vent III     Ric 2a     Arx com 52     Lary Reaction 52     Pryce test test     Code     1 2     2 3	Sets The analyse moder sends to be     11 (Third-E Instance of With Free Sector     174825-9	cond before additional encounter can in edited edited and additional encounter (200568-6) (200568-6) (200568-7) (2005	δ. δλακτις τημη [ 16]           φ = """ (Π) καταχώρ 27353           Q(T)           (QC-16)           1.2099338-10	65-10 6 Jonniger Right sine 1 W(T) 20(-37 2.4195796-13	K Cat we down wellmood     Kumper of our years 178     Woost Care Productiny     T26-16     1.2099136-10	Importance 1.60836553361184667-8 0.5194601420683177191
Per Capel Frank Am Se Per Capel Frank Am Se Per 2000 8 A Fail 82020.7 For Used A Fail 82020.7 For Used A For Used A Fo	Minimal Cut     Industrial Cut     Industrial Cut     Industrial     Industri     Industrial     Industria	Sets The analyse moder reach to be     Internet and the internet of UNIT from match     Internet     Inter     Internet     Internet     Internet     Internet     Internet	conditional additional proceedings can be addited and additional additional proceedings     (20086-9)     (Exemption Call Section 2019 (Machinese 2019586-7)     (2019)	Adams(rmg)         65           0         4"         (1) annual 27752	86-19. 8 Jamage Right care 1 46-19. 2.0(-17) 2.4193/986-11	A Cet is clear withinged Number of ect any 174 Woost Case Probability 1.05-16 1.2099335-10	Importance 1.600305523651364662-9 0.05194601425663177191
Per Capel From Am Ser	Minimal Cut      Industry 2     Provide the second se	Sets The analyse moder reach to be     11 (Phil-4) Instance of With Fore reach     11 (Phil-4) Instance of With Fore reach     11 (Phil-4)     Constant of With Fore reach     Constant of the set of the se	a candi belima additional anomenia carrier estimat activat association controllers) 725566-9 torentationary (Australianty (Australianty (275556-7 725566-7) «* Aug, gai Thi (Australianty 725556-7 (27556-7) «* Aug, gai Thi (Australianty 725556-7 (2757) (Minhead) Wei Short To -32 VCC (277) (Minhead) Wei Short To -32 VCC (377) (Mi	0         Maximum (mmg)         60           0         x*         (f) Anneque 77752           10         x*         (f) Anneque 77752 <td>86-10 6 Jamage Right care 1 46-11 200-17 2.00-17 2.4180525-10</td> <td>A         Get ten torsen unlimited           Nomen of not sen.         124           Worst Care Probability         126-16           1.2099335-10         1209336-9</td> <td>Importance 1.600305525651364666 0.5194604256853177191 0.1945055285527366685</td>	86-10 6 Jamage Right care 1 46-11 200-17 2.00-17 2.4180525-10	A         Get ten torsen unlimited           Nomen of not sen.         124           Worst Care Probability         126-16           1.2099335-10         1209336-9	Importance 1.600305525651364666 0.5194604256853177191 0.1945055285527366685
Per Conjust From. Am Sin           Per Conjust From. Am Sin           Per Conjust From. Am Sin           Per System           Per Sys	Minimal Cut     Industry 42     Proceedings     Annone 62     Proceedings     Annone 62     Proceedings	Sets         The analyse moder results to be 111(701-0) initiation of W21 from mode 114(82)-0           Marcal analysis         Area per fits (result); 7, 228/21-9           Op of forems         23, 27           H1, 216, 216         H1, 216, 216	cond before additional encounter can in sched encod analysis additional encounter of the scheduler T25586-9 T25586-9 T25586-9 Event of Cat Set Cond Set Cond Cond Set Cond Co	0         Masser(smg1         Mas	86-10. 10 January Right Song 1 201-17 24195786-13 24190025-19	Monte characteristic and an and a set of a set o	Importance 14.00045525451364662-3 0.0194401420683177197 0.194505128527366485
Per Corpus From Arm Sar         IP Thermody them Shows Tor           IP         30         IP Thermody them Shows To	Minimal Cut      Industry 42     Industry 42     Reg 22     Ann control (11)     Ordenized Year     Reg 22     Ann control (42     Propertiese text      Propertiese text      Orden      I     2     3     3     3	Sets The analyse moder sends to be     11 (111) -	cond before additional encounter can in sched encod addition conscience T25586-9     Conscience (Conscience) T25586-9     encode (Conscience) Events of Cot Set Conscience (Cot Set Conscience) Conscience (Cot Set Cot Set	0         Mountmell 65           0         6"           0         6"           0         7.153           0         6"           0         6.15           1.2099381-90           1.2099381-91	65-10 6 January Right care 1 96-10 200-37 24190786-13 24190286-13 24190286-13	N         Cat we clean wellmood           Number of our sets         174           Worst Care Probability         126-16           1.2093136-10         1.2093136-9           1.2093136-12         1.2093136-12	Importaince 1600/05/2383136466-8 0.0194601436683177197 0.194505128527566685

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.