Beyond Traditional Methods: Why Model-Based Systems Engineering is a Game-Changer for Safety Analysis

Kate Kovalovsky

18 October 2023

NDIA 26th Annual Systems & Mission Engineering Conference

AN ARCFIELD COMPANY

Approved for Public Release

Introduction

How does Model-Based Systems Engineering improve Safety analysis?

Which metrics can summarize system safety information?

How can Safety experts get the most out of MBSE?

**When integrated in an MBSE environment,
safety information can influence system design earlier in the lifecycle**

Purpose

Provide a concrete example of how experts from Safety and Systems Engineering domains can **work collaboratively** during system development to **proactively inform system design using MBSE**

Agenda

- Roles & Collaboration
- Model-Based Analysis Profile for Defense Safety
- Safety Analysis Metrics
- Conclusion

Roles and Collaboration

AN ARCFIELD COMPANY

Teamwork is Key

AN ARCFIELD COMPANY

Not doing MBSE? (yet)

The barrier to entry isn't as high as you may think

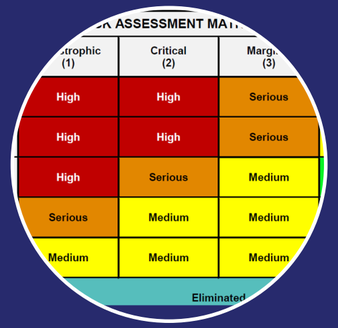
Today's Main Message:

Not everyone needs to know everything:

Safety and SE can work collaboratively to achieve success using MBSE

Teaming with experts in MBSE can provide the same benefits without the pressure of having to learn it all yourself!

Roles

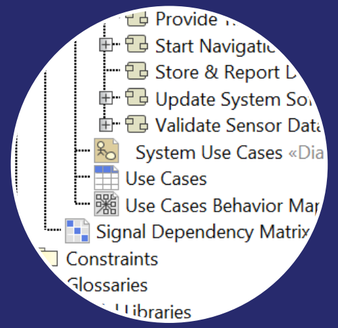


Safety Experts

Handle MIL-STD-882 Analyses

Provide “raw” data to SE

Refine analyses iteratively



Systems Engineers

Integrate safety into model

Analyze impacts

Provide feedback loop

Influence Design Together

Benefits of a Model-Based Approach

Increase opportunities for safety to proactively inform system design

- Safety can be “baked in”, not “bolted on”, as an integrated part of design throughout lifecycle
- The model captures key information about safety analysis to inform design
- Safety information can be traced across requirements, functionality, design, and verification elements
- Safety information evolves with system model
- History of safety decisions, rationale, and impacts tracked in line with system information
- Opens the door for Safety and Reliability to collaborate within model MBSE (less stove piping)
- Aligns with Risk Assessment and Software Safety Criticality Matrices from MIL-STD-882
- Users enter information and model automatically returns results (saves time, no errors)
- Enables metrics to be tracked throughout system lifecycle
- Can exchange data to/from Excel – Not everyone needs to be “in” the model to use the information within

Model-Based Analysis Profile for Defense Safety

AN ARCFIELD COMPANY

Approved for Public Release

Hazard & Risk Analysis

- Hazards can be rated according to the Risk Assessment Matrix directly in the model
- RAC values are automatically returned
- Enter for Initial, Current, and Final posture

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Risk Assessment Code (RAC): High Serious Medium Low Eliminated

Safety ID	Name	Severity	Safety Result	Probability Level Initial	Initial Risk Level	Probability Level Current	Current Risk Level	Probability Level Final	Final Risk Level
SC-50	Delete Recorded Data	Level IV: Negligible	Not Safety Significant	Level D: Remote	Low	Level E: Improbable	Low	Level F: Eliminated	Eliminated
SC-51	Download Recorded Data	Level IV: Negligible	Not Safety Significant	Level D: Remote	Low	Level E: Improbable	Low	Level F: Eliminated	Eliminated
SC-52	Initialize the System	Level II: Critical	Safety Critical	Level C: Occasional	Serious	Level E: Improbable	Medium	Level F: Eliminated	Eliminated
SC-53	Initiate Built-In Test	Level III: Marginal	Safety Related	Level C: Occasional	Medium	Level D: Remote	Medium	Level F: Eliminated	Eliminated
SC-54	Initiate System Shutdown	Level II: Critical	Safety Critical	Level B: Probable	High	Level C: Occasional	Serious	Level E: Improbable	Medium
SC-55	Load Cryptographic Keys	Level III: Marginal	Safety Related	Level C: Occasional	Medium	Level E: Improbable	Medium	Level F: Eliminated	Eliminated
SC-56	Initiate INS Alignment	Level II: Critical	Safety Critical	Level D: Remote	Medium	Level D: Remote	Medium	Level F: Eliminated	Eliminated

Software Analysis

- Enter information based on Software Safety Criticality Matrix
- Model automatically returns SwCI
- Can enter Partitioning information & Level of Rigor (LoR) Status also

SOFTWARE SAFETY CRITICALITY MATRIX				
	SEVERITY CATEGORY			
SOFTWARE CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

SwCI	Level of Rigor Tasks
SwCI 1	Program shall perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.
SwCI 2	Program shall perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SwCI 3	Program shall perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SwCI 4	Program shall conduct safety-specific testing.
SwCI 5	Once assessed by safety engineering as Not Safety, then no safety specific analysis or verification is required.

Name	Severity	SW Safety Result	SWControlCategory	Sw CI Calc	Partitioned	Partitioned Status	Status
Execute Periodic Built-In Test	Level II: Critical	Safety Critical	1Autonomous	SwCI1	true	Yes	Partially Met
Generate and Route Precision Time Outputs	Level II: Critical	Safety Critical	1Autonomous	SwCI1	true	Yes	Partially Met
Generate Download Status	Level IV: Negligible	Not Safety Significant	4Influential	SwCI4	false	N/A	Not Met
Generate IBIT Options Message	Level IV: Negligible	Not Safety Significant	2SemiAutonomous	SwCI4	false	N/A	Partially Met
Generate Sensor Capability Status Request	Level II: Critical	Safety Critical	3RedundantFaultTolerant	SwCI3	true	Yes	Partially Met
Generate software status	Level II: Critical	Safety Critical	2SemiAutonomous	SwCI2	true	Yes	Partially Met
GPS Signal Acquisition	Level II: Critical	Safety Critical	1Autonomous	SwCI1	true	Yes	Not Met
Initialize Periodic Built-in Test	Level III: Marginal	Safety Related	1Autonomous	SwCI3	false	N/A	Not Met

Safety Analysis Metrics

AN ARCFIELD COMPANY

Sample Project and MBSE Environment

AN ARCFIELD COMPANY

For presentation purposes, the profile and metrics were applied to a fictitious system

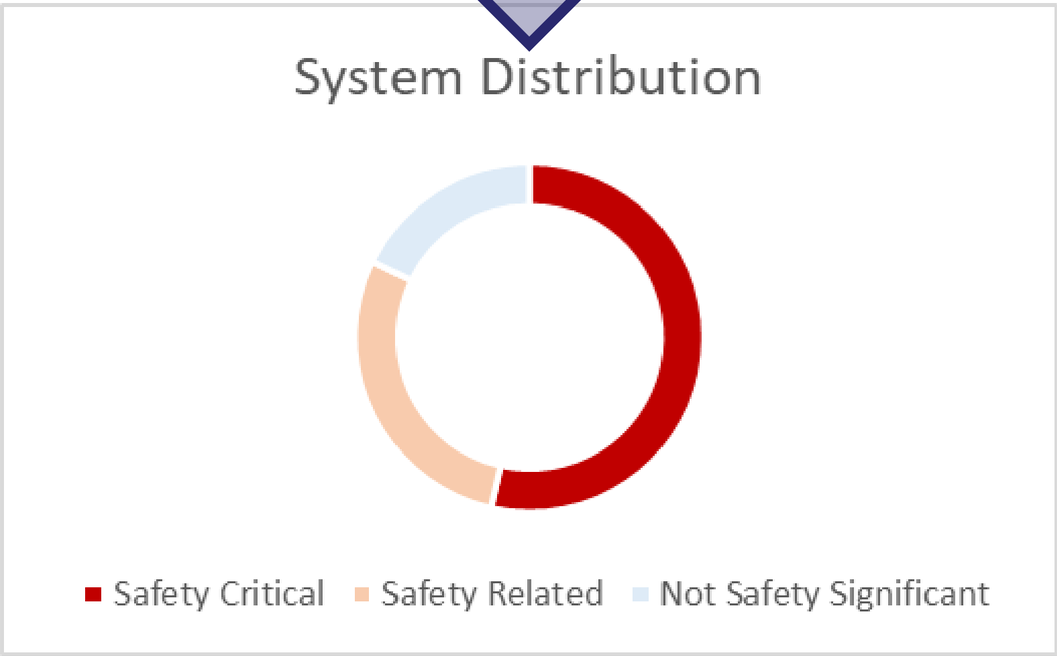
Can be applied to any MBSE / Systems Modeling Language (SysML) based effort

Validation-Based Metric Suites

- Validation suites in Cameo Systems Modeler provide a way of evaluating a set of data (model) against a specific expression
  - Helpful for consistency and quality checks
- Metric suites can summarize the counts and percentages of the validation results
- In this application, metric suites provide insight into the safety posture of a system
- Metric suites output to tables in Cameo
- Further visualization is done using Microsoft Excel

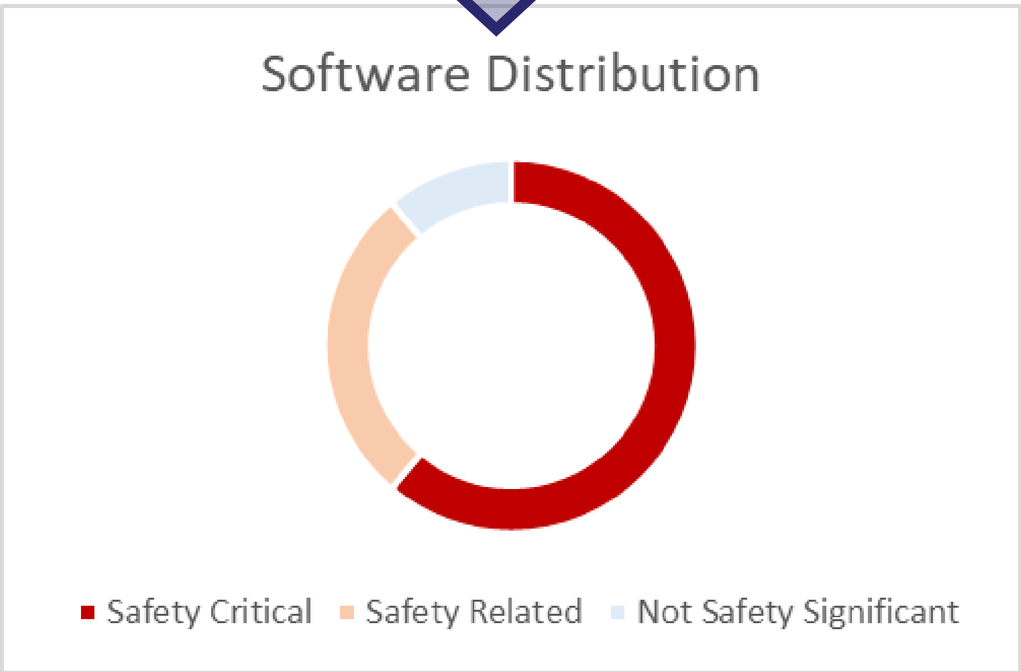
Distribution of System Level Functionality

Name	Safety Critical System Count	Safety Critical System Percentage	Safety Related System Count	Safety Related System Percentage	NSS System Count	NSS System Percentage
System Alpha	15	53.5714	8	28.5714	5	17.8571



Distribution of Software Functionality

Name	Safety Critical Software Count	Safety Critical Software Percentage	Safety Related Software Count	Safety Related Software Percentage	NSS Software Count	NSS Software Percentage
System Alpha	22	61.1111	10	27.7778	4	11



Risk Mitigation Across Lifecycle (1/2)

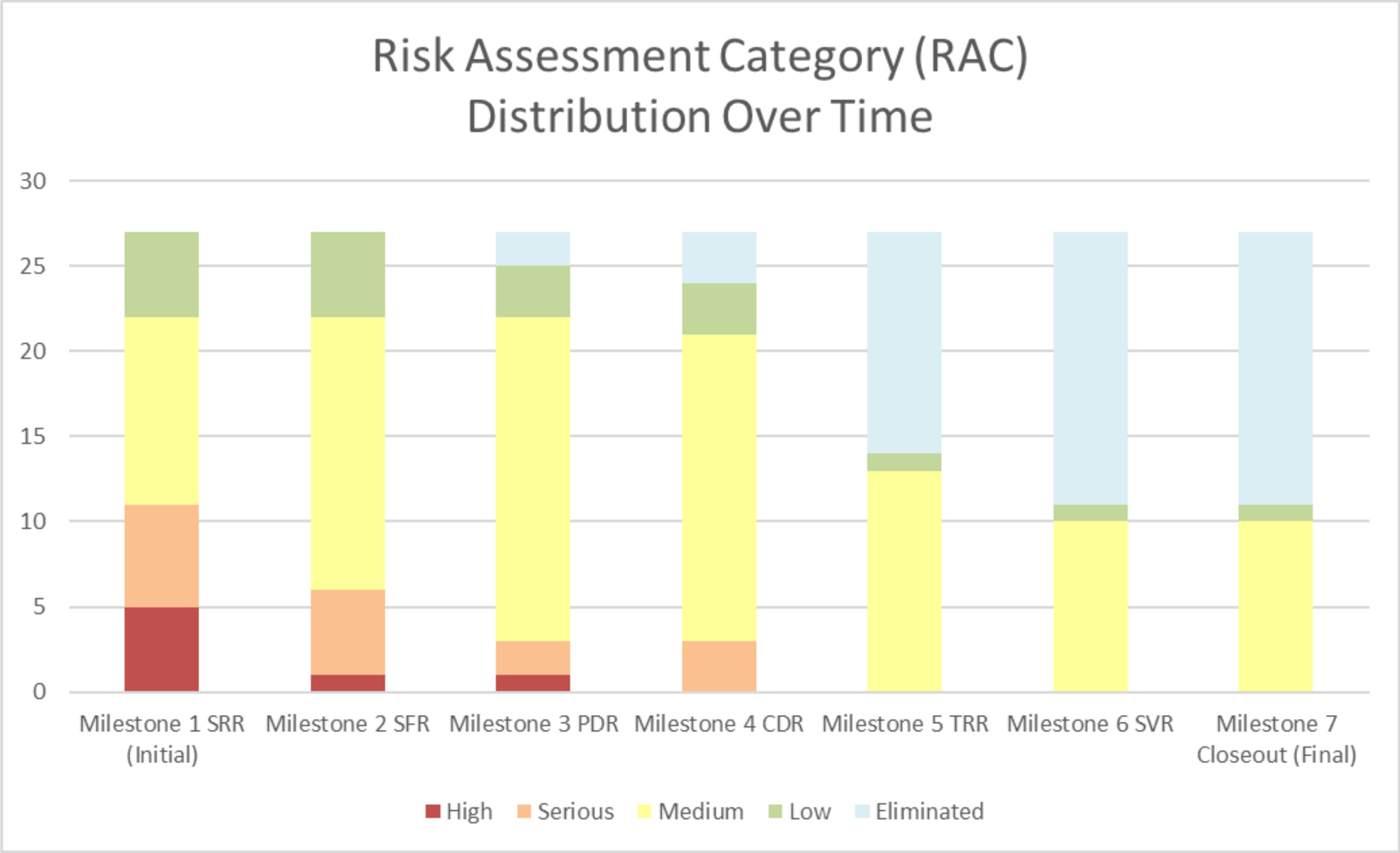
AN ARCFIELD COMPANY

Risk Assessment Code (RAC): High Serious Medium Low Eliminated

Safety ID	Name	Severity	Safety Result	Probability Level Initial	Initial Risk Level	Probability Level Current	Current Risk Level	Probability Level Final	Final Risk Level
SC-50	Delete Recorded Data	Level IV: Negligible	Not Safety Significant	Level D: Remote	Low	Level E: Improbable	Low	Level F: Eliminated	Eliminated
SC-51	Download Recorded Data	Level IV: Negligible	Not Safety Significant	Level D: Remote	Low	Level E: Improbable	Low	Level F: Eliminated	Eliminated
SC-52	Initialize the System	Level II: Critical	Safety Critical	Level C: Occasional	Serious	Level E: Improbable	Medium	Level F: Eliminated	Eliminated
SC-53	Initiate Built-In Test	Level III: Marginal	Safety Related	Level C: Occasional	Medium	Level D: Remote	Medium	Level F: Eliminated	Eliminated
SC-54	Initiate System Shutdown	Level II: Critical	Safety Critical	Level B: Probable	High	Level C: Occasional	Serious	Level E: Improbable	Medium
SC-55	Load Cryptographic Keys	Level III: Marginal	Safety Related	Level C: Occasional	Medium	Level E: Improbable	Medium	Level F: Eliminated	Eliminated
SC-56	Initiate INS Alignment	Level II: Critical	Safety Critical	Level D: Remote	Medium	Level D: Remote	Medium	Level F: Eliminated	Eliminated

Name	Initial High Count	Current High Count	Final High Count	Initial Serious Count	Current Serious Count	Final Serious Count	Initial Medium Count	Current Medium Count	Final Medium Count	Initial Low Count	Current Low Count	Final Low Count	Initial Eliminate Count	Current Eliminated Count	Final Eliminated Count
Milestone 1 SRR	5	5	0	6	6	0	11	11	11	5	5	1	0	0	15
Milestone 2 SFR	5	1	0	6	5	0	11	16	11	5	5	1	0	0	15
Milestone 3 PDR	5	1	0	6	2	0	11	19	11	5	3	1	0	2	15
Milestone 4 CDR	5	0	0	6	3	0	11	18	11	5	3	1	0	3	15
Milestone 5 TRR	5	0	0	6	0	0	11	13	10	5	1	1	0	13	16
Milestone 6 SVR	5	0	0	6	0	0	11	10	10	5	1	1	0	16	16
Milestone 7 Closeout	5	0	0	6	0	0	11	10	10	5	1	1	0	16	16

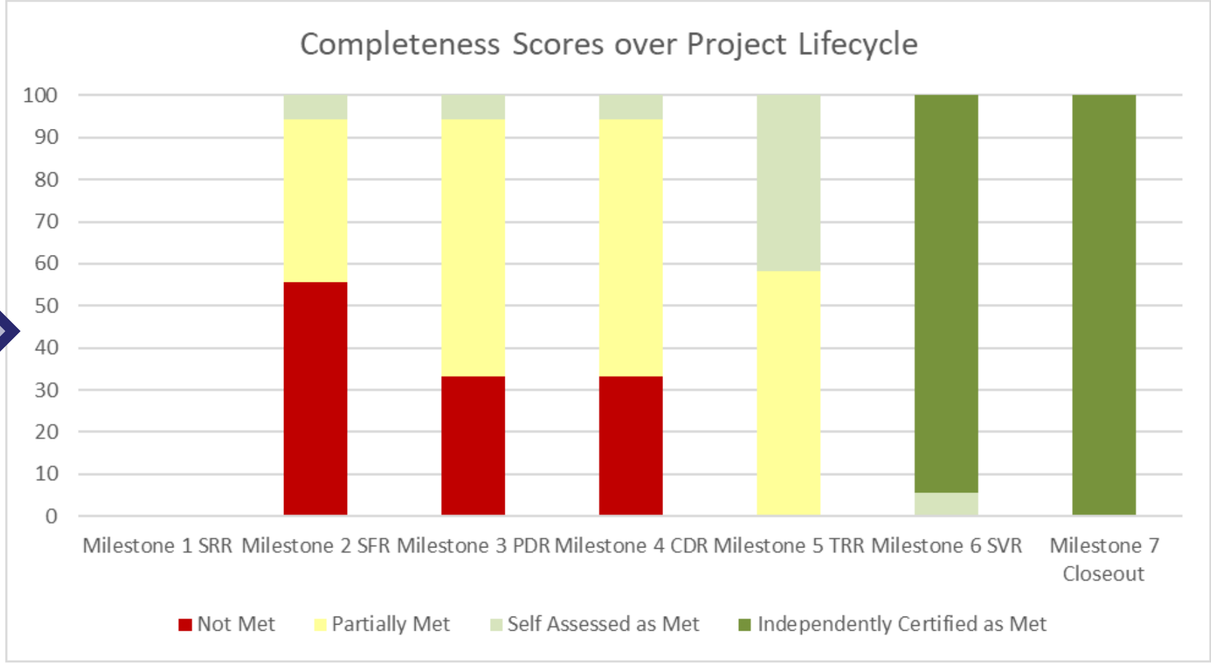
Risk Mitigation Across Lifecycle (2/2)



Software Level of Rigor Completeness

Shows progress toward meeting Level of Rigor requirements

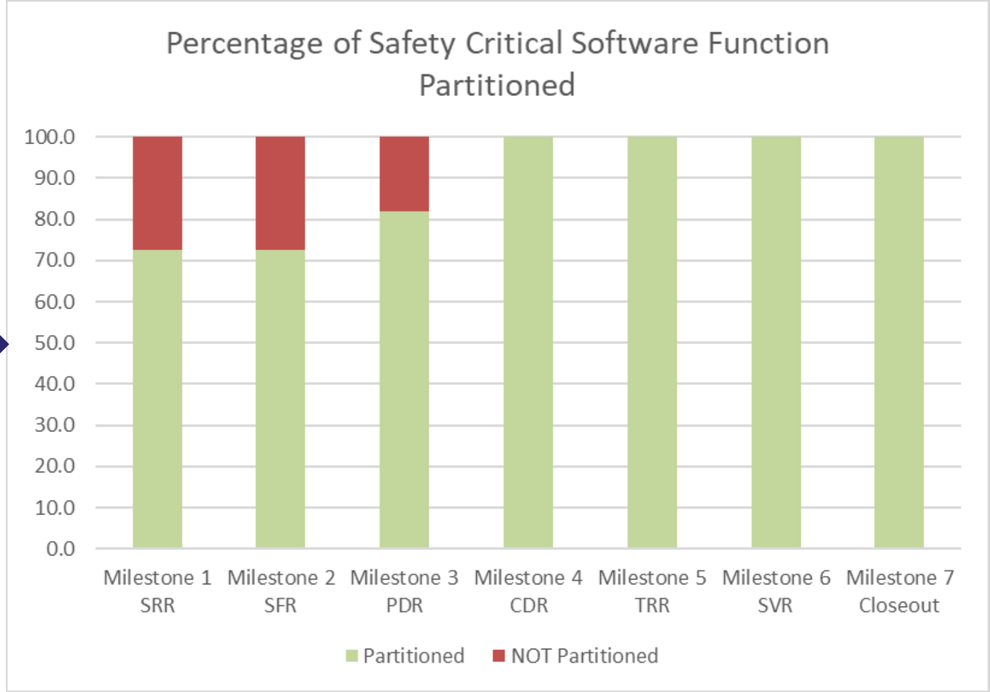
#	Name	Completeness Not Met Percentage	Completeness Partially Met Percentage	Completeness Self Assessed As Met Percentage	Completeness Independently Certified As Met Percentage
1	Milestone 1 SRR	0	0	0	0
2	Milestone 2 SFR	55.5556	38.8889	5.5556	0
3	Milestone 3 PDR	33.3333	61.1111	5.5556	0
4	Milestone 4 CDR	33.3333	61.1111	5.5556	0
5	Milestone 5 TRR	0	58.3333	41.6667	0
6	Milestone 6 SVR	0	0	5.5556	94.4444
7	Milestone 7 Closeout	0	0	0	100



Safety-Critical Partitioning Percentage

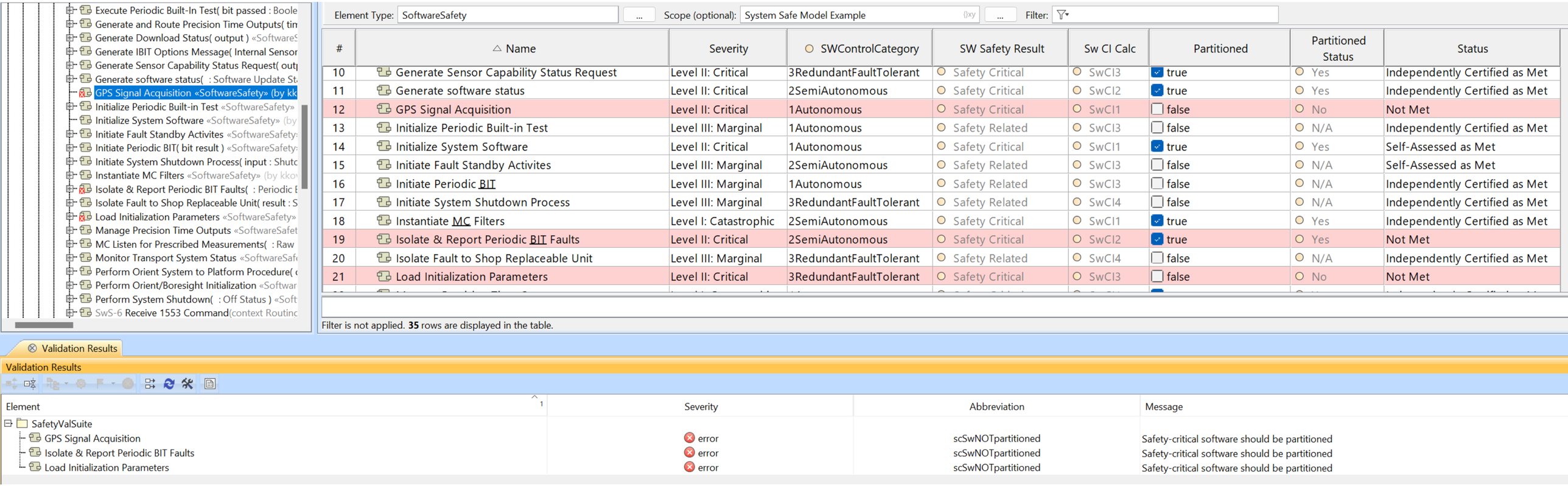
Safety-critical software should be partitioned away from non-safety-critical software

Name	Safety Critical Software Partitioned Percentage	Safety Critical Software NOT Partitioned Percentage
Milestone 1 SRR	72.7273	27.2727
Milestone 2 SFR	72.7273	27.2727
Milestone 3 PDR	81.8182	18.1818
Milestone 4 CDR	100	0
Milestone 5 TRR	100	0
Milestone 6 SVR	100	0
Milestone 7 Closeout	100	0



Error Checking

Software that should be partitioned, but isn't, will get flagged in the model:



#	Name	Severity	SWControlCategory	SW Safety Result	Sw CI Calc	Partitioned	Partitioned Status	Status
10	Generate Sensor Capability Status Request	Level II: Critical	3RedundantFaultTolerant	Safety Critical	SwCI3	true	Yes	Independently Certified as Met
11	Generate software status	Level II: Critical	2SemiAutonomous	Safety Critical	SwCI2	true	Yes	Independently Certified as Met
12	GPS Signal Acquisition	Level II: Critical	1Autonomous	Safety Critical	SwCI1	false	No	Not Met
13	Initialize Periodic Built-in Test	Level III: Marginal	1Autonomous	Safety Related	SwCI3	false	N/A	Independently Certified as Met
14	Initialize System Software	Level II: Critical	1Autonomous	Safety Critical	SwCI1	true	Yes	Self-Assessed as Met
15	Initiate Fault Standby Activites	Level III: Marginal	2SemiAutonomous	Safety Related	SwCI3	false	N/A	Self-Assessed as Met
16	Initiate Periodic BIT	Level III: Marginal	1Autonomous	Safety Related	SwCI3	false	N/A	Independently Certified as Met
17	Initiate System Shutdown Process	Level III: Marginal	3RedundantFaultTolerant	Safety Related	SwCI4	false	N/A	Independently Certified as Met
18	Instantiate MC Filters	Level I: Catastrophic	2SemiAutonomous	Safety Critical	SwCI1	true	Yes	Independently Certified as Met
19	Isolate & Report Periodic BIT Faults	Level II: Critical	2SemiAutonomous	Safety Critical	SwCI2	true	Yes	Not Met
20	Isolate Fault to Shop Replaceable Unit	Level III: Marginal	3RedundantFaultTolerant	Safety Related	SwCI4	false	N/A	Independently Certified as Met
21	Load Initialization Parameters	Level II: Critical	3RedundantFaultTolerant	Safety Critical	SwCI3	false	No	Not Met

Conclusion

AN ARCFIELD COMPANY

Conclusion

- Safety Experts and Systems Engineers should collaborate within an MBSE environment
- Increased opportunities to proactively inform system design toward more safe systems
- Systems Modeling Language (SysML) can be extended to integrating safety analyses with systems engineering models and provide meaningful information to stakeholders
- Metrics can be evaluated against the evolving system design to give valuable insight into the hazard and software safety posture of a system

Thank you for your time - Q&A

Kate Kovalovsky
Director of MBSE Services, Strategic Technology Consulting

kkovalovsky@strattechnologies.com