Modeling Cyber Survivability:

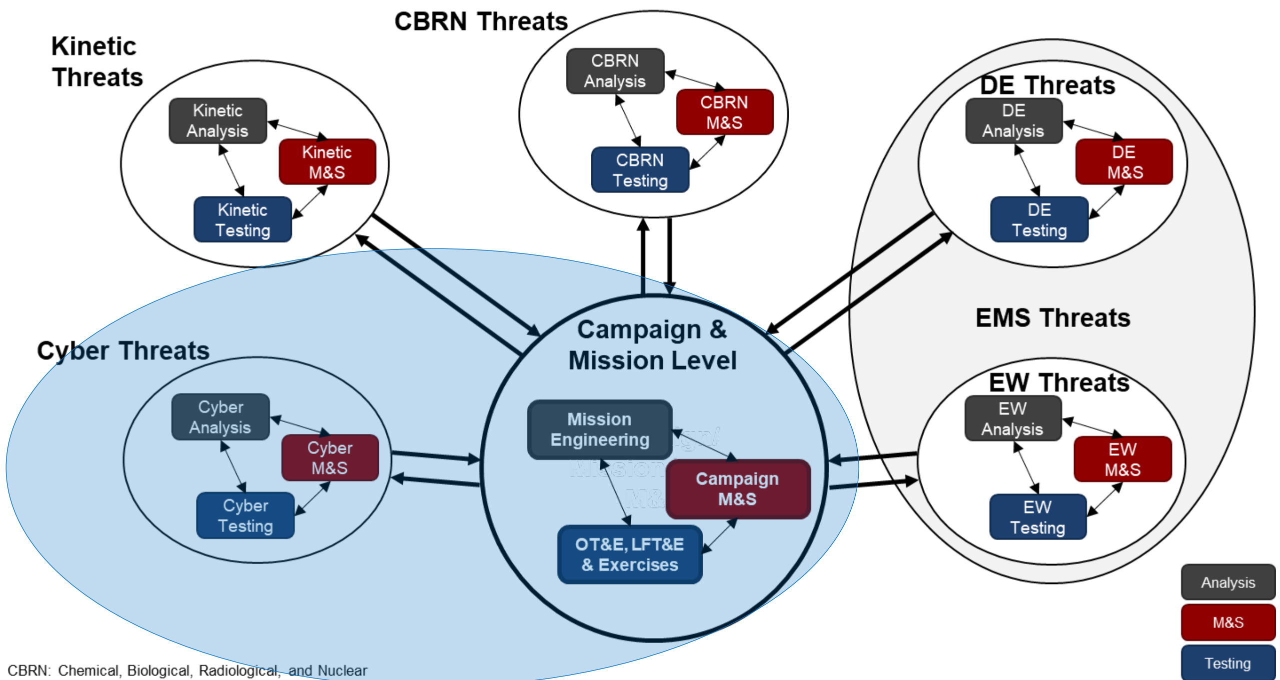
Score Small and let the Machines do the Math

Dr. Bill “Data” Bryant

8 Aug 24

Problem to be Solved

- FY22 NDAA Section 223 mandates integrated survivability testing across all threat types
- One approach is to utilize modeling and simulation as a "Universal Integrator"[1]
- The focus of this brief is on how we do that specific to cyber threats



CBRN: Chemical, Biological, Radiological, and Nuclear
DE: Directed Energy
EW: Electronic Warfare
EMS: Electromagnetic Spectrum
LFT&E: Live Fire Test and Evaluation
M&S: Modeling and Simulation
OT: Operational Test

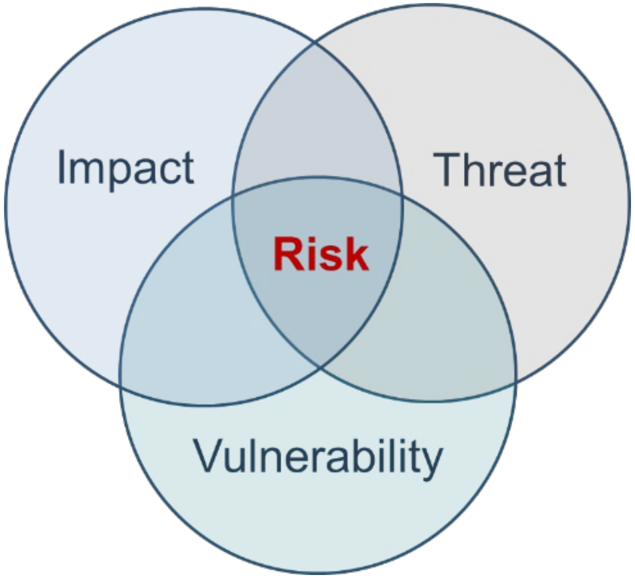
1. See Bill "Data" Bryant, Charlie Fisher, Daniel Boseman, and Juliana Ivancik "Digital Technology—a Universal Integrator—Enabling Full-Spectrum Survivability Evaluations." *Naval Engineers Journal*, Volume 136, (Spring 2024): 189-198.

Expected Mission Loss (EML)

- EML is borrowed from the financial world's Expected Financial Loss (EFL), where it has been used successfully for decades

$$\boldsymbol{EML = Likelihood\ of\ a\ Risk\ Occurring \times Mission\ Loss\ due\ to\ that\ Risk}$$

Risk scenario = story of a potential ***threat*** exploiting a ***vulnerability*** to ***impact*** a critical sub-system or component

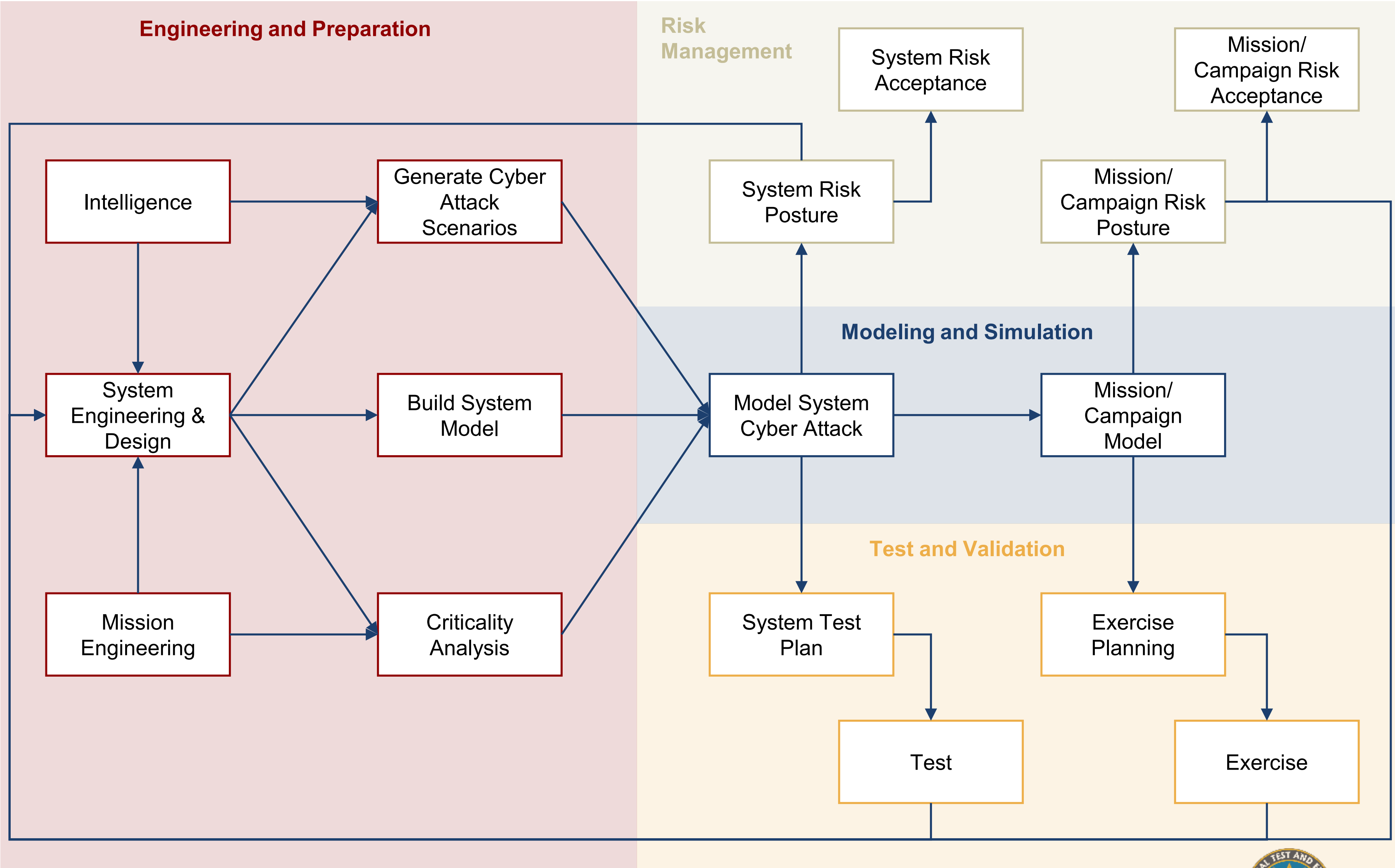


- The problem isn't the math—it's the inputs; where do they come from and how do we know they are correct?

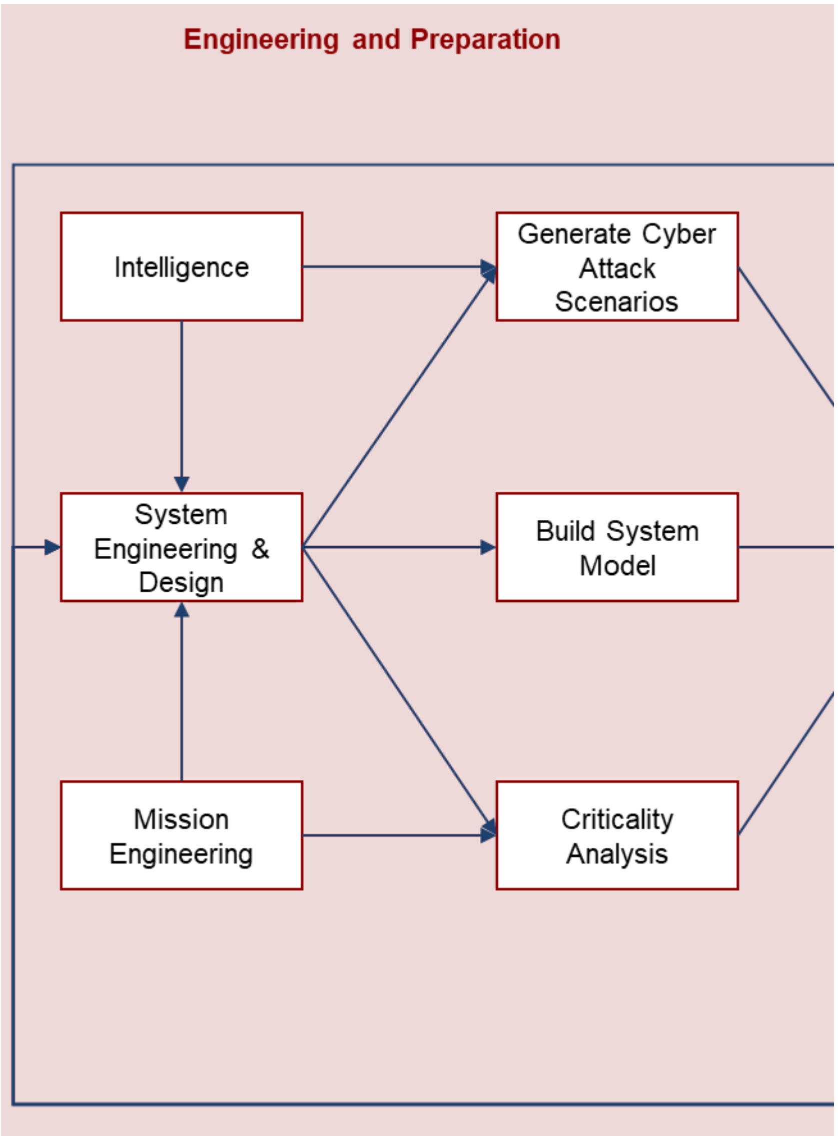
Current Methods of Measurement

- If cyber survivability is measured at all, it is most often measured in terms of an ordinal risk matrix
  - Cyber risks can be developed using a wide range of methodologies
  - Often traditional-IT vulnerability focused
  - Several degrees of separation from what we really care about—risk to mission accomplishment
- Measuring mission risk probabilistically is theoretically a better approach, but the issue of inputs becomes even more severe
  - Humans have numerous known issues generating accurate probabilities
  - Algorithms and AI have not shown any improvement over humans
  - Attack chains involve multiple steps the humans have to integrate
- **Approach: Model the attack in small discrete steps and use data for inputs whenever possible, human probabilistic assessment informed by data when not—then put into a simulation**

Cyber Survivability Measurement Process Flow



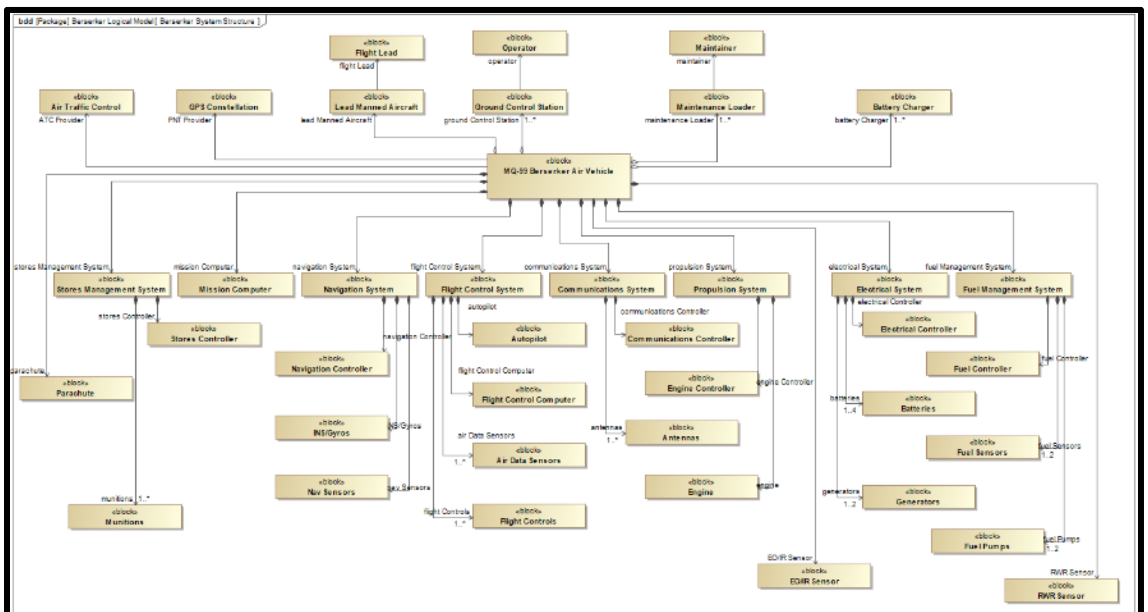
Engineering and Preparation



- Threat Intelligence is critical
- Mission engineering connects system to mission
- System design (or concept) informs system model
- Attack scenarios can be developed with numerous tools
  - MRAP-C
  - STPA-Sec
  - CTT
- Criticality analysis determines what components are most significant
  - Already part of Program Protection

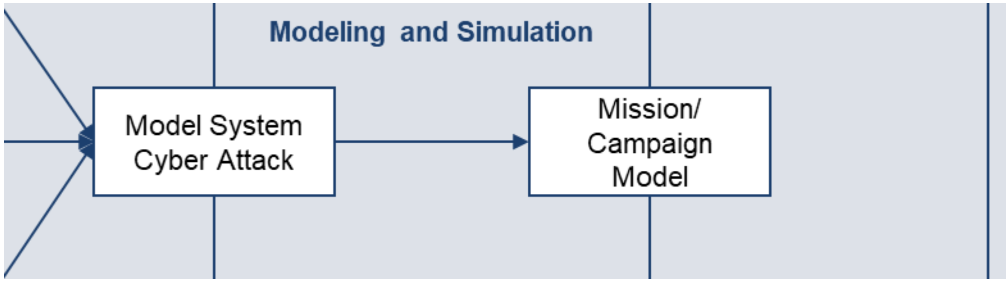
Notional Example: MQ-99 Berserker UAS

- Notional UAS at conceptual stage of design
- Any resemblance coincidental
- Basic CONOPS & architecture



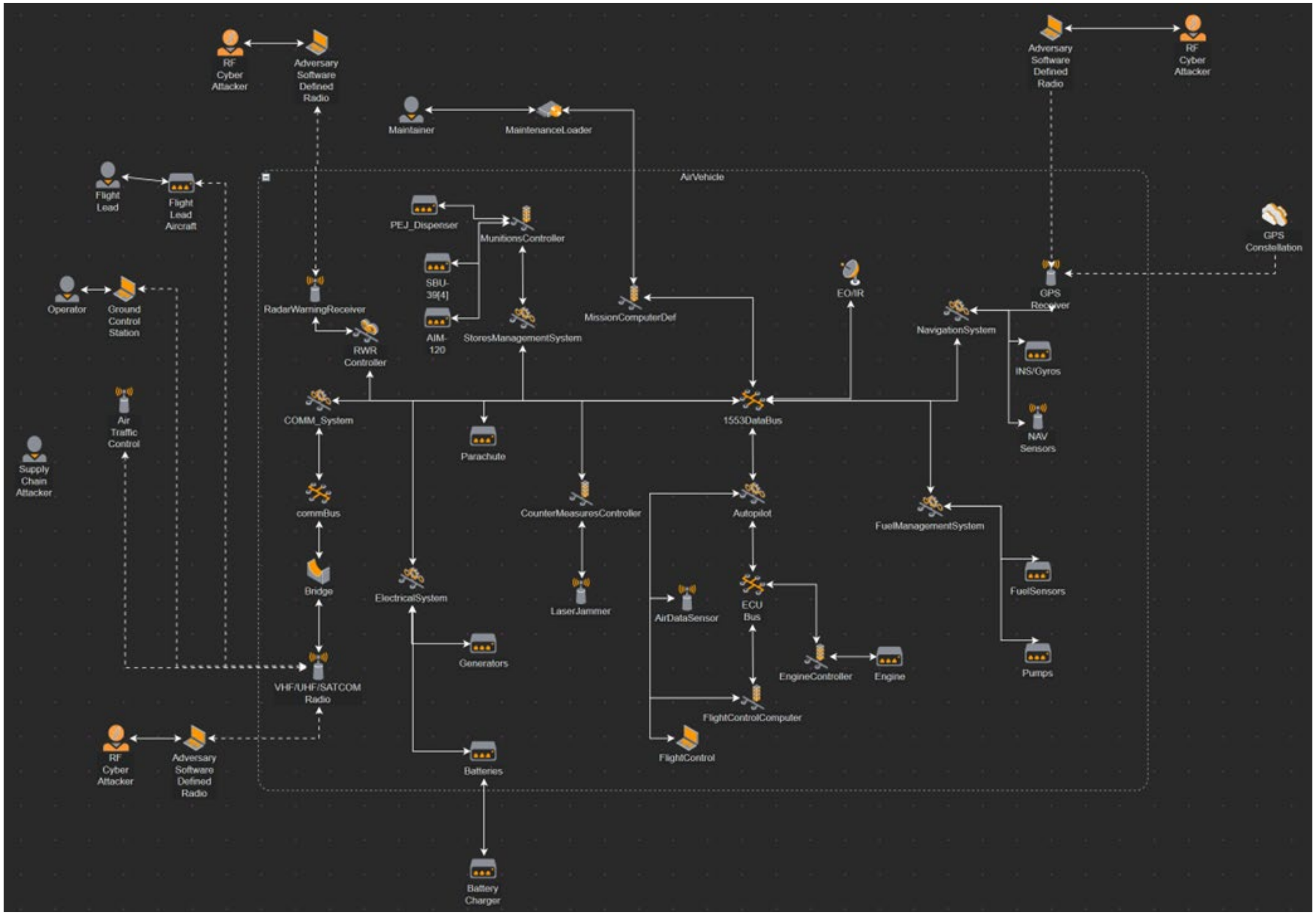
- Air-to-Air and Air-to Ground roles
- Semi-autonomous
- 2 x AMRAAM, or 6 x SDB
- Attritable

Modeling and Simulation

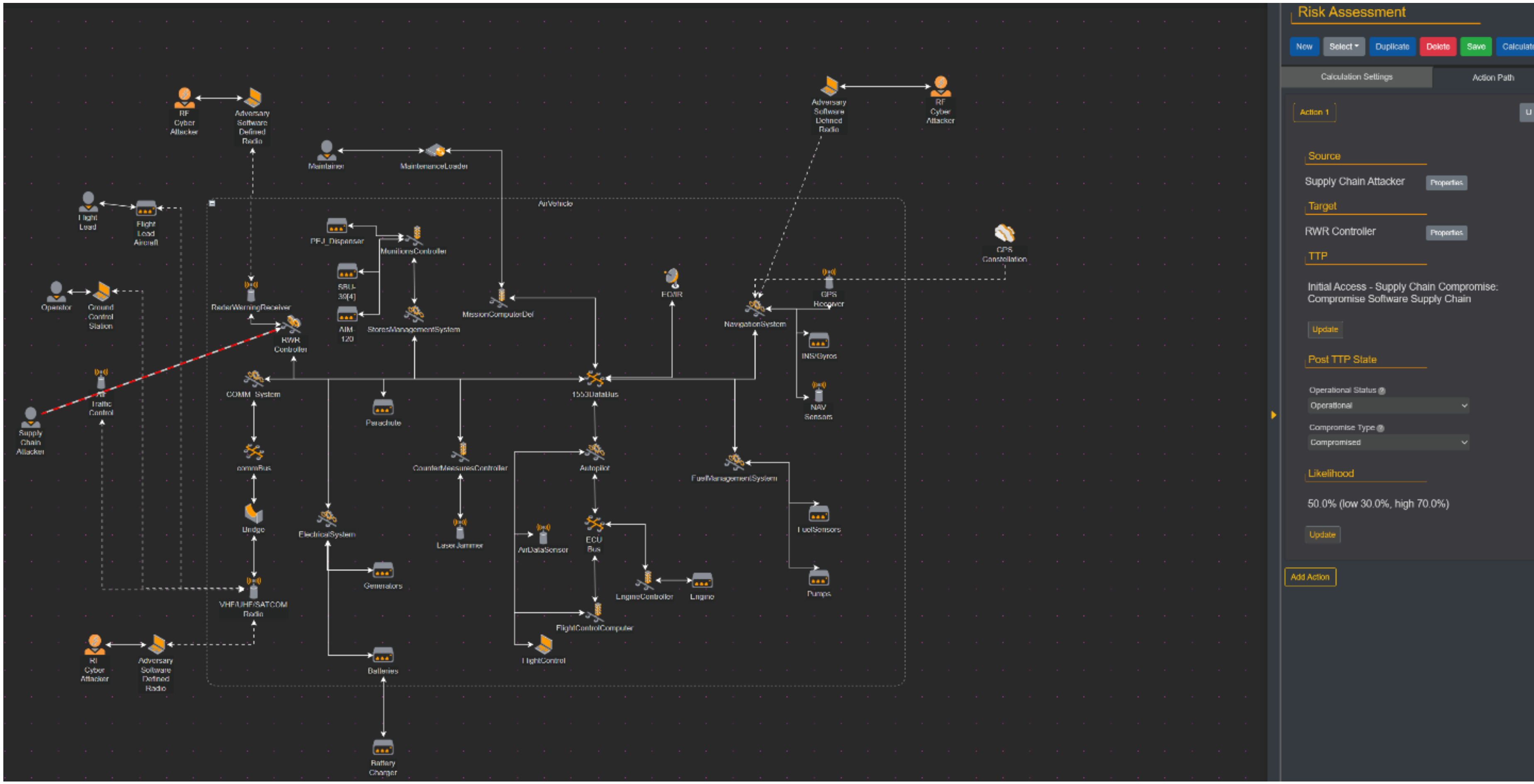


- Cyber Operations Lethality and Effectiveness (COLE) tool can model system level cyber attacks
  - Originally created for offensive attack planning on traditional-IT systems, has been expanded for modeling weapon systems by DOT&E and JASPO
  - Does not simulate data flow, but tracks component level hardware, software, and firmware down to the specific build with associated vulnerabilities
- Many different mission and campaign level simulations exist
  - Advanced Framework for Simulation Integration and Modeling (AFSIM)
  - Joint Simulation Environment (JSE)
  - Combat Forces Assessment Model (CFAM)

COLE MQ-99 Berserker System Model

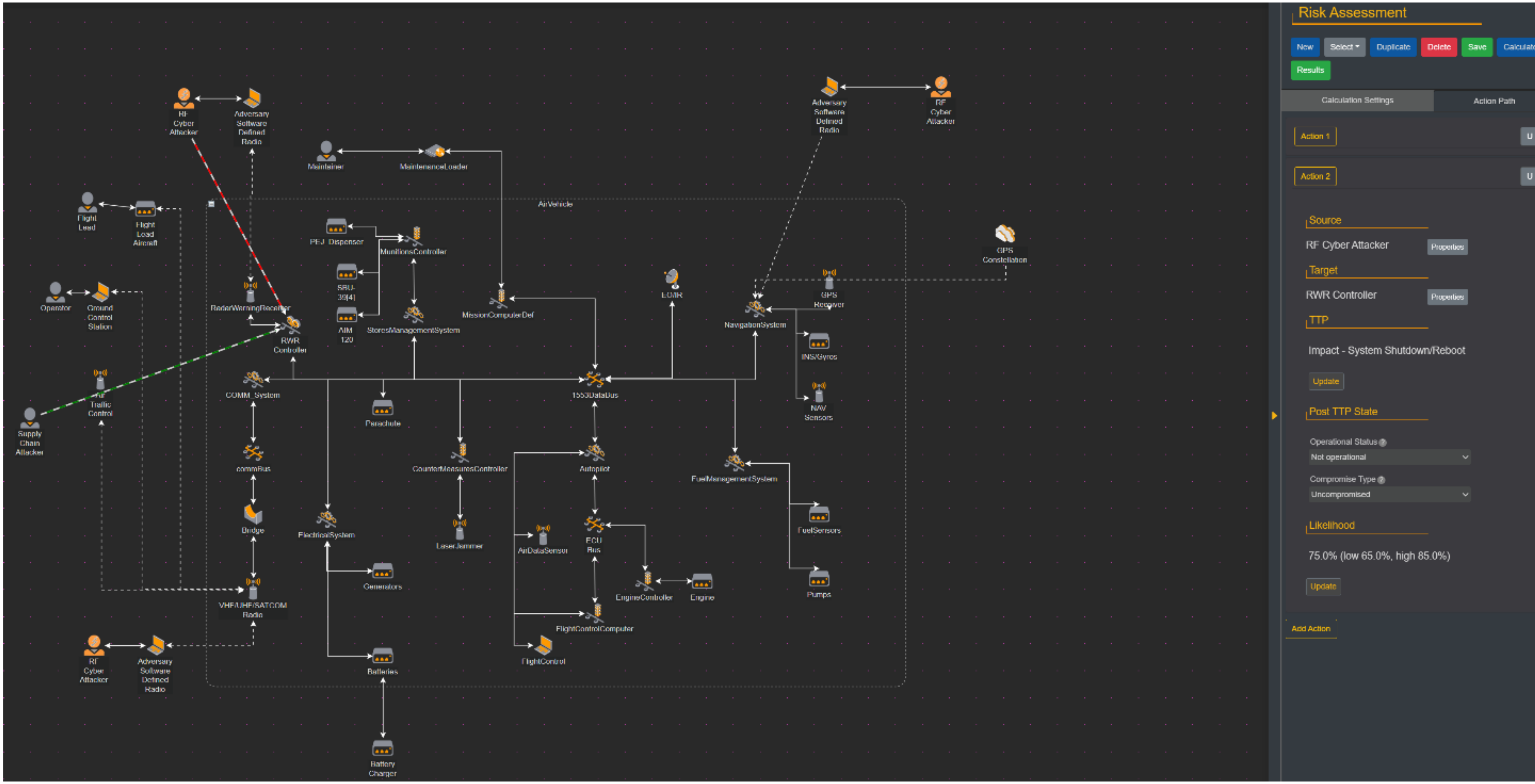


Simulated Attack Step 1—Supply Chain Attack



- Modeled as a 90% Confidence Interval (90CI) of 30-70% representing high uncertainty and high mean of 50%

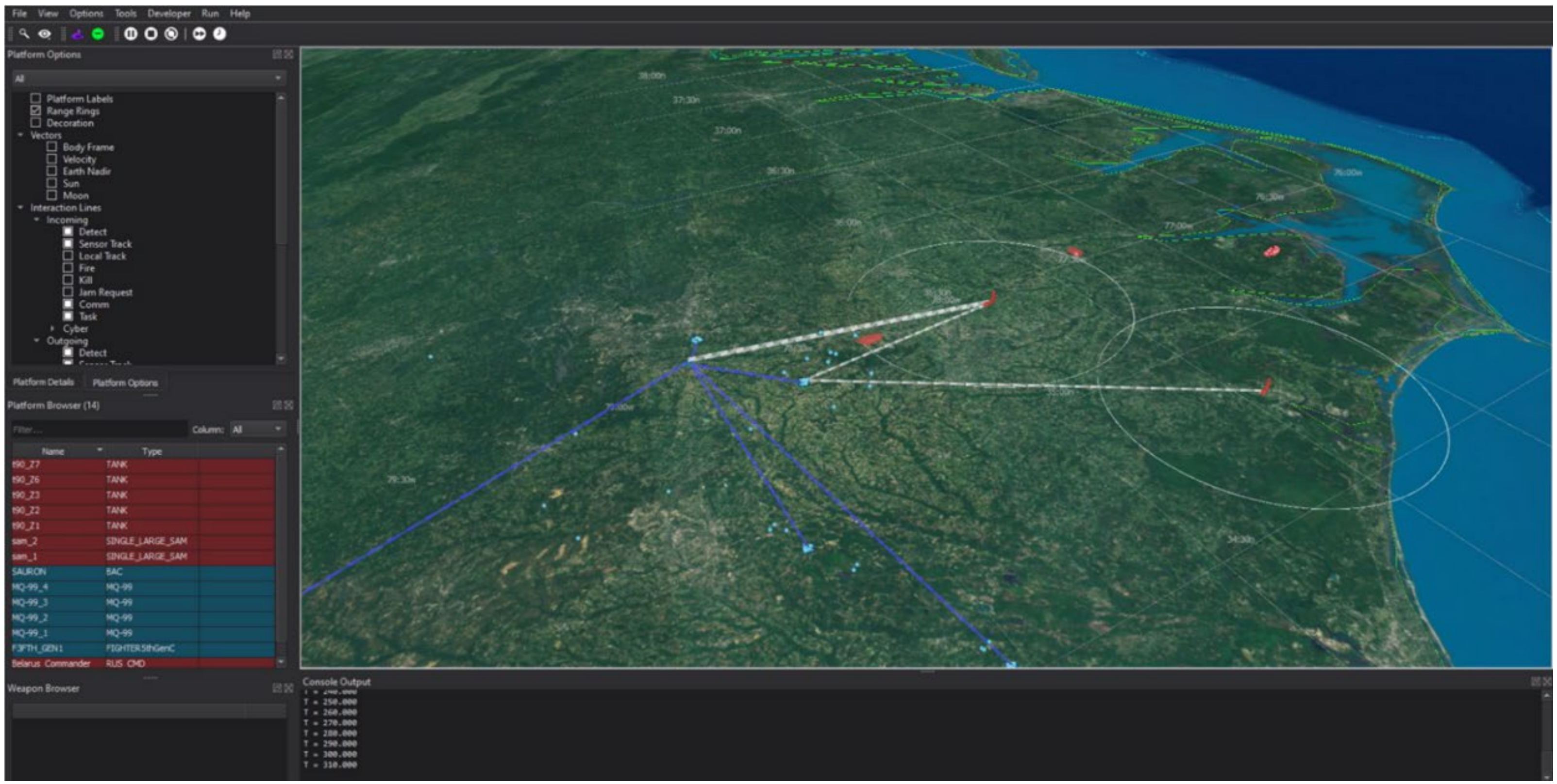
Simulated Attack Step 2—Triggered from RF



- 90CI of 65-85% for step 2 gives overall Likelihood 90CI of 21.9% to 53.1% with a mean of 37.4%

Baseline AFSIM Berserker Scenario

- 4 x Berserkers being controlled by an F-35, 2 x Berserkers attacking targets within a defended area with Small Diameter Bombs



AFSIM Berserker Scenario Results

- 50 Monte Carlo Baseline runs were done using the Full Spectrum Survivability Toolkit (FSST)[2]
- On average, 4.4 of 5.0 targets were struck and 10 Berserkers lost over the 50 simulation runs
- 100 more Monte Carlo AFSIM simulations were run with the cyber attack included
- On average, 2.5 out of 5.0 targets were struck and 42 Berserkers were lost over 50 simulation runs with the cyber attack
  - Note that likelihood is already embedded in this calculation as the probability of the cyber attack being successful was modeled in each individual simulation run

2. FSST was developed by DOT&E and is available for use

Mission Impact

- Mission impact can be measured by either how many more Berserkers were lost than in the baseline case or by how many fewer targets were destroyed

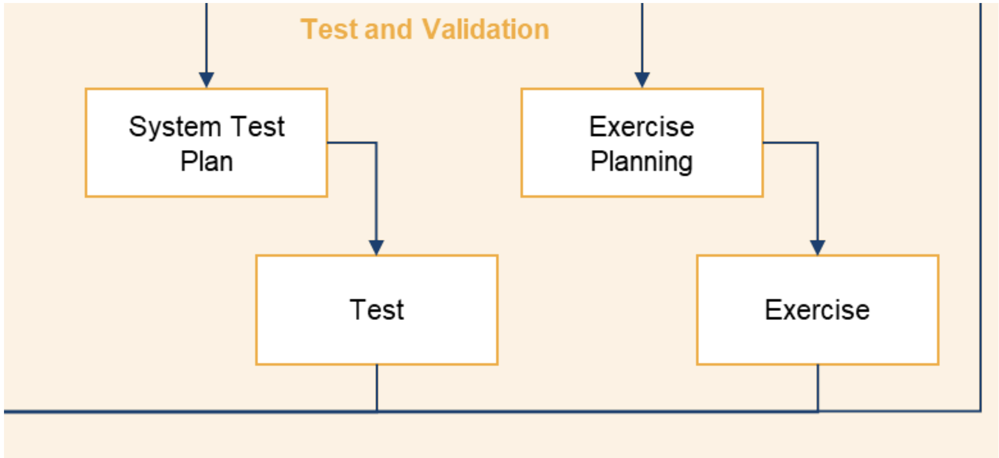
$$\boldsymbol{Mission\ Impact} = \frac{\boldsymbol{Berserker\ Destroyed\ with\ Cyber\ Attack - Berserker\ Destroyed\ Baseline}}{\boldsymbol{Berserkers\ Engaged}} = \frac{(\mathbf{42-10})}{\mathbf{100}} = \mathbf{32.0\%}$$

$$\boldsymbol{Mission\ Impact} = \frac{\boldsymbol{Targets\ Destroyed}\ \mathbf{Baseline} - \boldsymbol{Targets\ Destroyed\ Cyber\ Attack}}{\boldsymbol{Total\ Number\ of\ Targets}} = \frac{(\mathbf{222-125})}{\mathbf{250}} = \mathbf{38.8\%}$$

- Either could be EML if target destruction or survival is the critical mission element—or they can be combined with any desired weighting

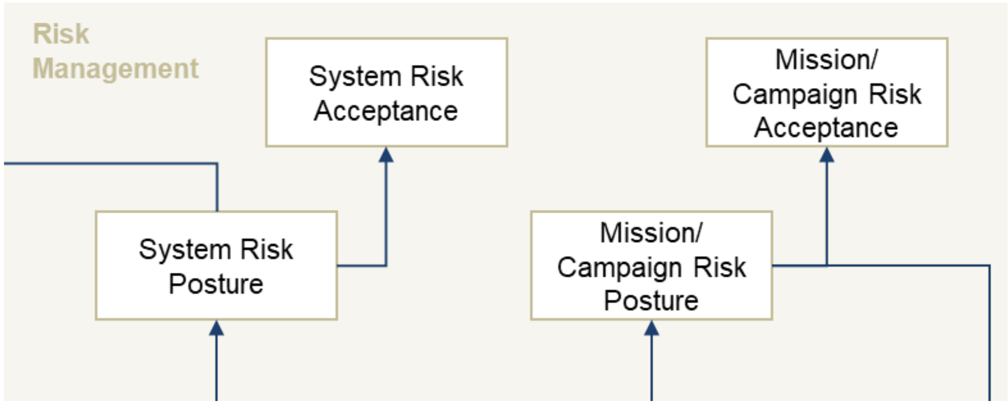
$$\boldsymbol{Average\ EML}(\mathbf{50\%\ weight\ on\ each\ element}) = \mathbf{35.4\%}$$

Test and Validation



- If modeling and simulation is going to used to inform decisions it must be validated as accurate enough
  - Calculated EML values should inform test planning
  - Executed tests should align with predicted valued from M&S
  - COLE has been verified, validated, and accredited by a tri-service and USCYBERCOM lead Model Review Committee in 2020 and 2023
- The same M&S processes and tools should be able to predict the outcomes of large scale exercises
  - DOT&E Cyber Assessment Program (CAP)

Risk Management



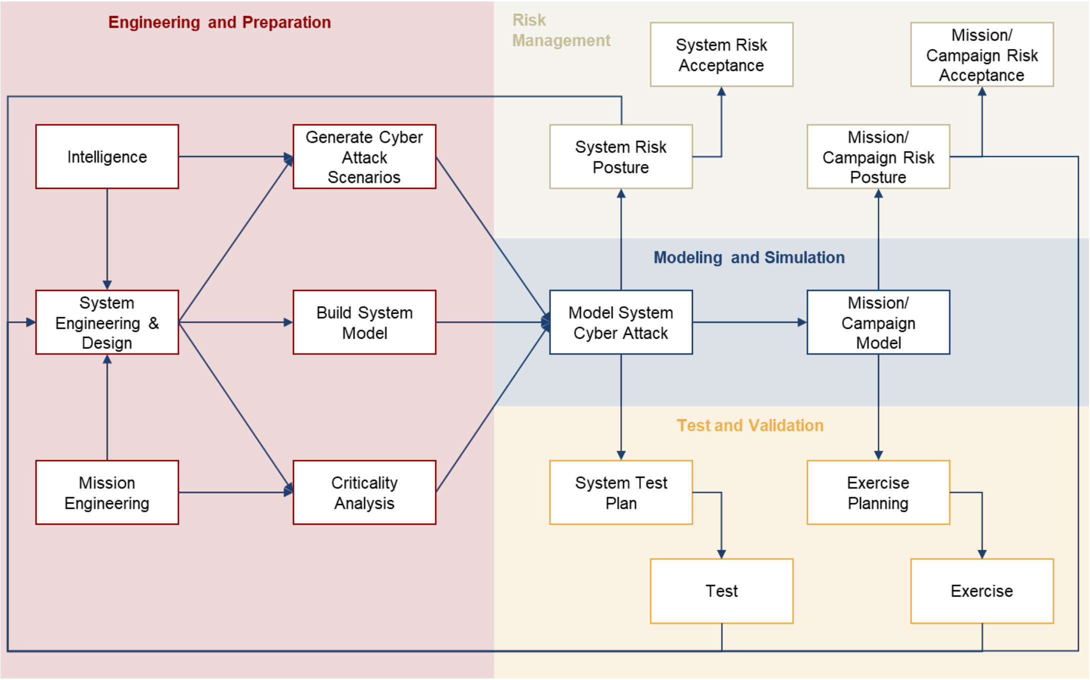
- EML provides a quantitative metric to understand mission impact for acquisition decision makers
  - EML can also be used in various mitigation scenarios to see which ones generate the greatest decrease in EML per cost or given a budget
  - Narrative descriptions of vulnerabilities or even risks are not as useful
- The same metrics rolled up to the campaign level can be utilized by combatant commander to inform resourcing and maneuver
  - Often simulations are already being run—this just adds another threat

Lessons Learned

- Results are very sensitive to the specific scenario
  - Scenarios must represent the mission
  - Multiple relevant scenarios or planned missions are better than a single mission
  - Best results will likely be obtained by rolling mission level results up to a campaign-level simulation
  - Whenever possible, simulations should be verified with large scale exercises
- Data on the likelihood of various attack stages does exist in many cases, but is hard to find
  - Would be a good potential use case for modern data methods
  - Classification remains a significant issue, commercial information can help
  - You probably have more data than you think you do
- Sensitivity analysis could help to determine where reducing uncertainty is most important

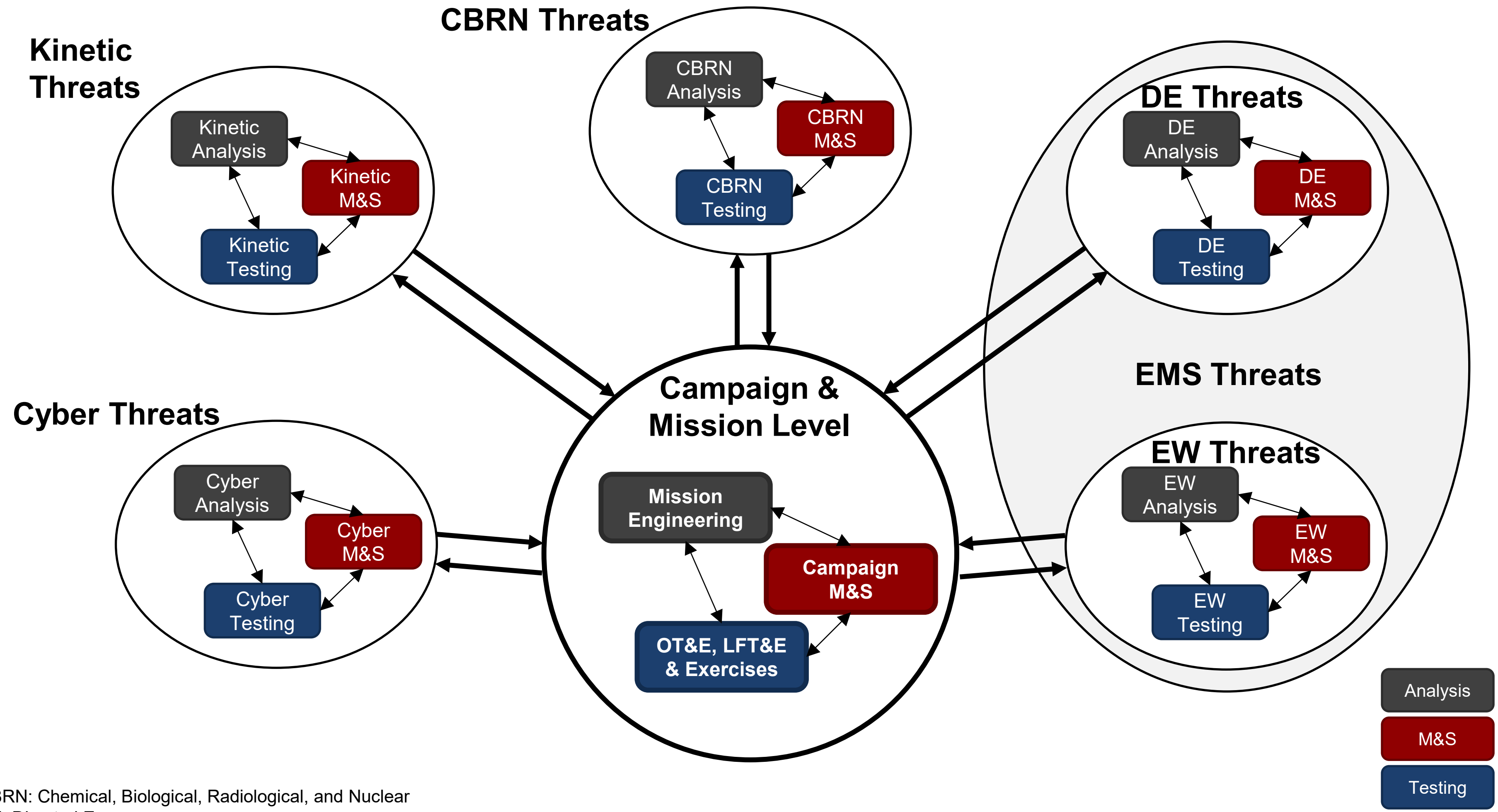
Conclusions

- Modeling cyber attacks can enable more discrete data driven inputs that can be mathematically combined to determine likelihood
- Those attacks can then be modeled in simulations at the mission level to determine mission impact
- Mission impact can be rolled up to a campaign level to determine campaign-level impact and drive risk mitigation decisions



Questions?

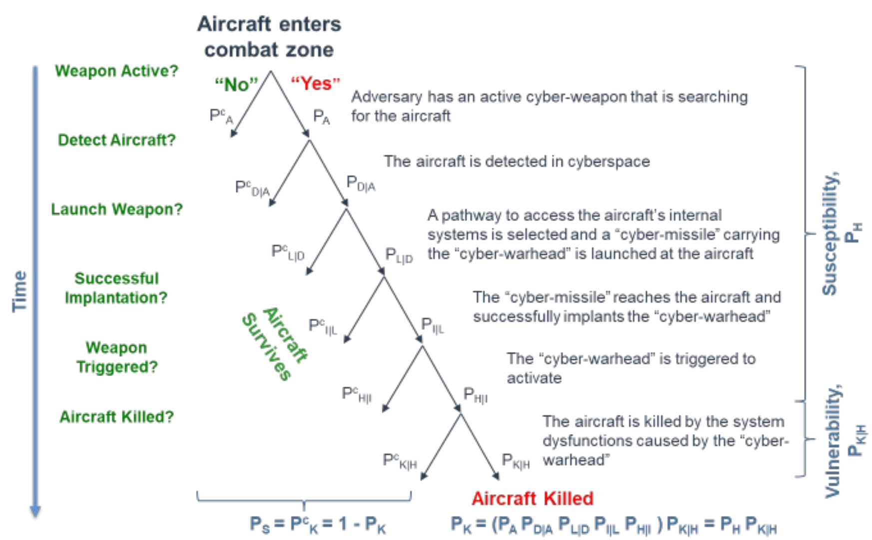
Overall M&S as an Integrator Concept



CBRN: Chemical, Biological, Radiological, and Nuclear
DE: Directed Energy
EW: Electronic Warfare
EMS: Electromagnetic Spectrum
LFT&E: Live Fire Test and Evaluation
M&S: Modeling and Simulation
OT: Operational Test

Probability of Kill (P_k)

- P_k represents the probability that a system is "killed" by a particular threat in a particular case
  - Can be an "attrition kill" where the system is damaged or destroyed
  - Can be a "mission kill" where the system is prevented from accomplishing its mission, but is available to try again the next day
- P_k is well understood for kinetic threats
- Non-kinetic threats can also use P_k for modeling



Survivability Domain Comparison

	Characteristics	Model & Simulation
Kinetic	• Well understood physics • Creates physical damage	• Typically generates a Pk for a specific 1 v 1 engagement, but then can be rolled up into a mission or campaign level • Many well validated and mature tools
Cyber	• Poorly understood and dynamic environment • Creates functional damage	• Cyber weapons are rarely simulated today • Can convert into Pk using the ACCS kill chain • Many unvalidated and immature tools
EW	• Physics better understood than cyber • Tends to create temporary functional effects	• Can model overall degradation of expected effectiveness • Can model more concretely in specific 1 v 1 scenarios
DE	• Physics are well understood but historically not powerful • Effects have tended towards temporary degrade or disrupt	• A mission or even attrition level Pk could be calculated using physics and engineering models
CBRN	• Physics are well-studied although complex • Effects range the gamut from degrade to destroy	• For specific attacks, a mission or even attrition level Pk could be calculated using physics and engineering models

Validation of Results

- Models and simulation can be the bridge between threat domains, but that bridge needs to be sound
- Validation of technical effects can be done in component level testing
- Validation of system level effects can be done through full-scale live fire testing
- Validation of mission level effects can be done in large force exercises

Full Spectrum Survivability Tool (FSST)

- The Full Spectrum Survivability Tool (FSST) effort includes the development of a **SysML v2** model that leverages the latest **Model-Based Systems Engineering** (MBSE) methodologies and M&S applications to examine full-spectrum survivability from a survivability requirements standpoint
- This prototype initiative will provide quantitative assessments of **survivability across multiple domains (e.g., cyber, EW, and potentially kinetic)** and will demonstrate adversary attacks against blue systems
  - This use case will provide a means for developing the overall infrastructure