MODERN TECHNOLOGY SOLUTIONS, INC.®

Unified Risk Assessment and Measurement System

Cutting the Gordian Knot

URAMS™

UNIFIED RISK ASSESSMENT AND MEASUREMENT SYSTEM

Dr. Bill “Data” Bryant

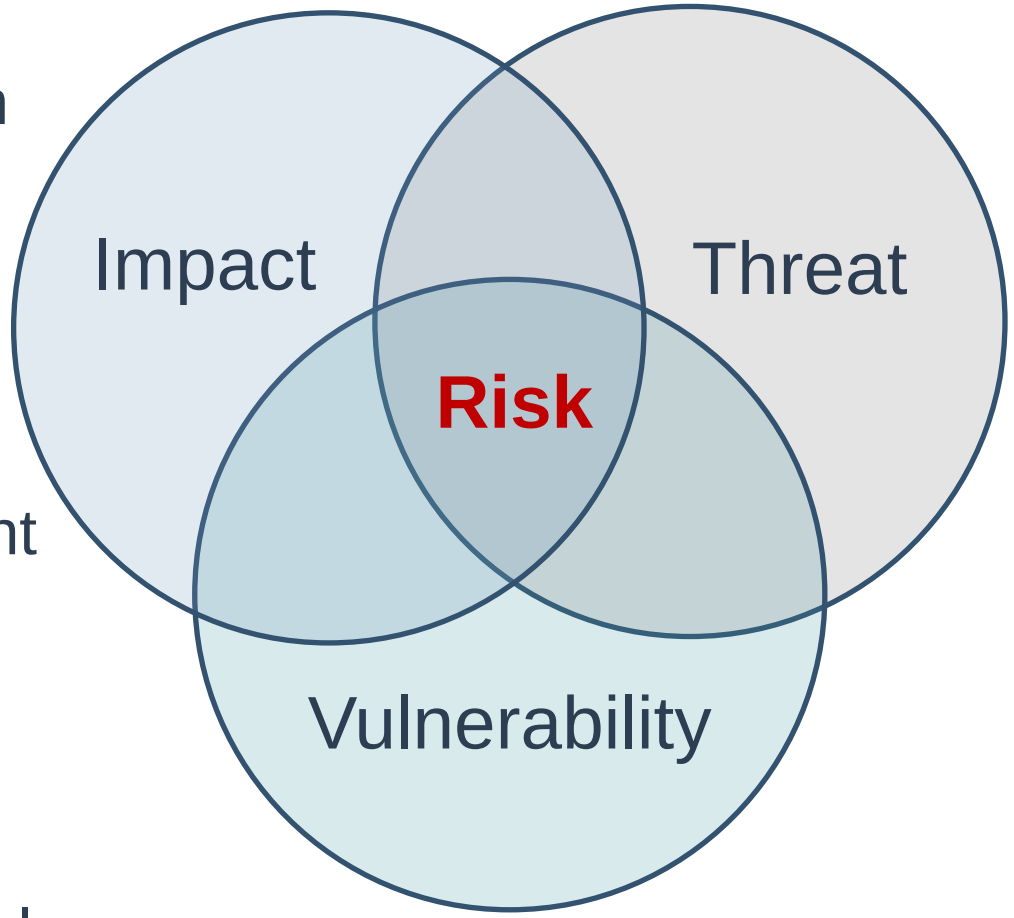
bill.bryant@mtsi-va.com

WHAT'S THE PROBLEM?

- There is no widely accepted way to effectively measure the risk of cyber attacks on aviation platforms and weapon systems
  - Multiple processes are in place from different organizations
  - Many of them are based upon approaches research has shown to be flawed, such as doing mathematical functions on ordinal number sets
- Assessments are also often disconnected from the design and engineering process, acting more like IRS audits than testing
- With an effective way to understand the level of risk, prioritize specific risks, and understand how effective proposed mitigations are—we have a much better path forward

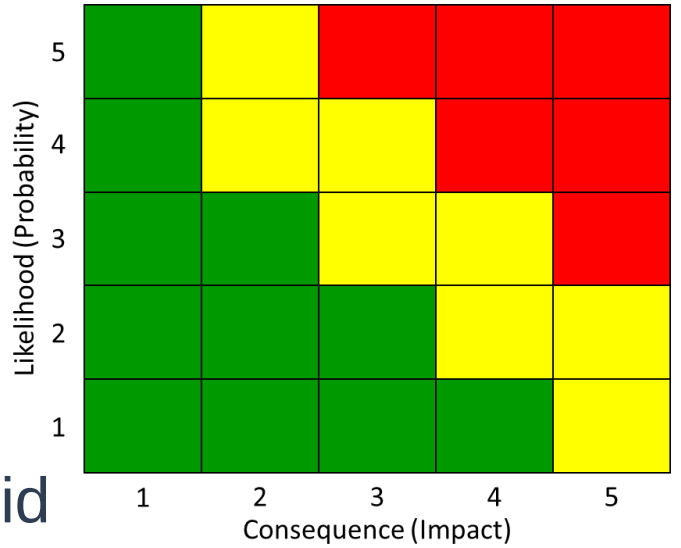
WHAT IS "RISK"?

- CNSS Definition: "A measure of the extent to which an entity is threatened by a potential circumstance or event and typically a function of:"
  1. "the adverse impacts that would arise if the circumstance or event occurs…"
  2. "the likelihood of occurrence"
- IDA study of more than 20 risk measurement methodologies found the same three elements combined in different ways to produce consequence and likelihood
- Risk scenario = story of a potential ***threat*** exploiting a ***vulnerability*** to ***impact*** a critical sub-system or component



CURRENT APPROACH ISSUES

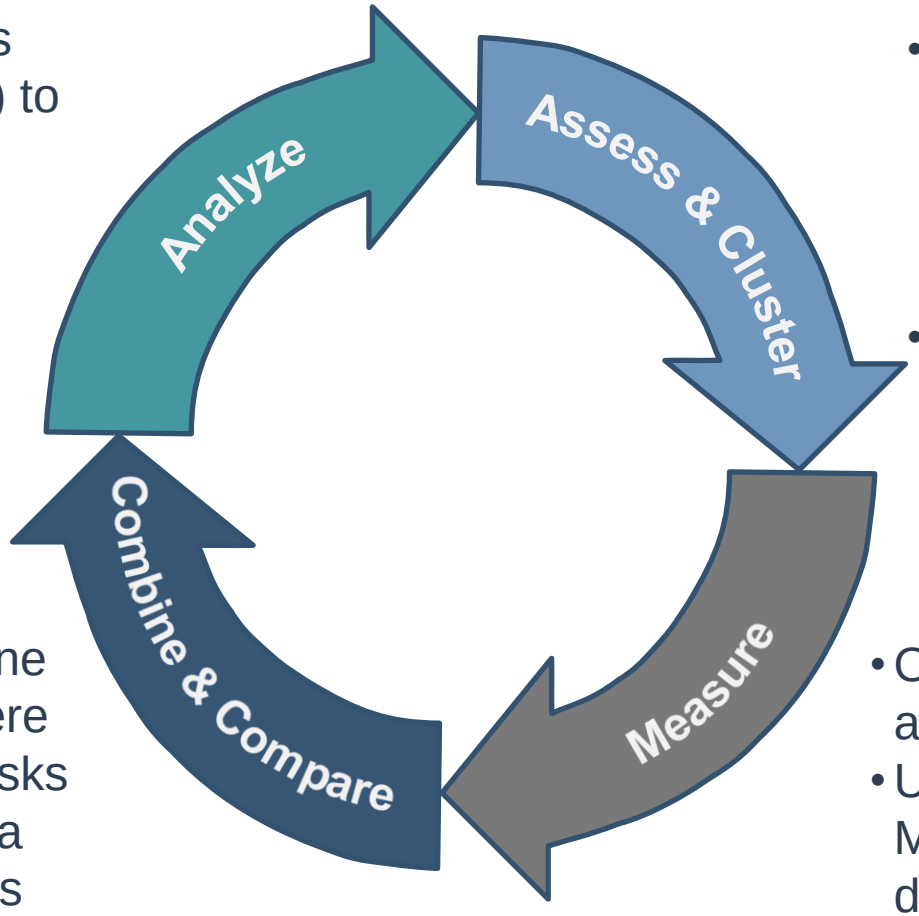
- Most common approaches used today to measure risk to weapon systems involve ranking likelihood and consequence on a scale of 1-5 and plotting them on “Risk Cubes”
- Numerous issues with this approach
  - Ordinal vs. ratio scale makes arithmetic combining invalid
  - No research evidence showing this approach is effective
  - What research does show
    - Cognitive bias issues and overconfidence
    - Inconsistency in scoring even using strict categorization
    - Range compression
    - Multiple areas on risk cubes where they cannot unambiguously score randomly selected pairs of hazards
    - Users feel better about risk, even if they don’t understand it better



URAMS Risk Spiral

Analyze

- Utilize System-Theoretic Process Analysis for Security (STPA-Sec) to analyze system
- Determine security requirements
- Determine security assumptions
- Develop risk scenarios



Assess & Cluster

- Typically utilizes Risk Assessment (RA) or Risk Assessment with Uncertainty (RAU) to identify high priority scenarios
- Inputs are from various types of Subject Matter Experts (SMEs)

Combine & Compare

- Utilizes a range of tools to combine risks depending on what tools were used to assess or measure the risks
- Can also compare overall risk in a portfolio with risk tolerance curves developed from leadership

Measure

- Optional step if quantitative results are desired at the current stage
- Utilizes Probabilistic Risk Measurement (PRM) to quantify desired risk scenarios
- Output includes uncertainty

URAMS Risk Assessment Toolkit

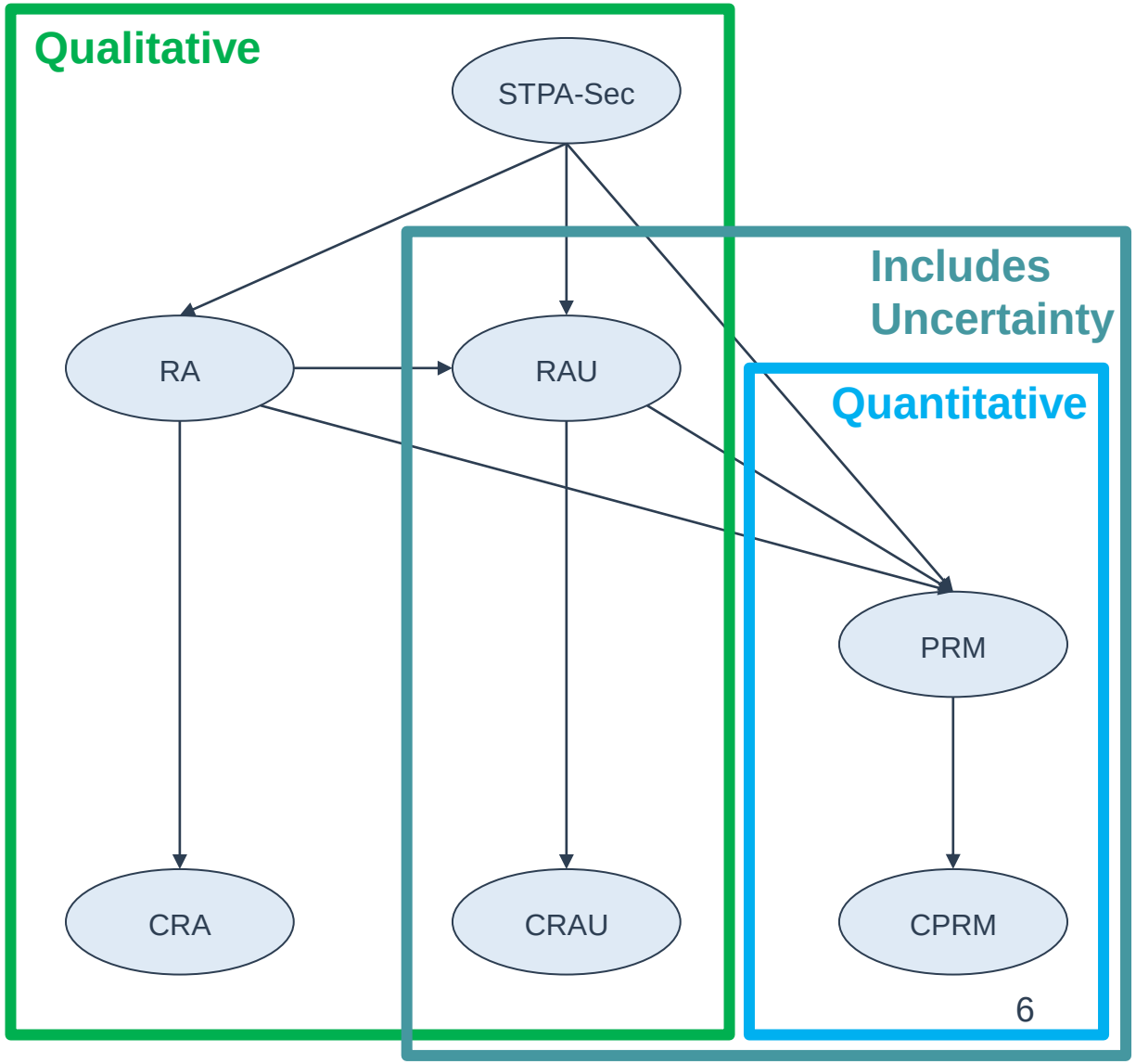
- All URAMS tools can characterize risk in terms of mission loss, financial loss, or both
- Each assessment or measurement tool has a corresponding combining and comparison tool
- Mix of qualitative (RA & RAU) and quantitative tools (PRM)
- RAU and PRM include an assessment or measurement of uncertainty

Analyze

Assess & Cluster

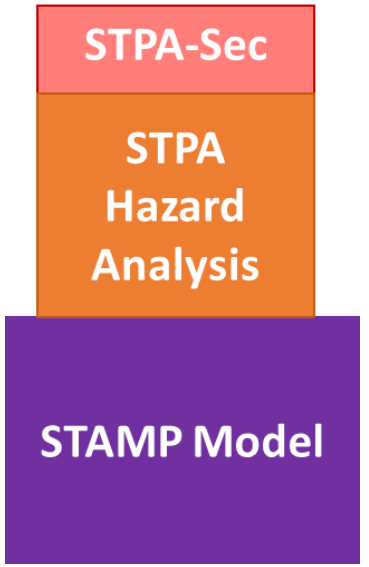
Measure

Combine & Compare

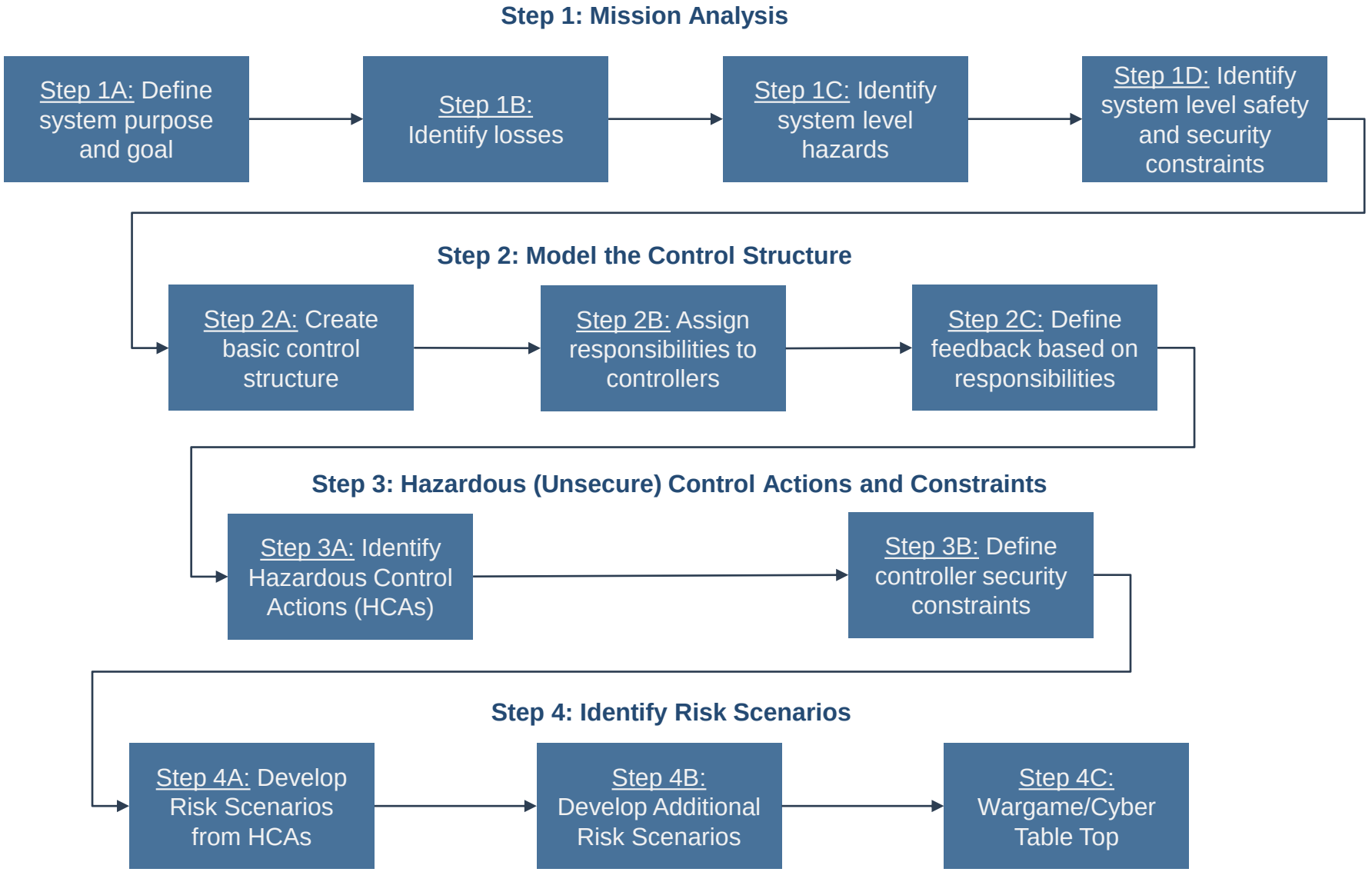


STPA-SEC BACKGROUND

- System-Theoretic Accident Model and Processes (STAMP) was developed by Dr. Nancy Leveson at MIT for the safety community
- System Theoretic Process Analysis (STPA) Hazard analysis is based on the STAMP model
  - STPA is based on systems thinking and focuses on safety as a emergent property of complex systems vs. only looking at the component level
  - Many years of experience with very positive results when compared to traditional safety approaches
- System-Theoretic Process Analysis for Security (STPA-Sec) is a security extension of STPA developed by Dr. William Young
  - Adds in a thinking adversary that can introduce unsecure control actions as well as the STPA unsafe control actions
  - Includes wargaming as an important element

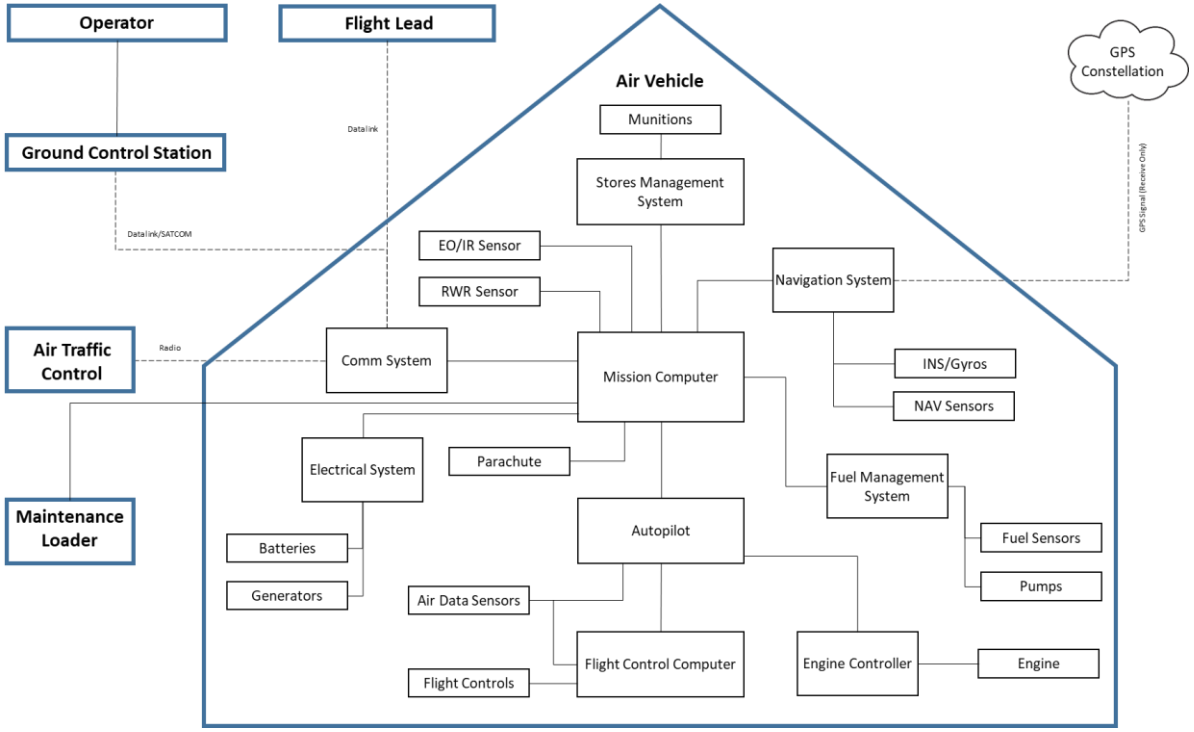


STPA-Sec Steps



NOTIONAL EXAMPLE: MQ-99 BERSERKER

- Completely notional example based on an artist's depiction in company promotional literature
- Any resemblance to a real system is completely coincidental
- System is at the conceptual stage of design



- Basic CONOPS & architecture developed
- Air-to-Air and Air-to Ground roles
- Can be semi-autonomous, controlled from ground station or by an airborne manned platform
- Weapons are 2 x AMRAAM, or 6 x SDB
- Attritable with remote ops location

MQ-99 Example Step 1 A-B System Purpose and Unacceptable Losses

- Step 1A is to define the system's purpose and goal
  - A system to do *{What = Purpose}* by means of *{How = Method}* in order to contribute to *{Why = Goals}*, while *{Constraints / Restraints}*
  - The MQ-99 Berserker is an Unmanned Aerial Vehicle system *to destroy hostile ground and air targets and decoy hostile defenses* by means of *loading, transiting, and employing ordnance* in order to contribute to *counterair and counterland air operations* while *preventing fratricide and collateral damage and meeting the attritable per-unit cost threshold*
- Step 1B is to identify the unacceptable losses
  - L-1: Loss of life or injury to friendly or neutral people
  - L-2: Significant damage to friendly or neutral objects
  - L-3: Unable to destroy assigned targets
  - L-4: Unable to decoy hostile air defenses when required

MQ-99 Risk Scenarios

Risk Scenario #	Risk Scenario
R-1	A tier 5 or higher cyber attacker gains access to the ground control station through a supply chain attack on the software production and/or transmission process and uses tampering to alter weapons release authorization, targeting, waypoint, or mission data [HCA-28, HCA-32, HCA-35, HCA-36, L-1, L-2, L-3]
R-2	A tier 5 or higher cyber attacker gains access to the air vehicle communications link through insecure communications channels with the ground station and uses spoofing to send malicious mission data to the air vehicle [HCA-28, L-1, L-2, L-3]
R-11	A tier 6 cyber attacker gains access to the air vehicle communications system through a supply chain attack and uses information disclosure to cause the air vehicle to send the location of the flight lead passed over the datalink [HCA-207, L-1, L-2]
R-21	A tier 6 cyber attacker gains access to the mission computer OFP through a supply chain attack on the software development and distribution system and uses tampering to modify the OFP to enable adversary control of the MQ-99 [HCA-325, L-1, L-2, L-3, L-4]
R-22	A tier 5 or higher cyber attacker gains access to the traditional-IT maintenance system through an Internet based attack and uses tampering to alter OFPs loaded onto the MQ-99 giving the attacker control over MQ-99 functioning [HCA-325, L-1, L-2, L-3, L-4]
R-23	A tier 6 adversary gains access to the OFP loading capability of the mission computer through an elevation of privilege attack that bypasses the physical safeguards on the vehicle and enables the adversary to load malicious OFPs into components [HCA-273, L-1, L-2, L-3, L-4]
R-30	A tier 5 cyber attacker gains access to the traditional-IT maintenance system through a supply chain attack and uses tampering to alter OFPs loaded onto the MQ-99 giving the attacker control over MQ-99 functioning [HCA-325, L-1, L-2, L-3, L-4]
R-31	A tier 6 adversary gains access to a component connected to the data bus through a supply chain attack and uses spoofing to manipulate or take control of the air vehicle [HCA-132, L-1, L-2, L-3, L-4]

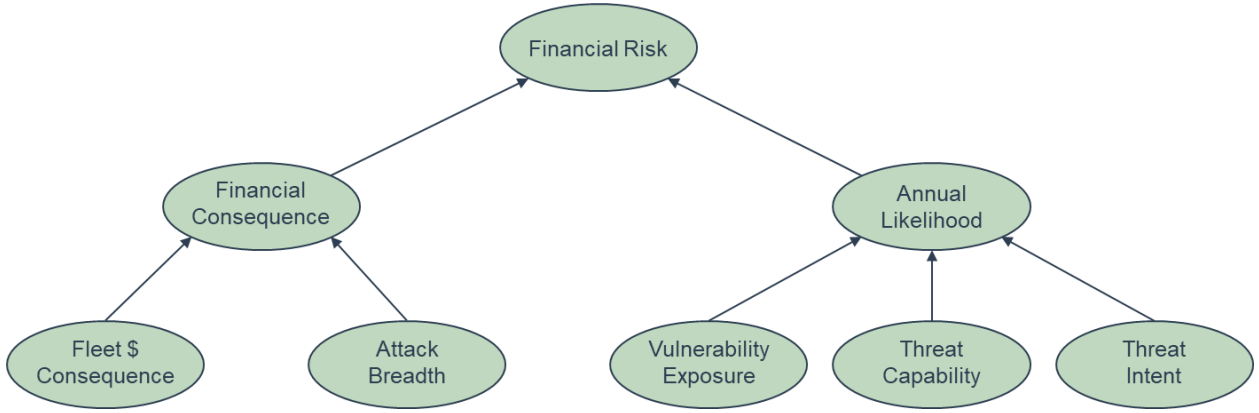
STPA-Sec and Tracking Assumptions

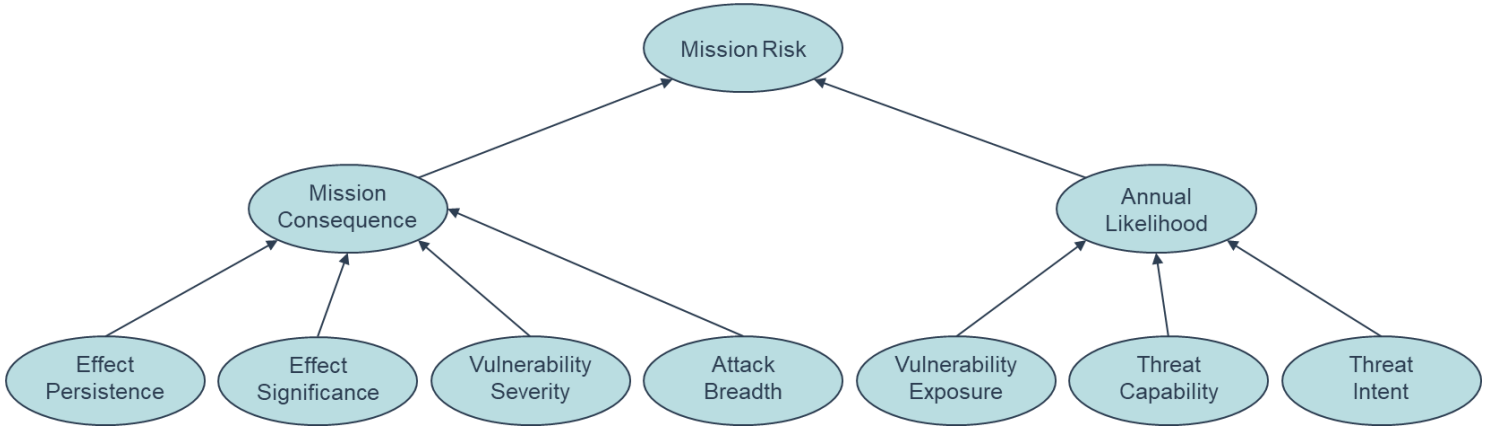
- The assumptions developed during STPA-Sec can be used as a way of monitoring for changes in the environment
- Some of the design assumptions from MQ-99 were:

Design Assumption #	Assumption
AD-1	MQ-99 will utilize NSA type 1 encryption on all communications channels used for command traffic
AD-2	All OFPs for MQ-99 systems and components will be cryptographically signed by the developers using industry best-practice encryption and each component will check the signature before accepting any new OFP load
AD-3	All logic bearing components and sub-systems of the MQ-99 will utilize a hardware root of trust and will send out an error message and refuse to power on if the root of trust cannot be verified
AD-4	MQ-99 will utilize a combination of a MIL-STD 1553 data bus and TCP/IP networks for passing data and messages between components
AD-5	MQ-99 maintenance loaders will be COTS notebooks running standard Windows operating systems that will be handled and stored in accordance with strict physical security measures
AD-6	MQ-99 maintenance loaders will have unneeded functionality removed via hardware whenever possible and software and registry settings when necessary
AD-13	MQ-99 can be powered on and OFPs can be loaded in all components through a single data port in the storage and shipping container, cryptographic keys can be loaded through a separate cryptographic keying port in the storage container
AD-14	MQ-99 will not have logging or monitoring built into the components or data bus
AD-15	All MQ-99 software will the thoroughly reviewed for potential security issues by state-of-the-art static and dynamic code checking techniques
AD-16	MQ-99 will not accept OFP loading into any component unless a physical maintenance load switch is activated on the individual vehicle placing it temporarily into maintenance mode

RISK ASSESSMENT (RA)

- Simplest and fastest tool to assess risk scenarios is RA
- Can score in terms of either mission loss or financial loss
- Sub-elements are scored by SMEs normally on a 0-100 scale
  - Clearly defined categorization criteria



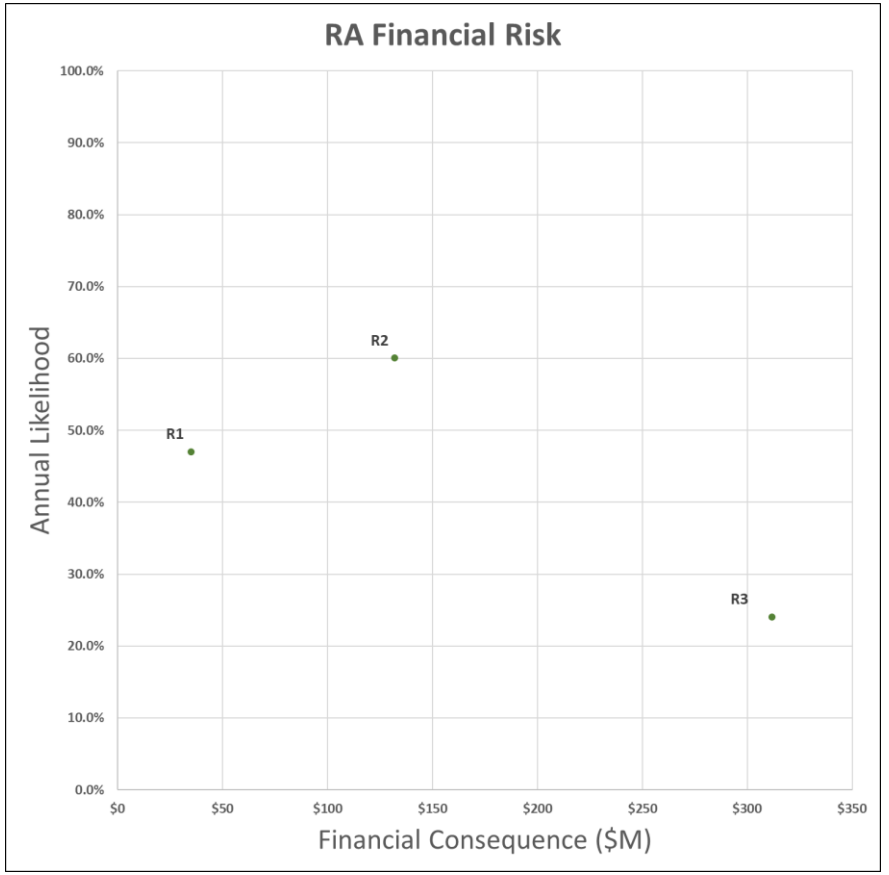


- Different experts normally used to score different areas
- In a military context the "year" used must be defined
- Scoring for fleet wide consequence is separated from attack breadth

RA Assumptions

- RA makes some key assumptions that must be understood
  1. Analysts can accurately assess the sub-elements of RA on a 0-100 scale with minimal training and will produce similar outputs for the same input
  2. RA scores are ratio data and thus can be legitimately multiplied together
  3. Risk scenarios are independent, and a scenario's occurring does not change the risk that other scenarios will occur
  4. Annual likelihood may be estimated as the result of vulnerability exposure, threat capability, and threat intent multiplied together, with each contributing equal weight
  5. Fleetwide financial consequence multiplied by the percentage of systems affected across the fleet will yield financial consequence and this relationship is linear where 10% of the fleet affected will equal 10% of the fleetwide cost and 90% of the fleet affected will yield 90% of the fleetwide cost
  6. Fleetwide mission consequence can be estimated as the result of effect persistence, effect significance, and vulnerability severity multiplied together, with each contributing equal weight
  7. Fleetwide mission consequence multiplied by the percentage of systems affected across the fleet will yield financial consequence and this relationships is linear where 10% of the fleet affected will equal 10% of the fleetwide cost and 90% of the fleet affected will yield 90% of the fleetwide cost

SIMPLE UAS RA EXAMPLE

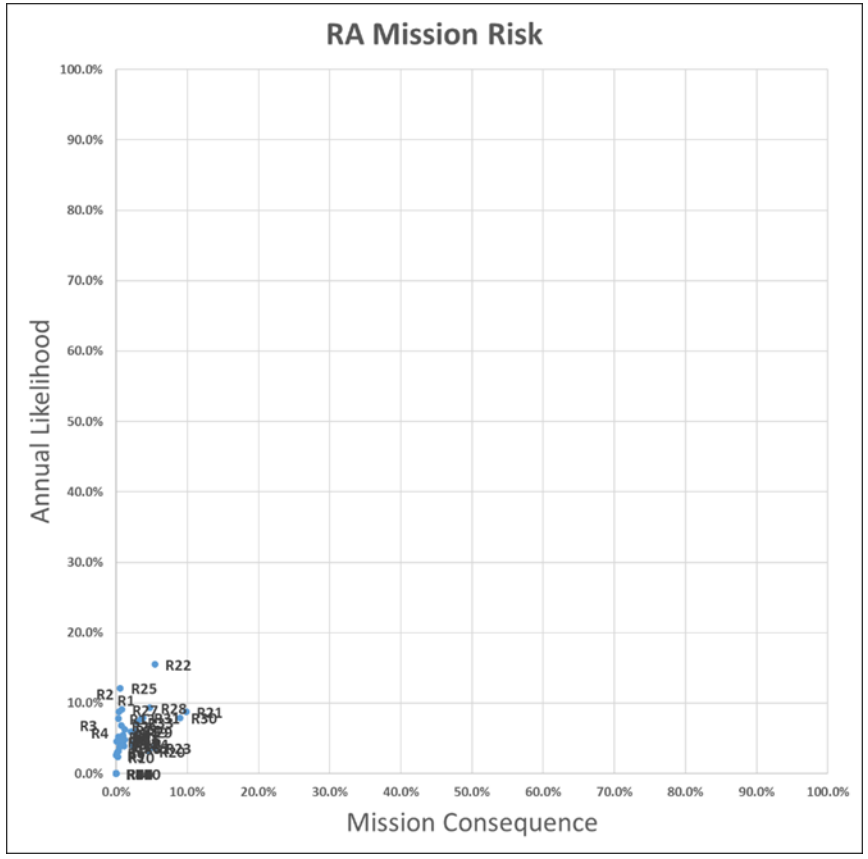


		Mission Risk
Risk Scenario	Short Description	Expected
R1	Exfiltrate Mission Data	0.0358
R2	Denial of Service	0.2568
R3	Command Injection	0.2077

		Financial Risk
Risk Scenario	Short Description	Expected
R1	Exfiltrate Mission Data	$16.5
R2	Denial of Service	$79.2
R3	Command Injection	$74.9

MQ-99 BERSERKER RA MISSION RISK RESULTS

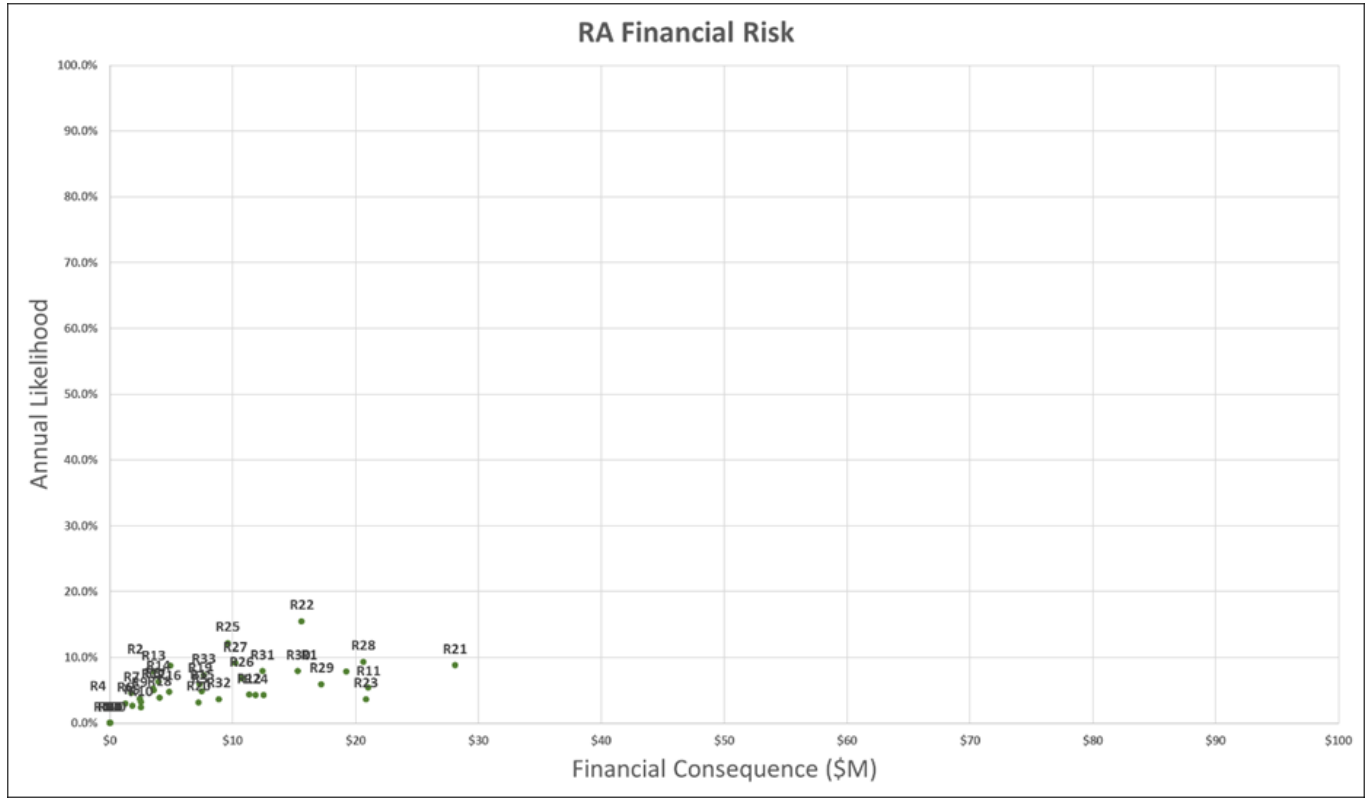
- 33 risk scenarios were scored with results clustering in the lower left
- Based on design assumptions, MQ-99 is secure



Risk Scenario	Short Description	Mission Risk
R21	Mission computer supply chain OFP adversary control	0.866%
R22	MX system via Internet tampering load OFPs	0.847%
R30	Supply chain MX system alter OFP loads	0.711%
R28	Supply chain tampered component alter data	0.444%
R31	Supply chain component take over data bus	0.300%
R1	GCS supply chain soft production/transmission	0.281%
R33	Supply chain component denial of service data bus	0.217%
R23	OFP Loading physical switch bypass	0.197%
R29	Supply chain tamper mission data load for RWR	0.163%
R20	GSC supply chain OFP tampering manipulate comms	0.144%
R19	Spoof C&C message authorize weapons employment	0.127%
R24	GPS position spoofing move AV	0.095%
R32	Supply chain tampering reduce engine life	0.091%
R25	GPS denial of service	0.077%
R14	AV comm link spoofing targeting data	0.077%
R27	Spoof C&C messages via insecure comms	0.073%
R15	AV comm link spoofing weapon release	0.059%
R16	AV comm link spoofing jettison command	0.056%
R11	Supply chain comm system attack send location	0.054%
R26	Crypto attack datalink spoofing IADS data	0.051%
R18	AV crypto broken dive into target	0.044%
R12	Supply chain software develop send location	0.039%
R2	AV comm link spoofing mission data	0.039%
R17	AV comm link information disclosure position	0.034%
R13	Wireless MX attack spoofing and tampering	0.030%
R3	Insider malicious mission computer info disclosure	0.028%
R9	Spoof parachute deploy via insecure comms	0.020%
R8	Spoof C&C messages via hardware supply chain	0.017%
R4	Insider support equip access to avionics	0.011%
R7	RF attack on comm system inject false	0.007%
R10	Spoof flight lead messages via insecure comms	0.006%
R6	RF attack on comm system mislead EO/IR	0.006%
R5	Insider plus crypto attack on GCS AV link	0.002%

MQ-99 Berserker RA Financial Risk Results

- Financial risk looks less clustered but note that the x-axis is not fixed
- Risks are in a very similar order to mission

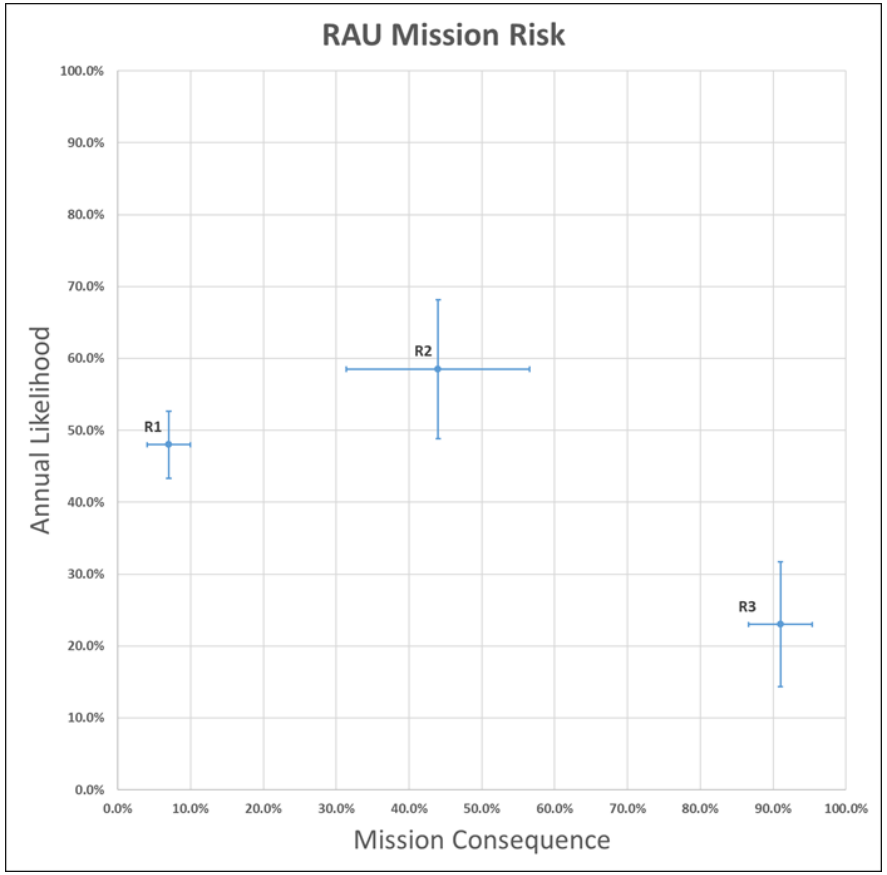


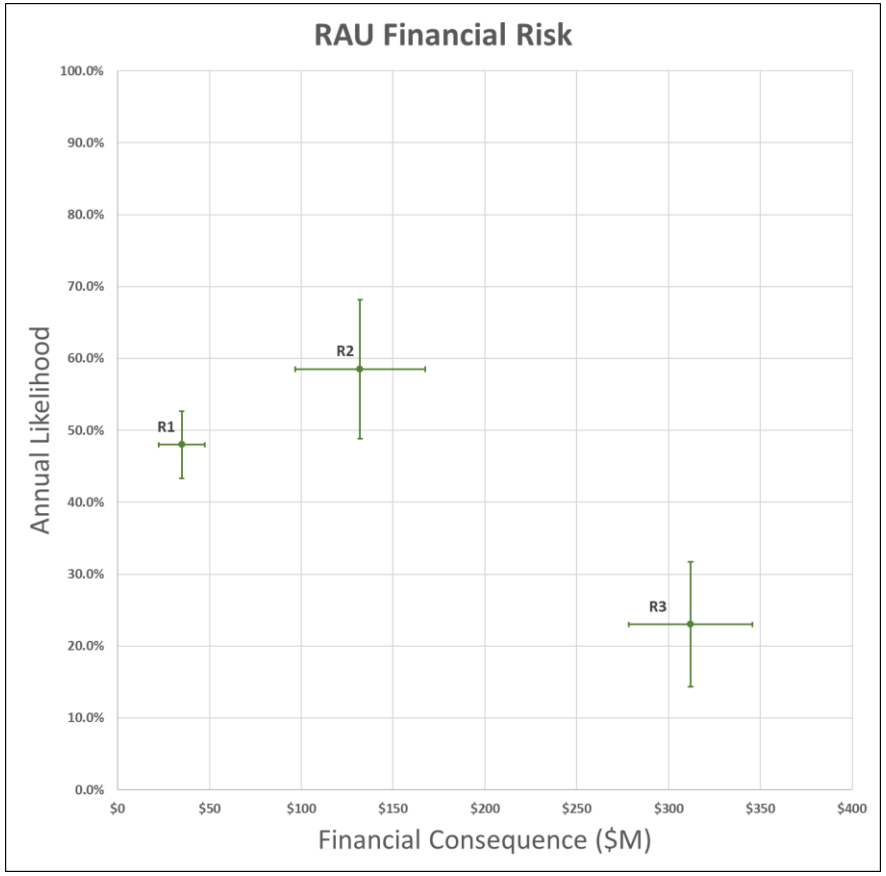
Risk Scenario	Short Description	Financial Risk
R21	Mission computer supply chain OFP adversary control	$2.458
R22	MX system via Internet tampering load OFPs	$2.417
R28	Supply chain tampered component alter data	$1.917
R1	GCS supply chain soft production/transmission	$1.503
R30	Supply chain MX system alter OFP loads	$1.206
R25	GPS denial of service	$1.162
R11	Supply chain comm system attack send location	$1.139
R29	Supply chain tamper mission data load for RWR	$1.011
R31	Supply chain component take over data bus	$0.978
R27	Spoof C&C messages via insecure comms	$0.927
R23	OFP Loading physical switch bypass	$0.757
R26	Crypto attack datalink spoofing IADS data	$0.729
R33	Supply chain component denial of service data bus	$0.556
R3	Insider malicious mission computer info disclosure	$0.531
R24	GPS position spoofing move AV	$0.501
R12	Supply chain software develop send location	$0.488
R19	Spoof C&C message authorize weapons employment	$0.433
R2	AV comm link spoofing mission data	$0.429
R15	AV comm link spoofing weapon release	$0.360
R32	Supply chain tampering reduce engine life	$0.322
R13	Wireless MX attack spoofing and tampering	$0.278
R14	AV comm link spoofing targeting data	$0.247
R16	AV comm link spoofing jettison command	$0.230
R20	GSC supply chain OFP tampering manipulate comms	$0.226
R8	Spoof C&C messages via hardware supply chain	$0.184
R17	AV comm link information disclosure position	$0.178
R18	AV crypto broken dive into target	$0.157
R9	Spoof parachute deploy via insecure comms	$0.090
R7	RF attack on comm system inject false	$0.080
R4	Insider support equip access to avionics	$0.080
R10	Spoof flight lead messages via insecure comms	$0.059
R5	Insider plus crypto attack on GCS AV link	$0.048
R6	RF attack on comm system mislead EO/IR	$0.038

RISK ASSESSMENT WITH UNCERTAINTY (RAU)

- RAU has the same structure and tracks very closely to RA with the same assumptions, categorization, etc.
- The major difference is that RA uses three-point estimation
  - Expected
  - Best-case
  - Worst-case
- This provides a way to assess uncertainty
- Adding the assumption that the data follows the Gaussian or normal distribution enables calculation of 90% Confidence Intervals (90CI)
- Calculating 90CIs provides a way to compare RAU and PRM results

SIMPLE UAS RAU EXAMPLE



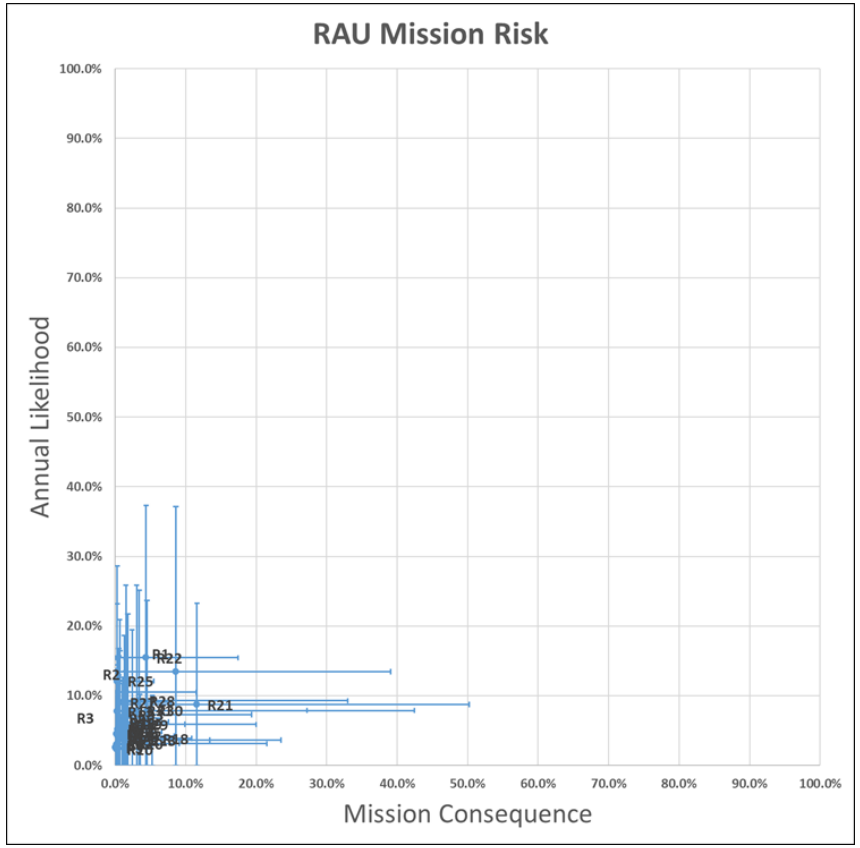


		Mission Risk		
Risk Scenario	Short Description	Expected	90CI Low	90CI High
R1	Exfiltrate Mission Data	3.4%	1.6%	5.1%
R2	Denial of Service	25.7%	13.9%	37.6%
R3	Command Injection	20.9%	12.1%	29.8%

		Financial Risk		
Risk Scenario	Short Description	Expected	90CI Low	90CI High
R1	Exfiltrate Mission Data	$16.8	$9.2	$24.4
R2	Denial of Service	$77.2	$43.5	$110.9
R3	Command Injection	$71.8	$36.8	$106.7

MQ-99 Berserker RAU Mission Risk Results

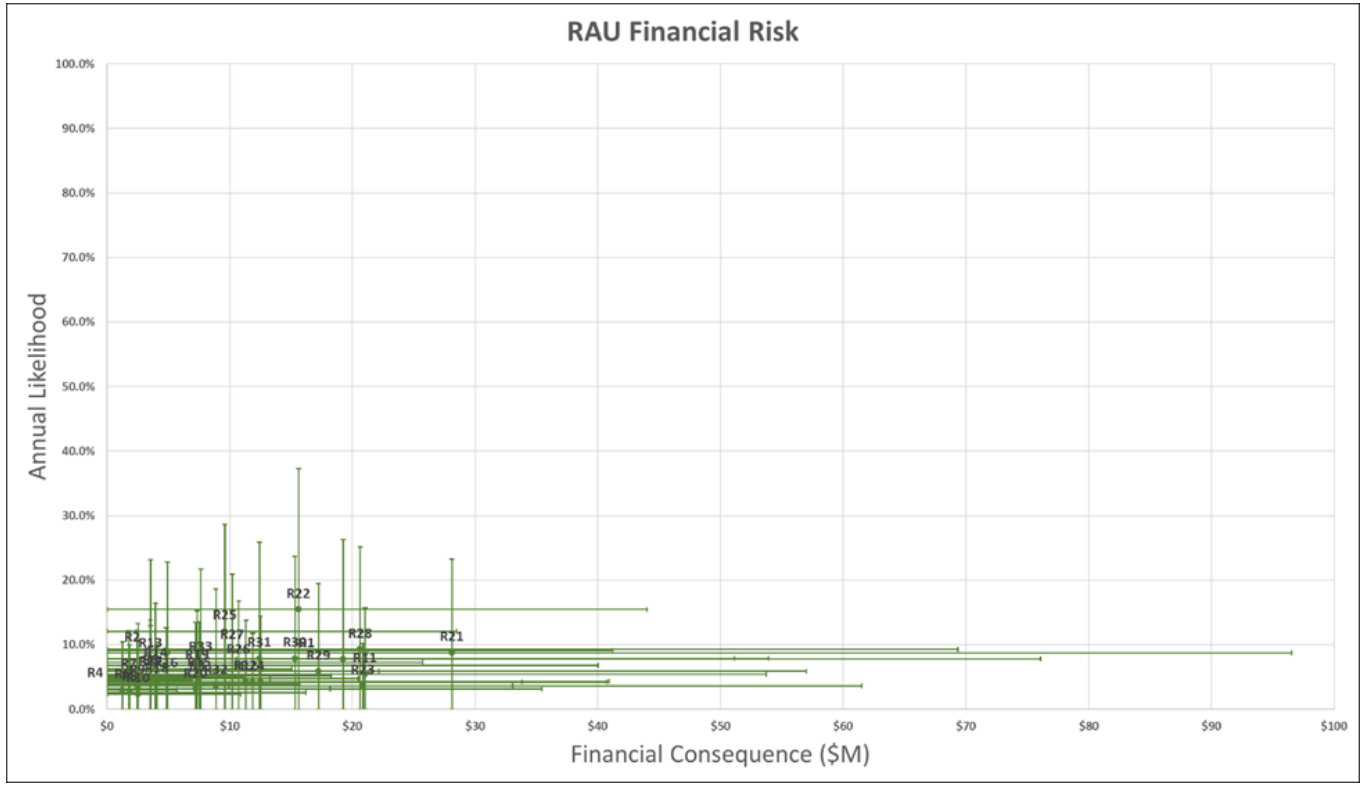
- RAU shows a significant amount of uncertainty in the assessments of risk



Risk Scenario	Short Description	EML	Standard Deviation
R21	Mission computer supply chain OFP adversary control	0.866%	5.482%
R22	MX system via Internet tampering load OFPs	0.847%	2.863%
R30	Supply chain MX system alter OFP loads	0.711%	5.489%
R28	Supply chain tampered component alter data	0.444%	4.356%
R31	Supply chain component take over data bus	0.300%	3.985%
R1	GCS supply chain soft production/transmission	0.281%	4.452%
R33	Supply chain component denial of service data bus	0.217%	2.312%
R23	OFP Loading physical switch bypass	0.197%	1.217%
R29	Supply chain tamper mission data load for RWR	0.163%	2.189%
R20	GSC supply chain OFP tampering manipulate comms	0.144%	1.799%
R19	Spoof C&C message authorize weapons employment	0.127%	0.744%
R24	GPS position spoofing move AV	0.095%	0.516%
R32	Supply chain tampering reduce engine life	0.091%	1.589%
R25	GPS denial of service	0.077%	0.819%
R14	AV comm link spoofing targeting data	0.077%	0.648%
R27	Spoof C&C messages via insecure comms	0.073%	0.813%
R15	AV comm link spoofing weapon release	0.059%	0.437%
R16	AV comm link spoofing jettison command	0.056%	0.322%
R11	Supply chain comm system attack send location	0.054%	0.300%
R26	Crypto attack datalink spoofing IADS data	0.051%	0.557%
R18	AV crypto broken dive into target	0.044%	0.353%
R12	Supply chain software develop send location	0.039%	0.344%
R2	AV comm link spoofing mission data	0.039%	0.773%
R17	AV comm link information disclosure position	0.034%	0.180%
R13	Wireless MX attack spoofing and tampering	0.030%	0.279%
R3	Insider malicious mission computer info disclosure	0.028%	0.422%
R9	Spoof parachute deploy via insecure comms	0.020%	0.332%
R8	Spoof C&C messages via hardware supply chain	0.017%	0.405%
R4	Insider support equip access to avionics	0.011%	0.772%
R7	RF attack on comm system inject false	0.007%	0.088%
R10	Spoof flight lead messages via insecure comms	0.006%	0.093%
R6	RF attack on comm system mislead EO/IR	0.006%	0.091%
R5	Insider plus crypto attack on GCS AV link	0.002%	0.091%

MQ-99 Berserker RAU Financial Risk Results

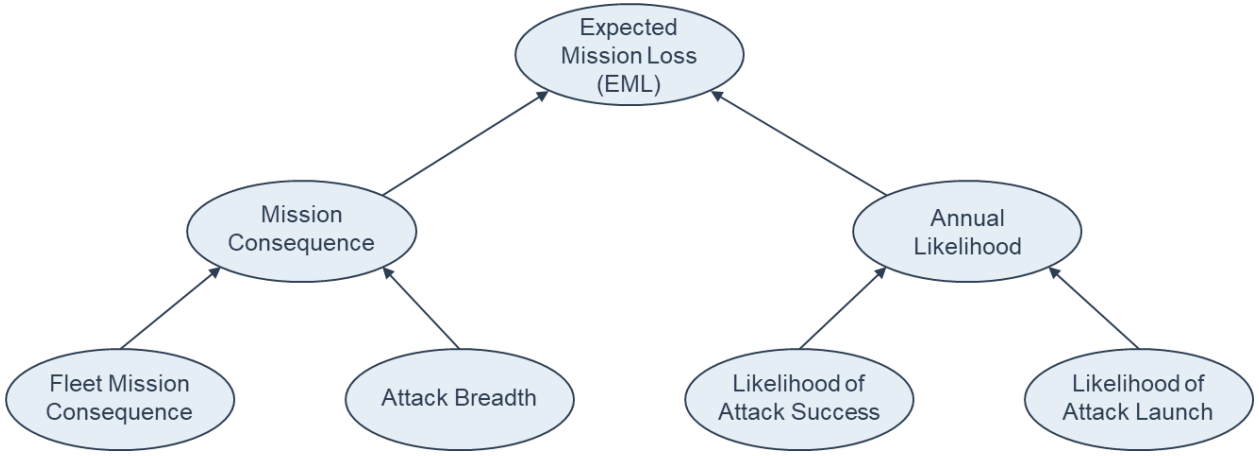
- MQ-99 Financial risk has even larger amounts of uncertainty with RAU

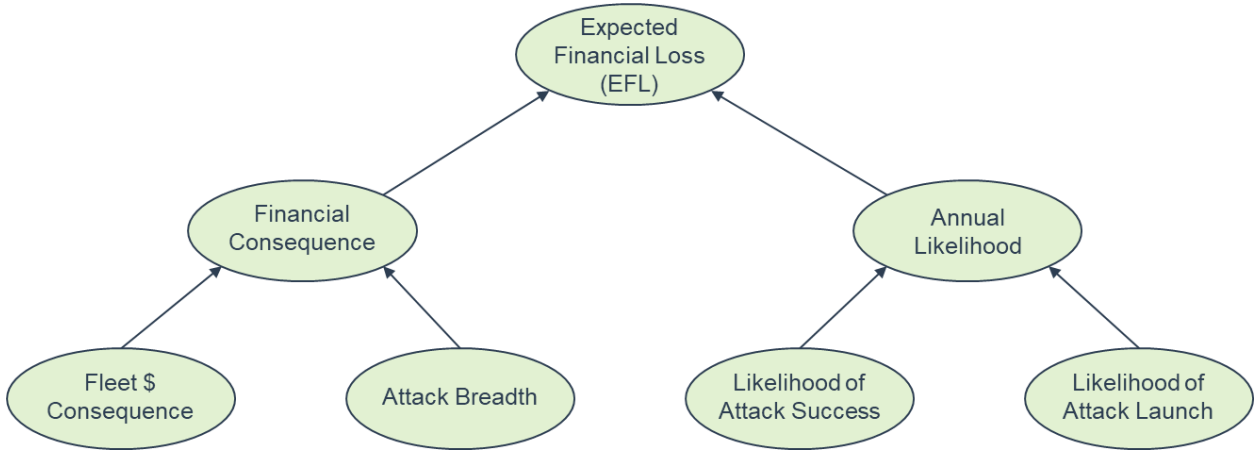


Risk Scenario	Short Description	EFL	Standard Deviation
R21	Mission computer supply chain OFP adversary control	$2.458	$10.082
R22	MX system via Internet tampering load OFPs	$2.417	$6.574
R28	Supply chain tampered component alter data	$1.917	$7.711
R1	GCS supply chain soft production/transmission	$1.503	$10.466
R30	Supply chain MX system alter OFP loads	$1.206	$6.058
R25	GPS denial of service	$1.162	$3.203
R11	Supply chain comm system attack send location	$1.139	$3.501
R29	Supply chain tamper mission data load for RWR	$1.011	$5.283
R31	Supply chain component take over data bus	$0.978	$6.702
R27	Spoof C&C messages via insecure comms	$0.927	$3.688
R23	OFP Loading physical switch bypass	$0.757	$2.687
R26	Crypto attack datalink spoofing IADS data	$0.729	$2.900
R33	Supply chain component denial of service data bus	$0.556	$2.534
R3	Insider malicious mission computer info disclosure	$0.531	$2.289
R24	GPS position spoofing move AV	$0.501	$2.175
R12	Supply chain software develop send location	$0.488	$2.827
R19	Spoof C&C message authorize weapons employment	$0.433	$1.439
R2	AV comm link spoofing mission data	$0.429	$2.332
R15	AV comm link spoofing weapon release	$0.360	$1.202
R32	Supply chain tampering reduce engine life	$0.322	$3.385
R13	Wireless MX attack spoofing and tampering	$0.278	$1.066
R14	AV comm link spoofing targeting data	$0.247	$1.135
R16	AV comm link spoofing jettison command	$0.230	$0.684
R20	GSC supply chain OFP tampering manipulate comms	$0.226	$2.734
R8	Spoof C&C messages via hardware supply chain	$0.184	$1.256
R17	AV comm link information disclosure position	$0.178	$0.617
R18	AV crypto broken dive into target	$0.157	$0.724
R9	Spoof parachute deploy via insecure comms	$0.090	$0.617
R7	RF attack on comm system inject false	$0.080	$0.378
R4	Insider support equip access to avionics	$0.080	$1.430
R10	Spoof flight lead messages via insecure comms	$0.059	$0.510
R5	Insider plus crypto attack on GCS AV link	$0.048	$0.964
R6	RF attack on comm system mislead EO/IR	$0.038	$0.309

PROBABILISTIC RISK MEASUREMENT (PRM)

- More robust & quantitatively based
- Can also score in terms of either mission loss or financial loss
- Analysts are asked to provide 90% Confidence Intervals (90CI) for each input
  - Requires expert "calibration"



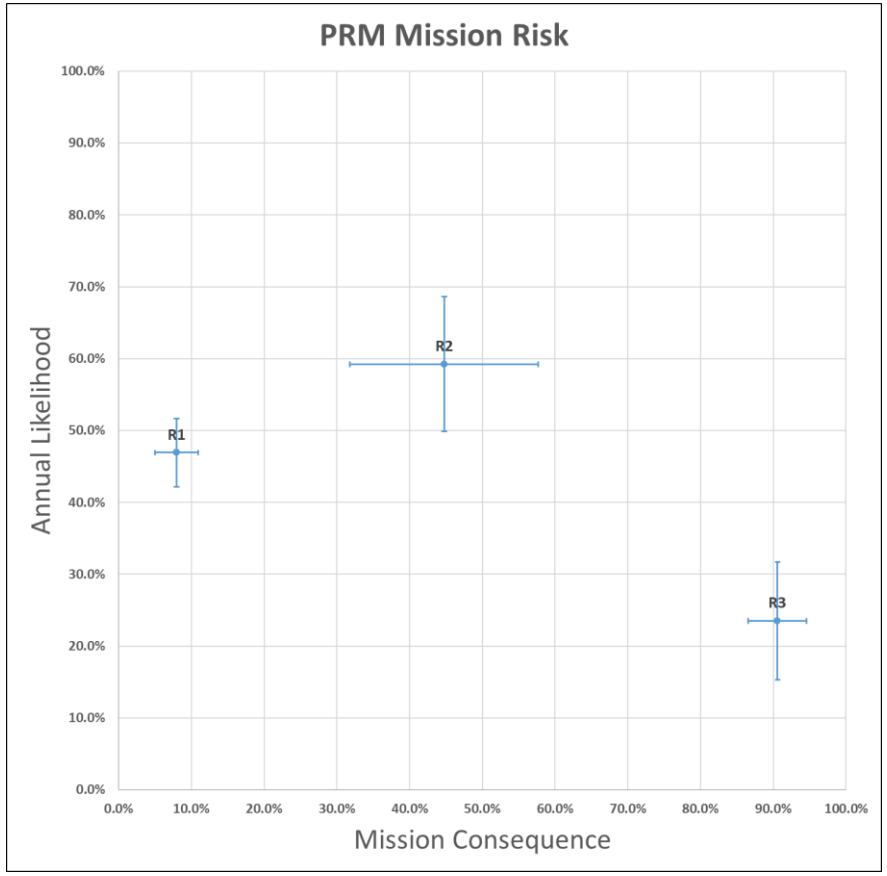


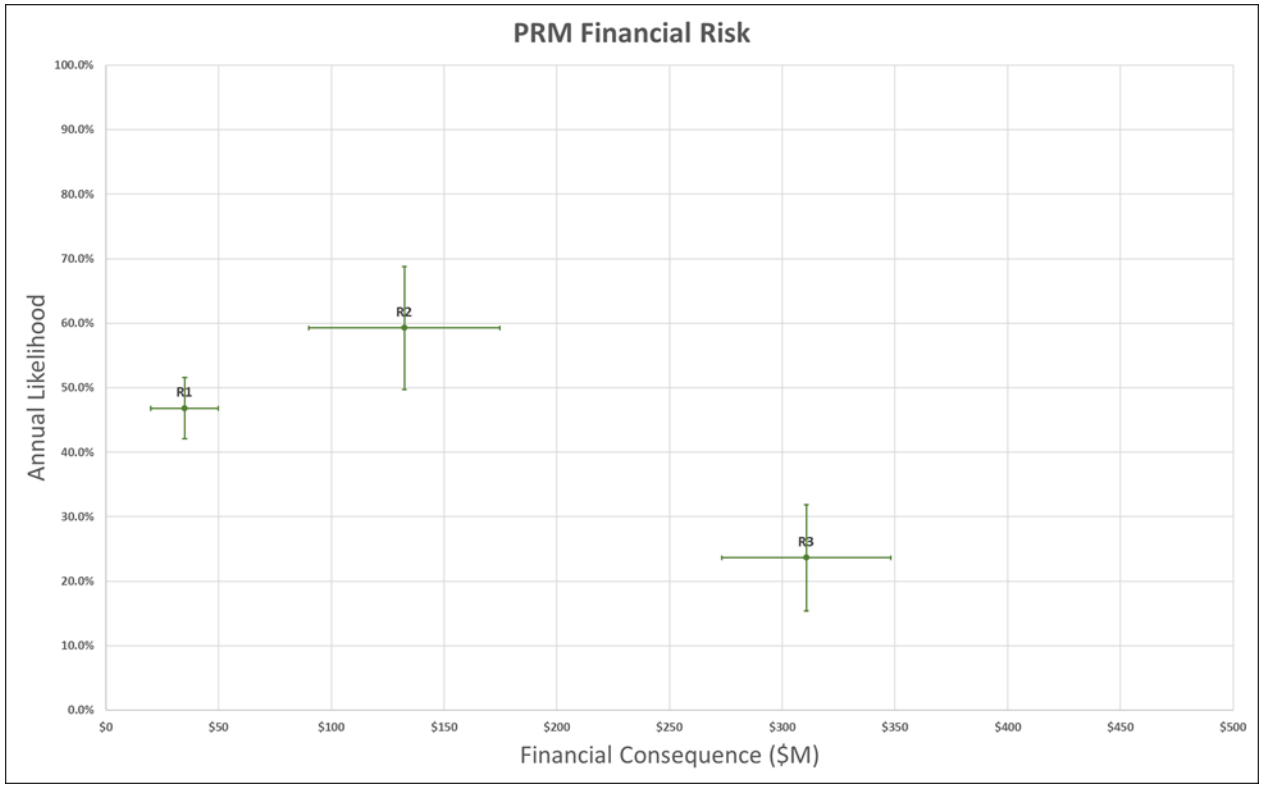
- Doing math with probability distributions requires Monte Carlo simulations
- Directly measures likelihood
  - Two separate inputs
- Output is given in terms of expected loss

PRM Assumptions

- PRM makes fewer assumptions than RA and RAU but understanding what they are is still important
  1. Analysts can accurately assess the probabilities of likelihood and consequence for the relevant cyber attacks
  2. Risk scenarios are independent, and a scenario's occurring does not change the risk that other scenarios will occur
  3. Weapon systems and aviation platform cyber risk likelihood and consequence can be reasonably modeled as Gaussian, or normal, probability distributions
  4. Fleetwide financial consequence multiplied by the percentage of systems affected across the fleet will yield financial consequence and this relationship is linear where 10% of the fleet affected will equal 10% of the fleetwide cost and 90% of the fleet affected will yield 90% of the fleetwide cost
  5. Fleetwide mission consequence multiplied by the percentage of systems affected across the fleet will yield financial consequence and this relationships is linear where 10% of the fleet affected will equal 10% of the fleetwide cost and 90% of the fleet affected will yield 90% of the fleetwide cost

SIMPLE UAS PRM EXAMPLE



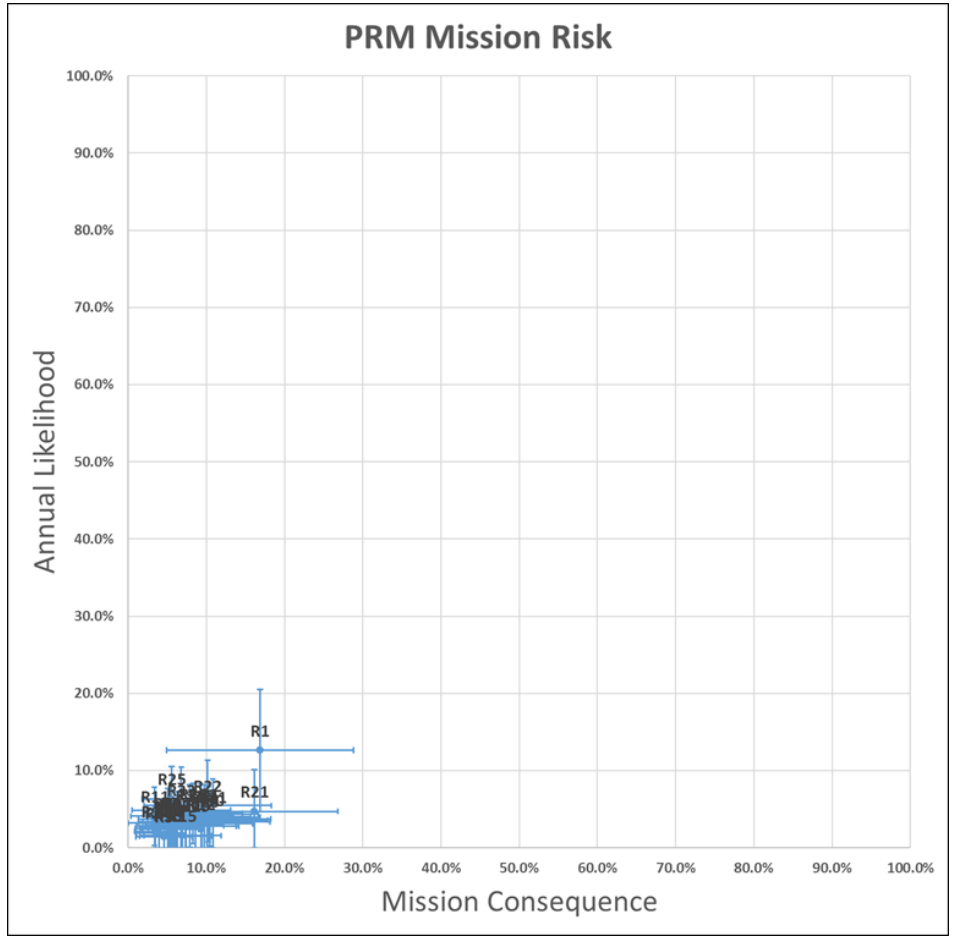


		Expected Mission Loss (EML)		
Risk Scenario	Short Description	Mean	90CI Low	90CI High
R1	Exfiltrate Mission Data	3.7%	2.3%	5.2%
R2	Denial of Service	26.5%	17.8%	35.3%
R3	Command Injection	21.4%	14.0%	28.8%

		Expected Financial Loss (EFL)		
Risk Scenario	Short Description	Mean	90CI Low	90CI High
R1	Exfiltrate Mission Data	$16.4	$9.2	$23.5
R2	Denial of Service	$78.1	$49.8	$106.5
R3	Command Injection	$73.5	$46.8	$100.3

MQ-99 Berserker PRM Mission Risk Results

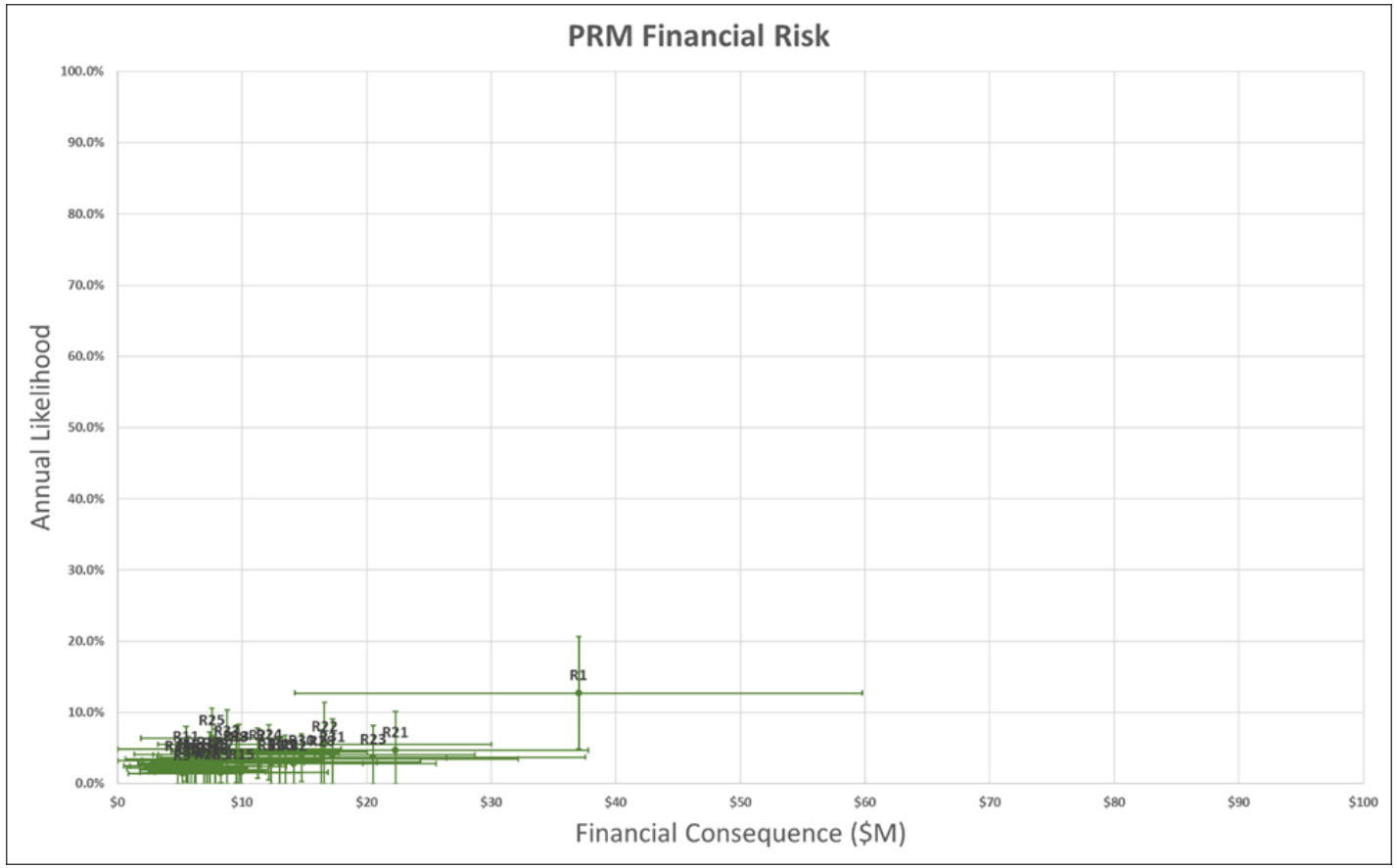
- In the PRM scoring R1 moved up in importance but risks were similar



Risk Scenario	Short Description	EML	Standard Deviation
R1	GCS supply chain soft production/transmission	2.140%	1.273%
R21	Mission computer supply chain OFP adversary control	0.754%	0.661%
R22	MX system via Internet tampering load OFPs	0.561%	0.476%
R2	AV comm link spoofing mission data	0.440%	0.294%
R31	Supply chain component take over data bus	0.435%	0.373%
R30	Supply chain MX system alter OFP loads	0.380%	0.283%
R8	Spoof C&C messages via hardware supply chain	0.379%	0.299%
R24	GPS position spoofing move AV	0.362%	0.274%
R25	GPS denial of service	0.358%	0.209%
R23	OFP Loading physical switch bypass	0.357%	0.354%
R28	Supply chain tampered component alter data	0.329%	0.324%
R33	Supply chain component denial of service data bus	0.326%	0.330%
R13	Wireless MX attack spoofing and tampering	0.325%	0.253%
R12	Supply chain software develop send location	0.292%	0.256%
R19	Spoof C&C message authorize weapons employment	0.250%	0.211%
R20	GSC supply chain OFP tampering manipulate comms	0.216%	0.190%
R17	AV comm link information disclosure position	0.208%	0.187%
R32	Supply chain tampering reduce engine life	0.204%	0.204%
R27	Spoof C&C messages via insecure comms	0.190%	0.151%
R7	RF attack on comm system inject false	0.178%	0.130%
R29	Supply chain tamper mission data load for RWR	0.164%	0.190%
R4	Insider support equip access to avionics	0.139%	0.121%
R14	AV comm link spoofing targeting data	0.137%	0.124%
R11	Supply chain comm system attack send location	0.136%	0.114%
R6	RF attack on comm system mislead EO/IR	0.136%	0.107%
R5	Insider plus crypto attack on GCS AV link	0.131%	0.133%
R18	AV crypto broken dive into target	0.124%	0.129%
R15	AV comm link spoofing weapon release	0.111%	0.111%
R3	Insider malicious mission computer info disclosure	0.093%	0.072%
R16	AV comm link spoofing jettison command	0.082%	0.082%
R26	Crypto attack datalink spoofing IADS data	0.080%	0.064%
R10	Spoof flight lead messages via insecure comms	0.074%	0.082%
R9	Spoof parachute deploy via insecure comms	0.066%	0.067%

MQ-99 Berserker PRM Financial Risk Results

- Large uncertainties highlight areas to examine
  - Decomposition, modeling, and testing could all be valuable and worthwhile



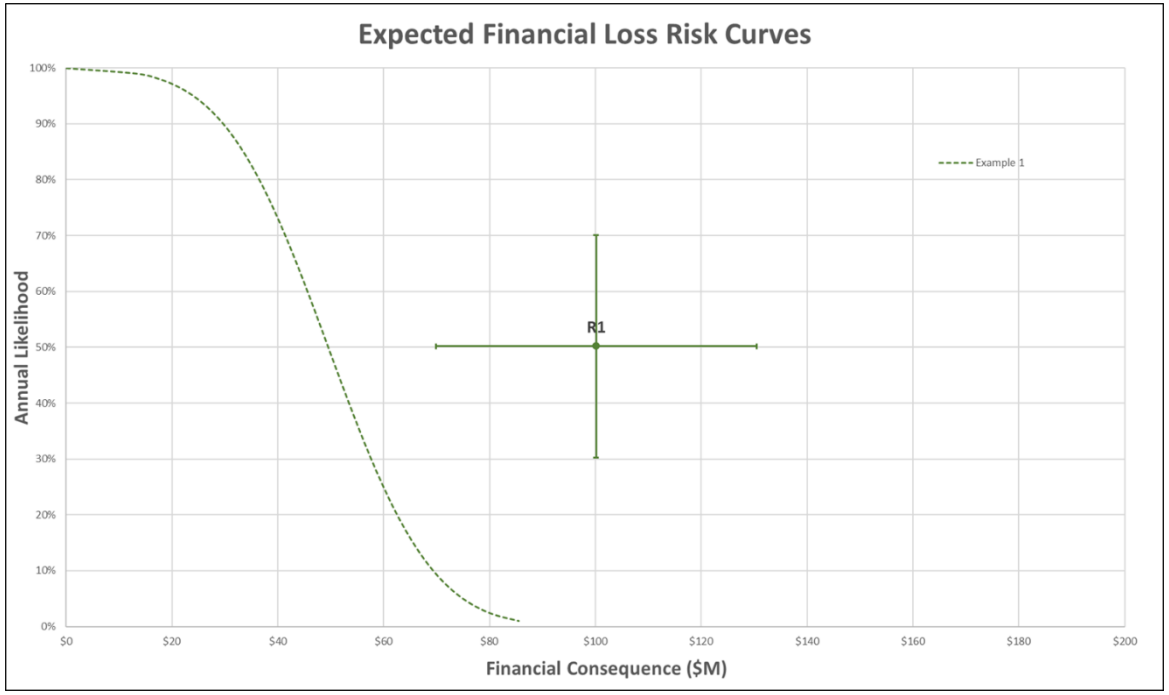
Risk Scenario	Short Description	EFL	Standard Deviation
R1	GCS supply chain soft production/transmission	$4.728	$2.601
R21	Mission computer supply chain OFP adversary control	$1.061	$0.916
R22	MX system via Internet tampering load OFPs	$0.917	$0.799
R23	OFP Loading physical switch bypass	$0.766	$0.732
R31	Supply chain component take over data bus	$0.700	$0.637
R28	Supply chain tampered component alter data	$0.571	$0.581
R30	Supply chain MX system alter OFP loads	$0.534	$0.419
R24	GPS position spoofing move AV	$0.531	$0.370
R25	GPS denial of service	$0.483	$0.308
R2	AV comm link spoofing mission data	$0.480	$0.306
R33	Supply chain component denial of service data bus	$0.422	$0.439
R12	Supply chain software develop send location	$0.418	$0.396
R32	Supply chain tampering reduce engine life	$0.400	$0.380
R8	Spoof C&C messages via hardware supply chain	$0.397	$0.317
R13	Wireless MX attack spoofing and tampering	$0.396	$0.300
R20	GSC supply chain OFP tampering manipulate comms	$0.386	$0.326
R19	Spoof C&C message authorize weapons employment	$0.341	$0.291
R17	AV comm link information disclosure position	$0.245	$0.220
R27	Spoof C&C messages via insecure comms	$0.244	$0.217
R29	Supply chain tamper mission data load for RWR	$0.244	$0.302
R11	Supply chain comm system attack send location	$0.229	$0.176
R7	RF attack on comm system inject false	$0.185	$0.144
R18	AV crypto broken dive into target	$0.182	$0.189
R15	AV comm link spoofing weapon release	$0.160	$0.160
R4	Insider support equip access to avionics	$0.156	$0.143
R6	RF attack on comm system mislead EO/IR	$0.149	$0.118
R5	Insider plus crypto attack on GCS AV link	$0.147	$0.156
R26	Crypto attack datalink spoofing IADS data	$0.132	$0.112
R14	AV comm link spoofing targeting data	$0.130	$0.110
R3	Insider malicious mission computer info disclosure	$0.127	$0.101
R16	AV comm link spoofing jettison command	$0.120	$0.115
R10	Spoof flight lead messages via insecure comms	$0.119	$0.139
R9	Spoof parachute deploy via insecure comms	$0.074	$0.079

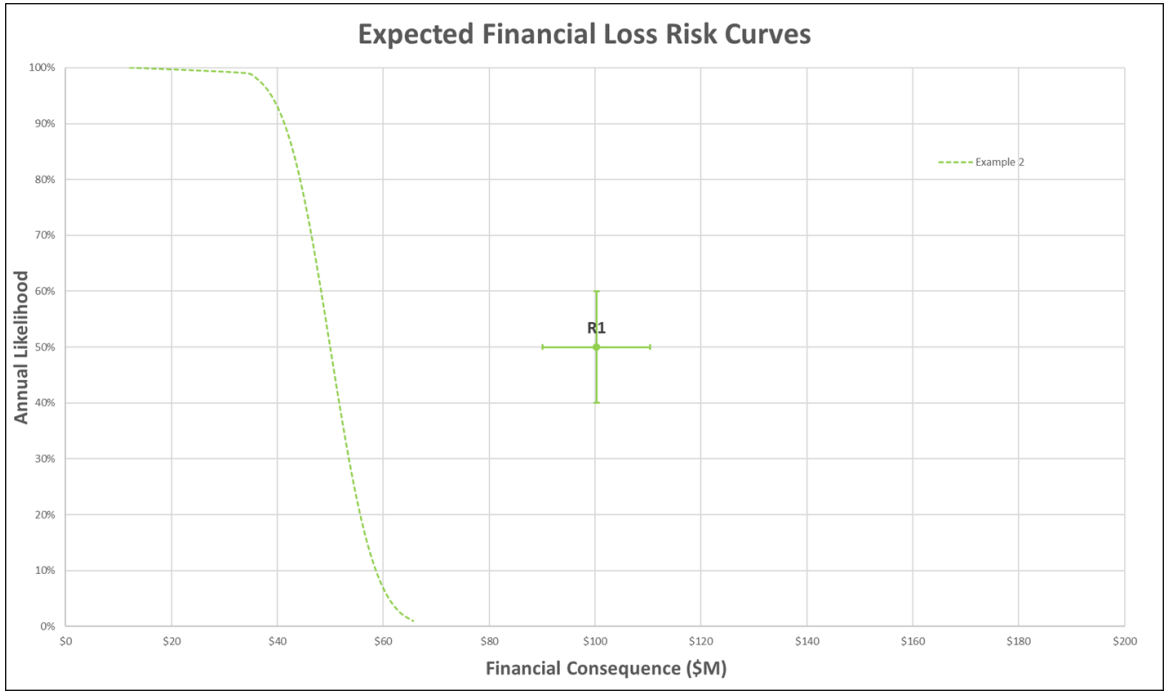
COMBINING RISKS

- Each risk assessment and measurement tool also has a tool that enables the combination of risks via a Monte Carlo simulation
  - Multiple risks are allowed to either occur or not based on the probability distribution and random chance
  - Loss is pulled from the appropriate probability distribution for each risk that occurs
  - Losses in each “year” are added up
  - Simulation repeats thousands of times and an average is taken
- Results can be displayed on risk charts similar to previous examples
- Another option is to present risk as risk curves

RISK CURVES

- A visualization of risk using the same x and y axes as a risk chart
- Displays a continuous curve versus a central point with a distribution

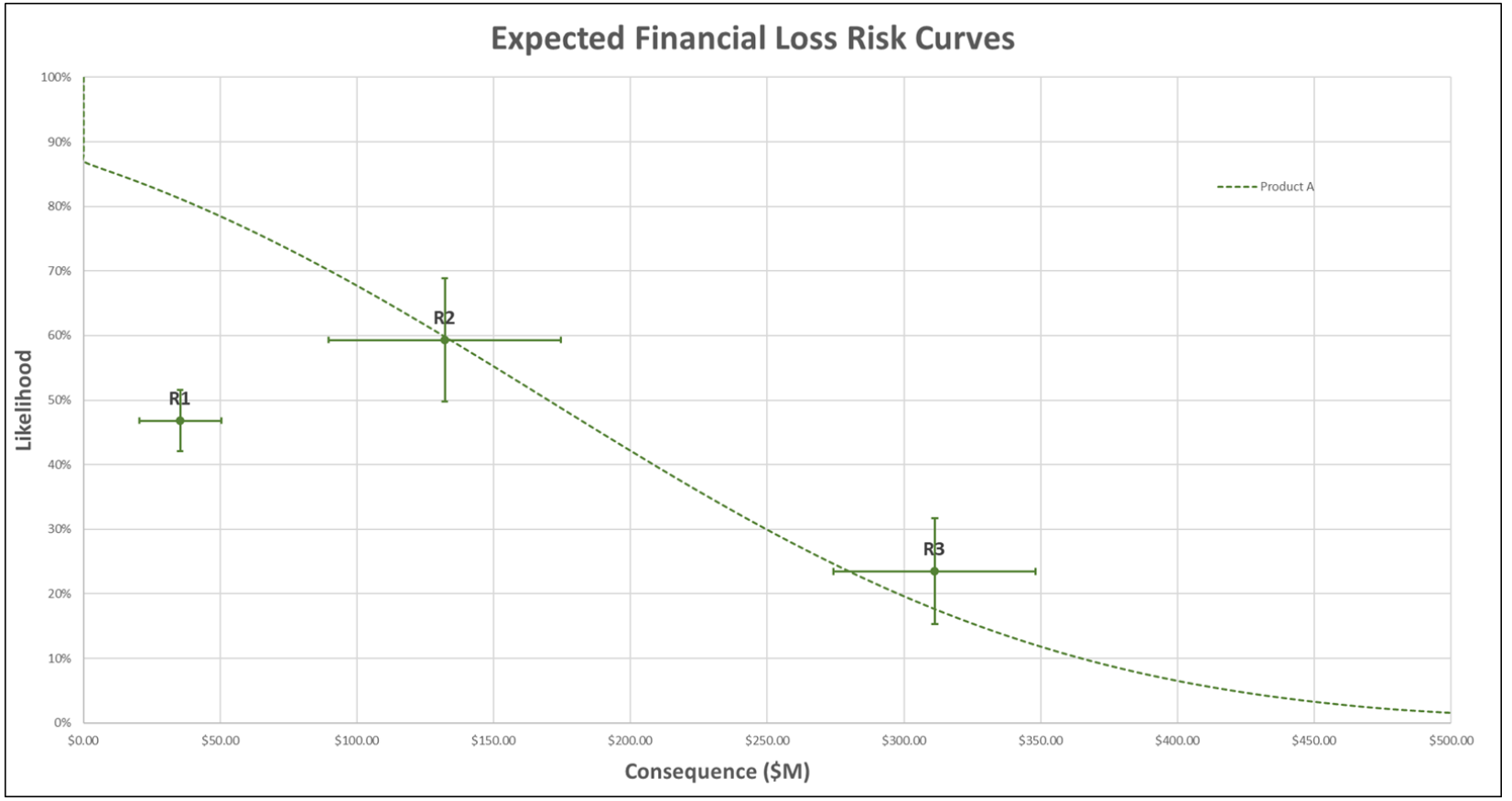




- Total area under the curve equals risk, shallower slope equals more uncertainty

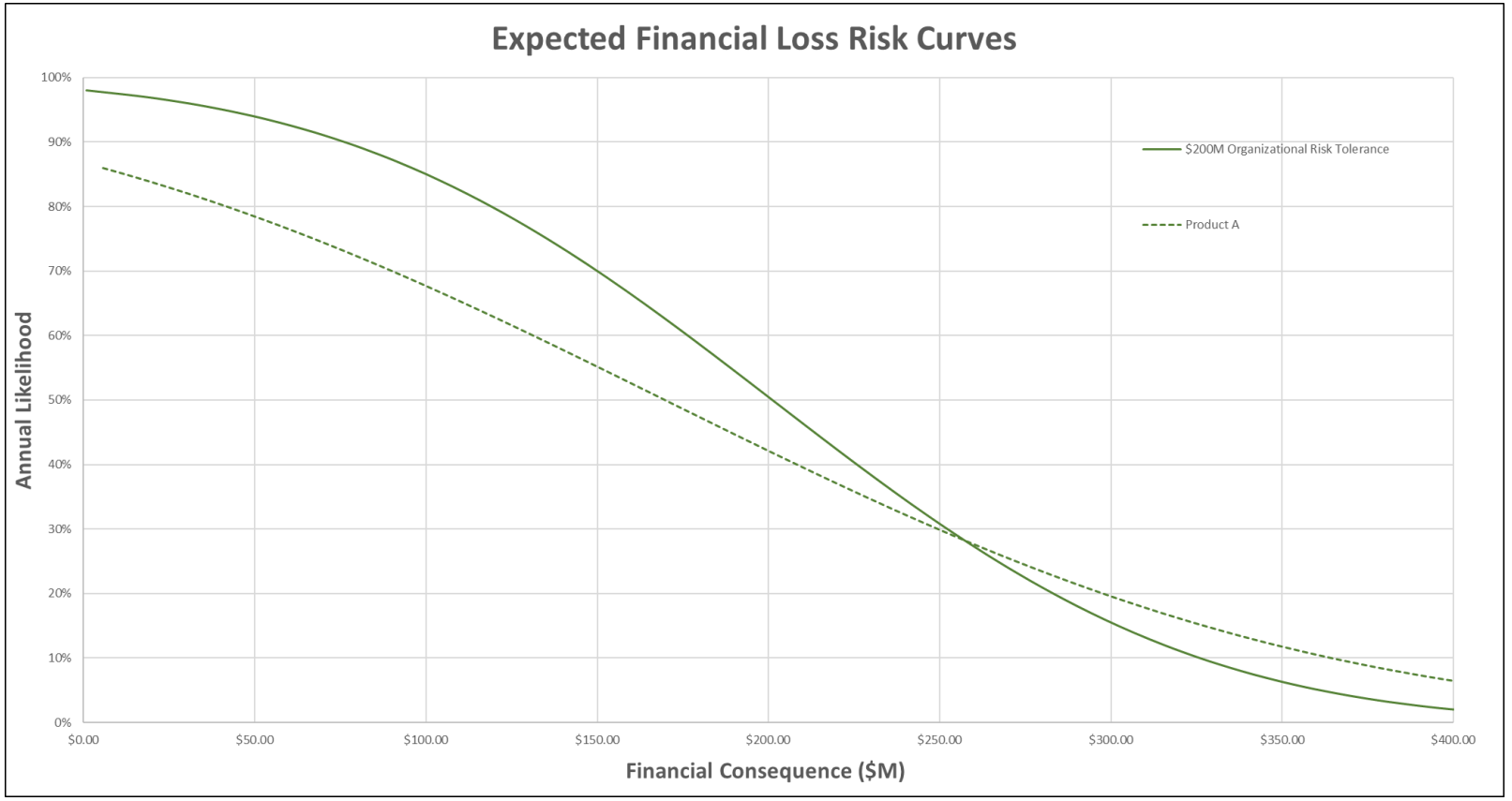
SIMPLE UAS EXAMPLE RISK CURVE

- Large uncertainties drive shallow slopes to risk curves
- Multiple spread out distributed risks create shallower risk curves as there are so many potential outcomes for each “year” of simulation



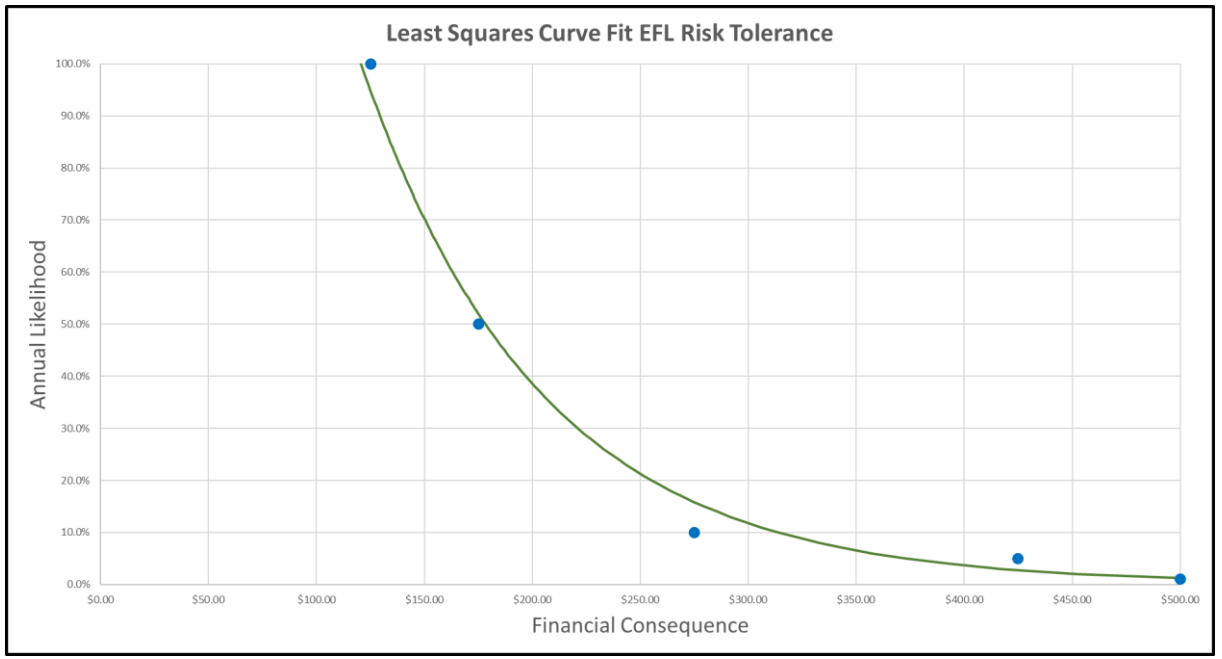
RISK TOLERANCE

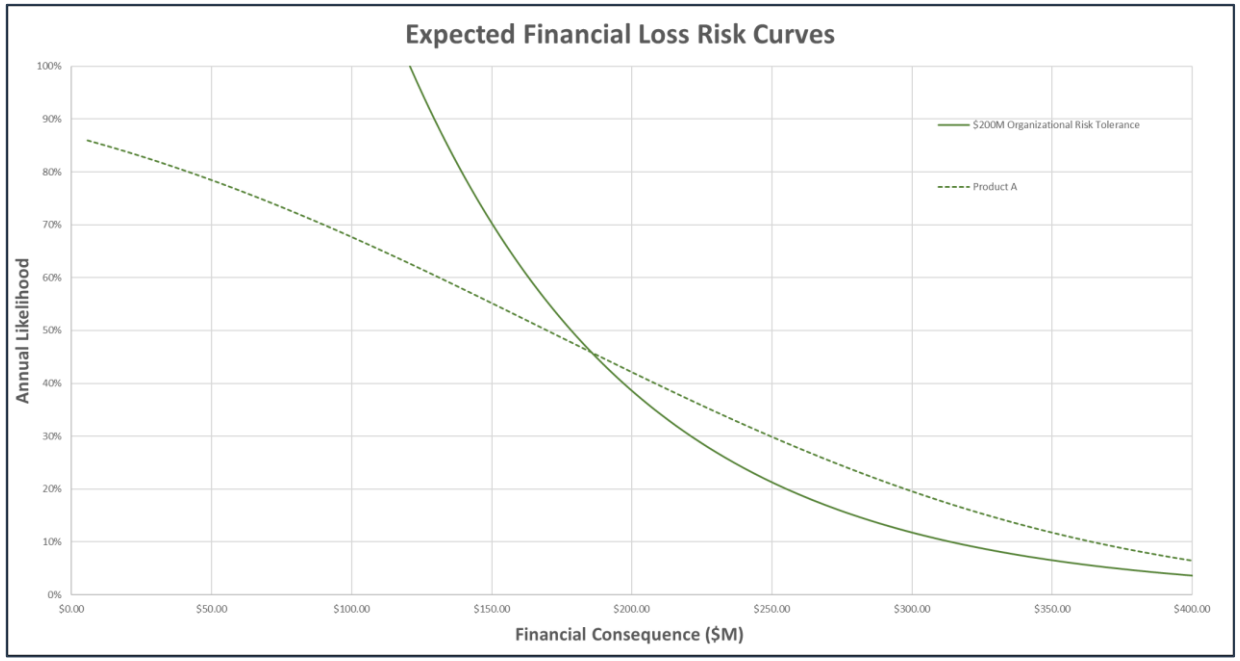
- The amount of risk an organization is willing to take on is its risk tolerance or risk acceptance
- If there is additional risk, something should be done to alter the risk or tolerance
- A simple “risk neutral” risk tolerance curve can be created by a single 90CI pair of values



Risk Tolerance 2

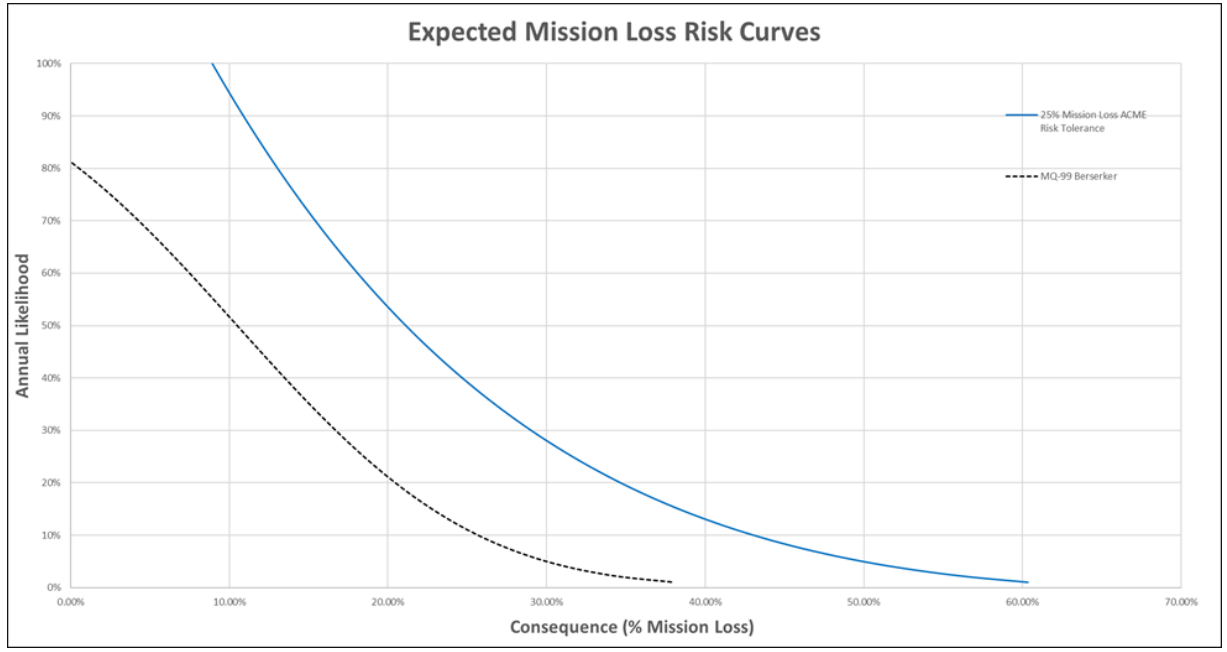
- However, most people are not “risk neutral” and would rather accept a 90% chance of losing $100 than a 0.9% chance of losing $10,000 despite their identical expected loss of $9
- To build a more accurate risk tolerance, determine with senior leaders how much risk they would be willing to accept at 4-5 points and then create a curve based on those points

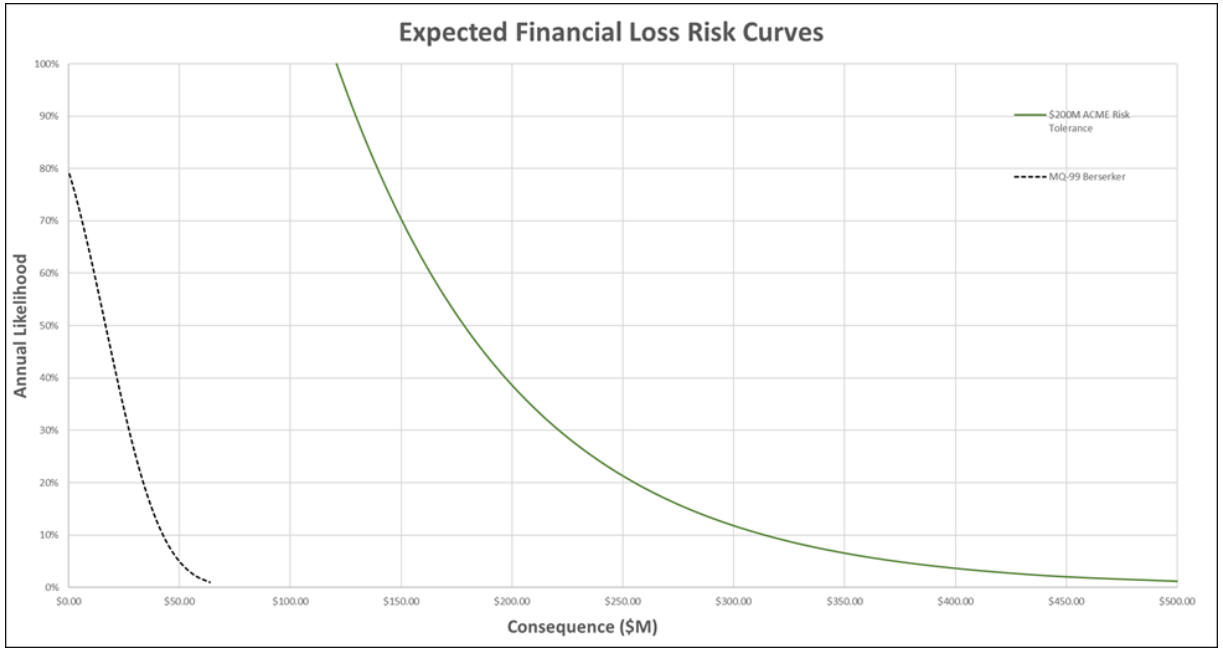




MQ-99 Berserker Risk Curves

- MQ-99 has a very low level of risk when compared to ACME aircraft corporation's $200M risk tolerance curve
- Due to robust secure design assumptions





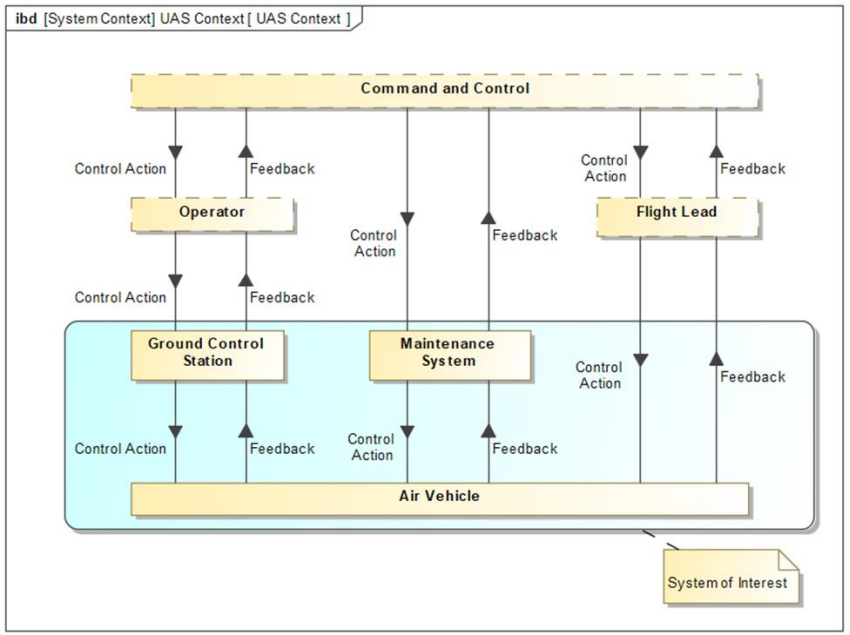
- Mission risk is potentially more problematic

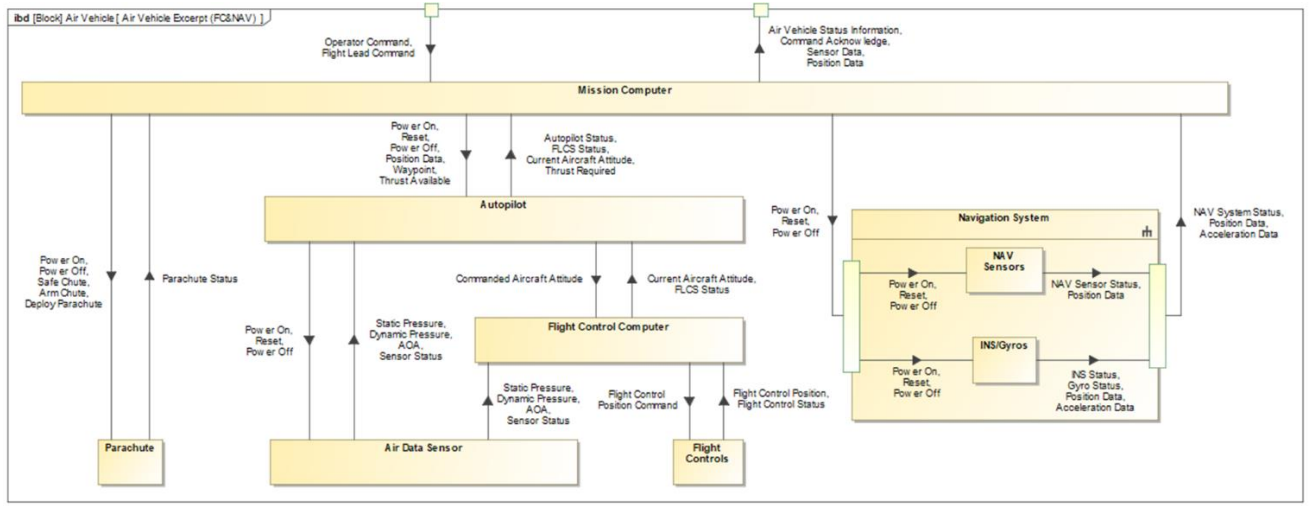
MQ-99 Berserker Risk Summary

- Five risks were in the top-10 of each risk tool
  - R1: GCS supply chain software production/transmission
  - R21: Mission computer OFP supply chain attack enabling adversary control
  - R22: Maintenance System tampering with OFP loading via an Internet attack
  - R31: Supply chain attack on component to take over the data bus
  - R30: Supply chain attack on maintenance loaders to alter OFP loads
- Several themes come out of just these five risks worth addressing
  - Supply chain risks
  - Highly connected components (i.e. maintenance systems)
- The residual risk is very low due to the robust design assumptions—if those change, there is potential for dramatic risk changes as well

URAMS AND MBSE

- MBSE is revolutionizing weapons system design
- URAMS can be implemented within MBSE tools and doing so provides significant benefits

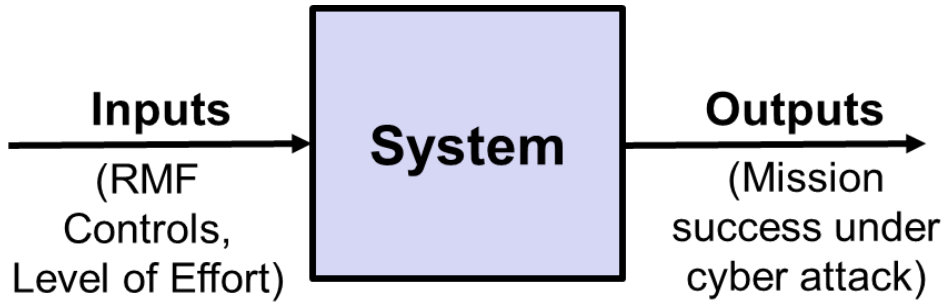




#	ID	Documentation	Caused Losses	Mitigated By
1	H-1	MQ-99 targets friendly or neutral objects or personnel	L-1 Loss of life or injury L-2 Significant damage to objects	SC-1 MQ-99 will only target hostiles
2	H-2	MQ-99 employs weapons too close to friendly or neutral objects or personnel	L-1 Loss of life or injury L-2 Significant damage to objects	SC-2 MQ-99 prevents unacceptable collateral damage
3	H-3	MQ-99 does not successfully destroy assigned targets.	L-3 Unable to destroy assigned targets	SC-3 MQ-99 successfully destroys assigned targets
4	H-4	MQ-99 does not fly required profile to stimulate desired hostile defense response.	L-4 Unable to decoy hostile air defenses	SC-4 MQ-99 executes required profile
5	H-5	MQ-99 operates outside of established operational envelope	L-1 Loss of life or injury L-2 Significant damage to objects L-3 Unable to destroy assigned targets L-4 Unable to decoy hostile air defenses	SC-5 MQ-99 only operates inside established ops envelope
6	H-6	MQ-99 presents electrical, chemical, or kinetic hazards to friendly personnel or objects in the vehicle's immediate vicinity.	L-1 Loss of life or injury L-2 Significant damage to objects	SC-6 MQ-99 will not present electrical, chemical, kinetic hazards

URAMS AND RMF

- RMF is a certainty for DoD programs
- The largest problem with RMF is how late it happens in the lifecycle and that it measures inputs into a complex system and assumes outputs



- URAMS is not RMF, but it can greatly facilitate creating RMF artifacts
- URAMS provides a defensible analytical way of doing tailoring
- Instead of adding RMF as a security process after design is completed, URAMS enables security to be baked in from the beginning and then to take credit for it in RMF
- Multiple alternate RMF pathways exist that are even more flexible and amenable to URAMS driven tailoring, USAF's Fast Track ATO is a good example of this

CONCLUSIONS

- The lack of agreement on risk assessment and measurement is one of the most pressing issues with weapon systems cybersecurity
- URAMS provides a suite of qualitative and quantitative tools that can fill this need by offering:
  - Starts with rigorous engineering analysis using STPA-Sec
  - Qualitative single-point analysis with RA & CRA
  - Qualitative three-point analysis with RAU & CRAU
  - Quantitative analysis with PRM & CPRM
  - Comparison of results across tools
- It can help drive a secure design from concept forward
- It provides a quicker and easier way to gain accreditation based on the secure design that has already been accomplished

Thank you for your time

Please reach out with any questions

Dr. Bill “Data” Bryant
bill.bryant@mtsi-va.com

MRAP-C AND URAMS