32nd Annual INCOSE international symposium

hybrid event

Detroit, MI, USA
June 25 - 30, 2022

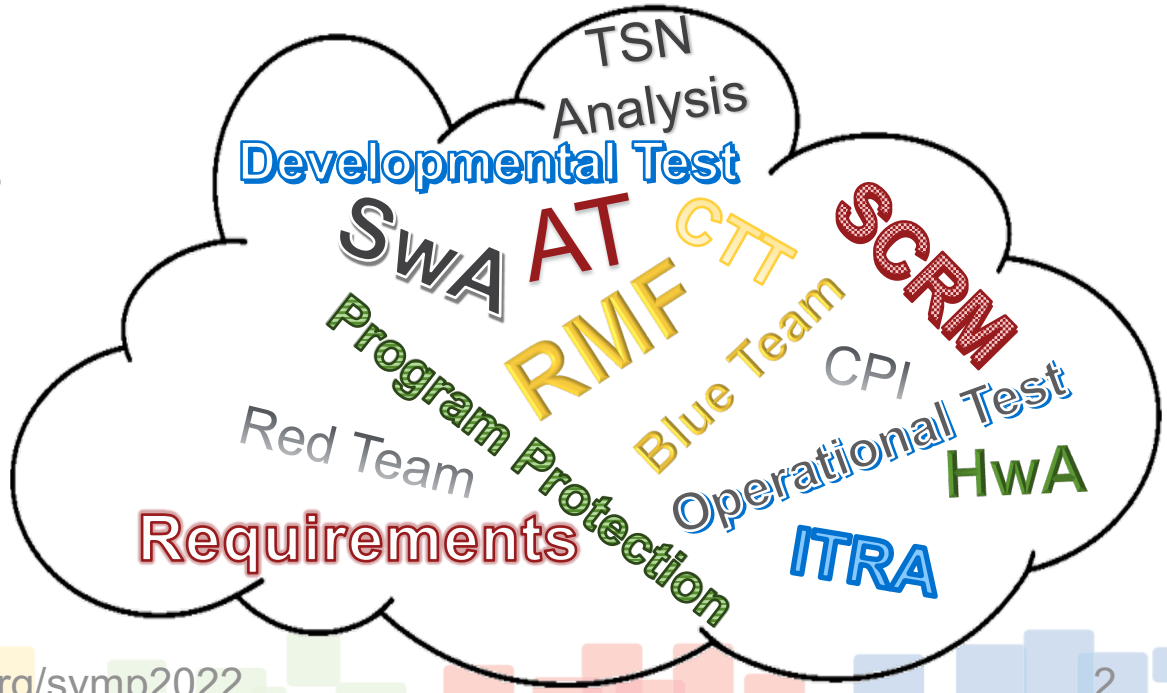
Cutting the Gordian Knot

# The Unified Risk Assessment and Measurement System (URAMS™)

www.incose.org/symp2022

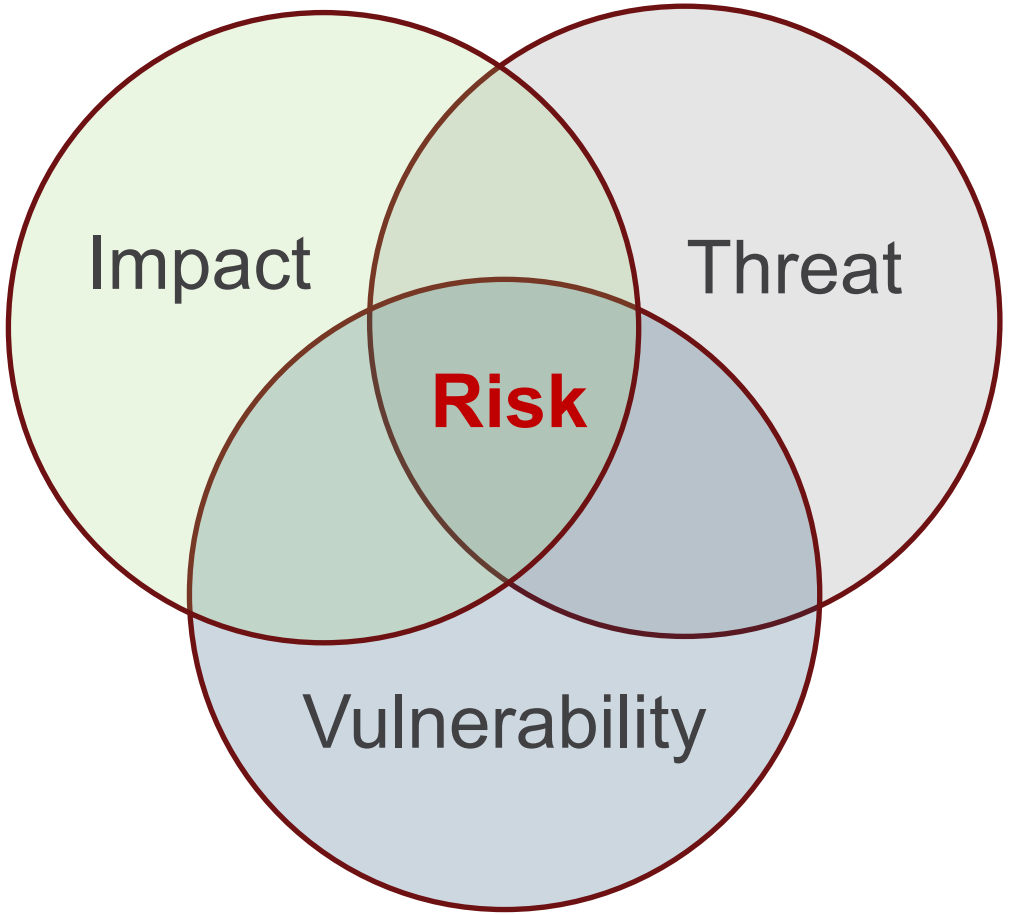
# What's the Problem?

- There is no widely accepted way to effectively measure the risk of cyber attacks on cyber physical systems such as aviation platforms
  - 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
- If we could measure risk in a meaningful way—we would have a much better path forward



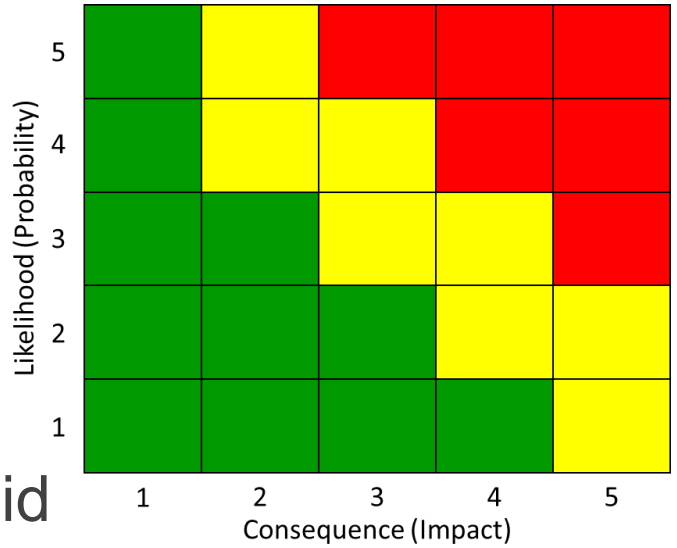
# What is “Risk”?

- 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
- 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



# Risk Measurement Inputs

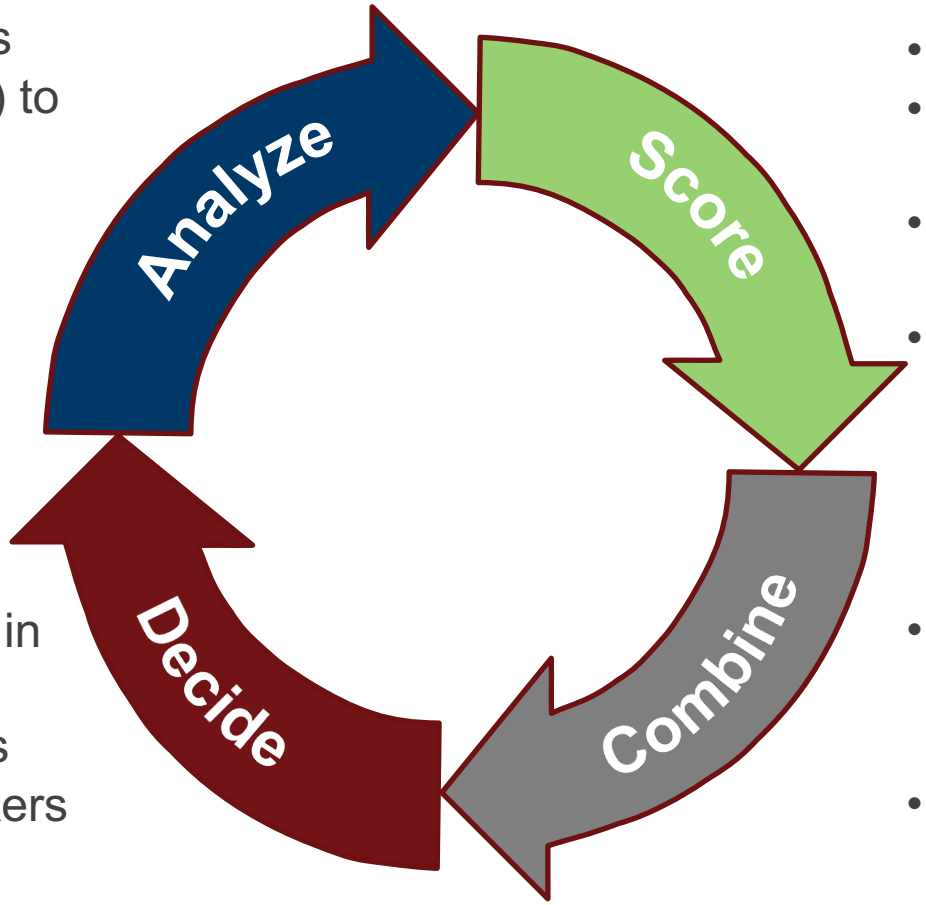
- There are two measurement instruments currently available
  - Human SMEs
  - Algorithms/AI
- Both have advantages and disadvantages

- Algorithms are very good at finding specific things in an ocean and they are fast, consistent, and natively unbiased
- Humans are very good at integrating fragmentary data elements—combine the two, but humans have the final say

# 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




**Score**

- Score the risk from scenarios
- Can utilize qualitative or quantitative risk assessment tools
- Some tools include the capability to also score uncertainty
- Inputs are from various types of Subject Matter Experts (SMEs)

**Decide**

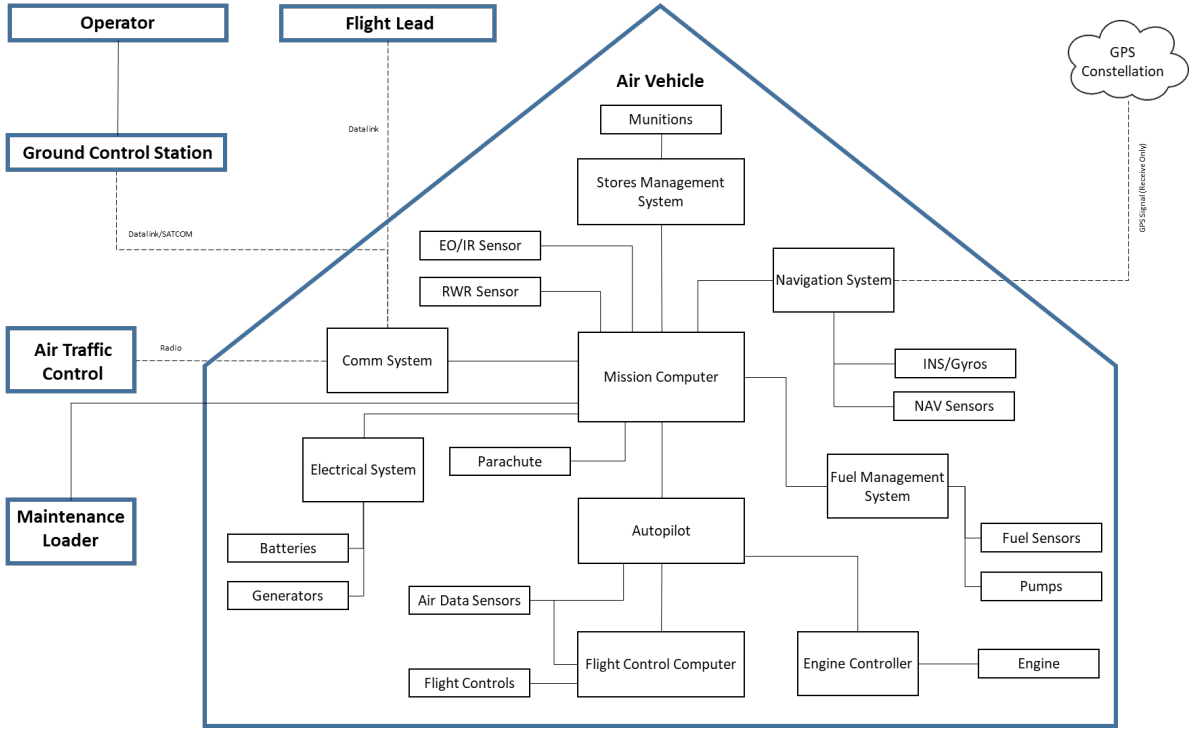
- Presents risk to decision makers in a clearly understandable way
- Uses structured assurance cases
- Provides options to decision makers on how to address risk

**Combine**

- Utilizes a range of tools to combine risks depending on what tools were used to score the risks
- Provides an understanding of the total level of risk for a system

# Notional Example: MQ-99 Berserker UAS

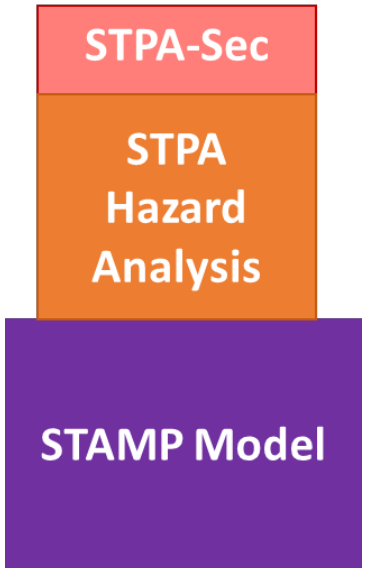
- Completely notional example UAS based on an artist's depiction
- Any resemblance to a real system is completely coincidental
- System is at the conceptual stage of design



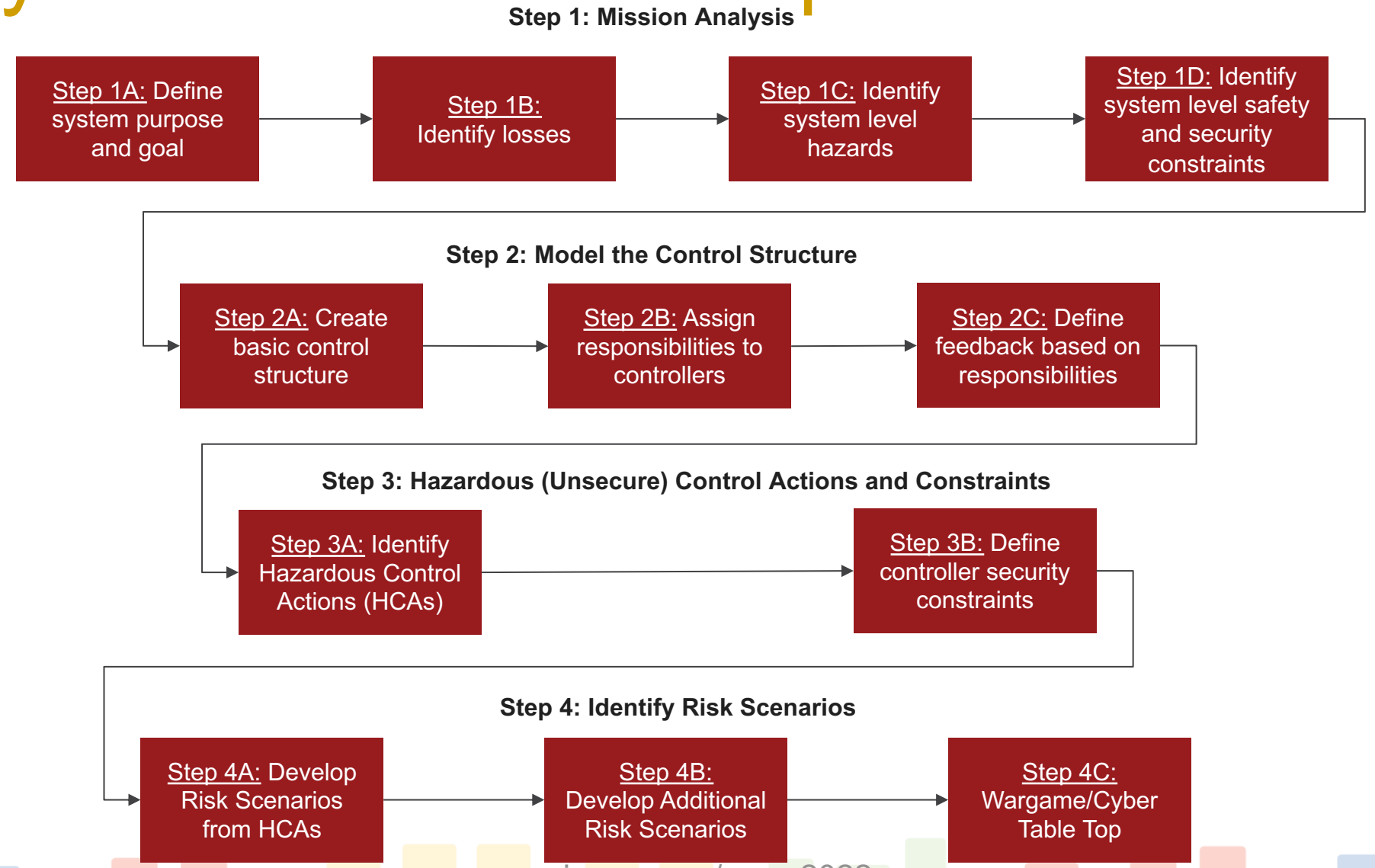

- Basic CONOPS & architecture developed
- Air-to-Air and Air-to Ground roles
- Can be semi-autonomous, controlled from ground station or by an airborne manned platform
- Attritable with remote ops location

# Analyze—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 an emergent property of complex systems vs. only looking at the component level
  - Many years of experience with very positive results
- 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



# Analyze—STPA-Sec Steps



# 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] |

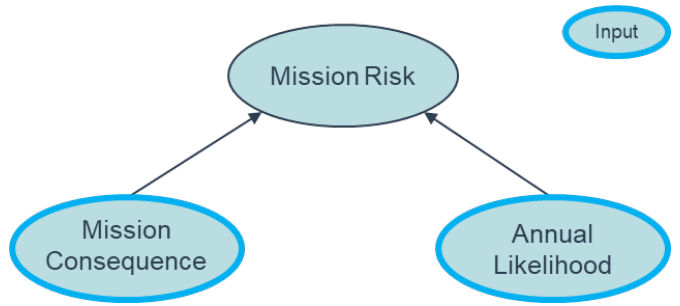
# Score—Risk Scoring Toolkit

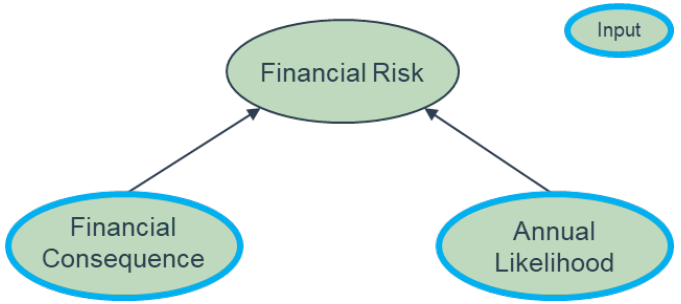
- All URAMS risk scoring tools can characterize risk in terms of mission loss, financial loss, or both, units = Expected Mission/Financial Loss (EML/EFL)
- Tools are characterized by a model of what components make up risk and what format the inputs to those components take
  - Model options include: 2-Factor (2F), 3-Factor (3F), 4-Factor (4F), and 7-Factor (7F)
  - Input options include: single-point (-1), confidence (-2), three-point (-3), and 90% confidence interval (-9)
- Other tools can be utilized as well
  - Clear model of factors → risk
  - Scoring should be 0-1.0
- With those two elements, any risk scoring system can combine individual risks into overall risk

| | 2-Factor | 3-Factor | 4-Factor | 7-Factor |
|---|---|---|---|---|
| **Single-Point** | 2F-1 | 3F-1 | 4F-1 | 7F-1 |
| **Confidence** | 2F-2 | 3F-2 | 4F-2 | 7F-2 |
| **Three-Point** | 2F-3 | 3F-3 | 4F-3 | 7F-3 |
| **90% CI** | 2F-9 | 3F-9 | 4F-9 | 7F-9 |

# 2-Factor Risk Model (2F)

- 2F is the simplest risk model short of directly assessing risk and is broadly accepted
- While 2F is simple, it is not easy as it requires SMEs to directly and correctly estimate mission consequence and likelihood
- 2F comes closest to standard risk cubes but uses ratio scoring (0-1.0, $0-$X)
- What type of operation are included in the annual year must be defined

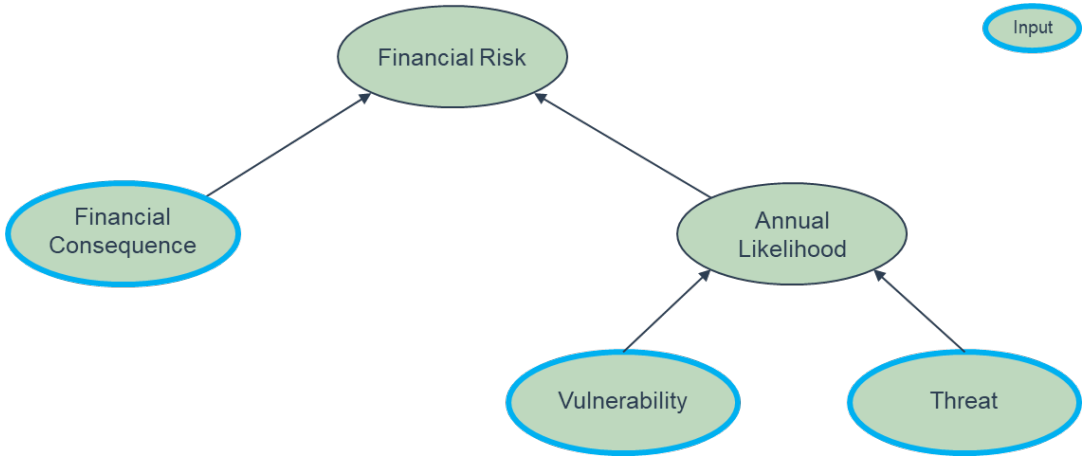


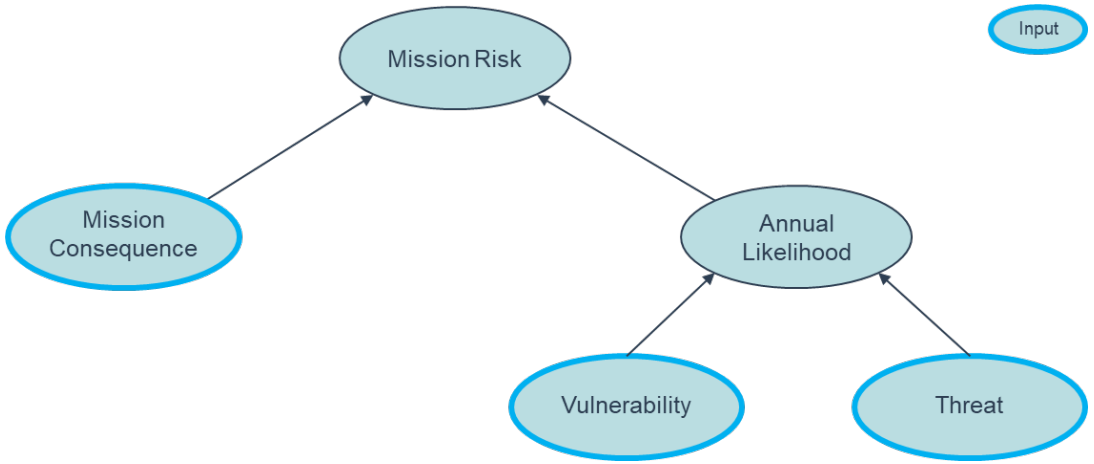




- The other risk scoring models that will be presented all accept these relationships, but add an additional layer of factors underneath consequence and likelihood

# 3-Factor Risk Model (3F)

- 3F is based on DoD's TSN analysis that is widely used
- 3F models annual likelihood as vulnerability multiplied by threat

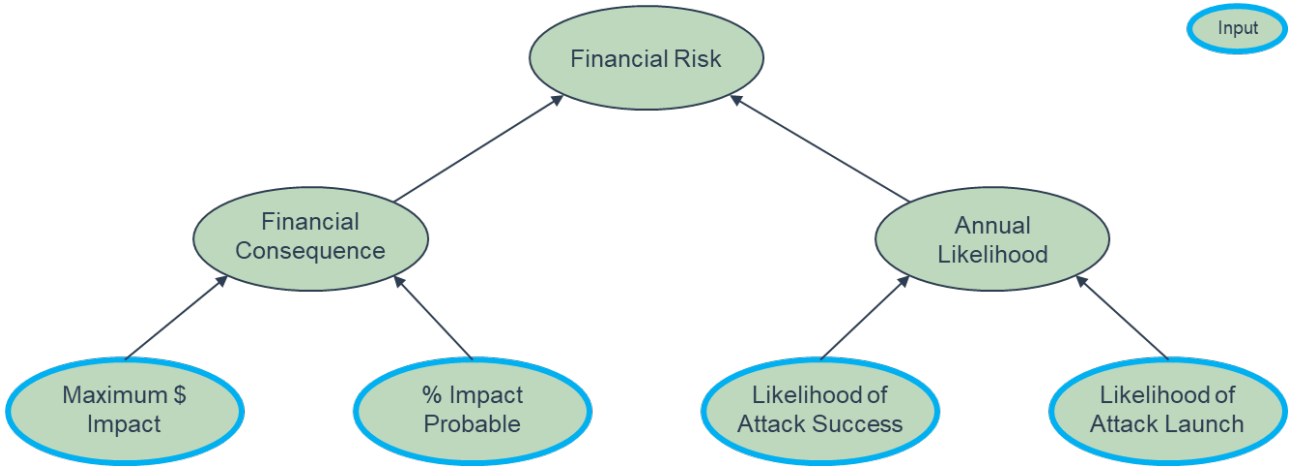


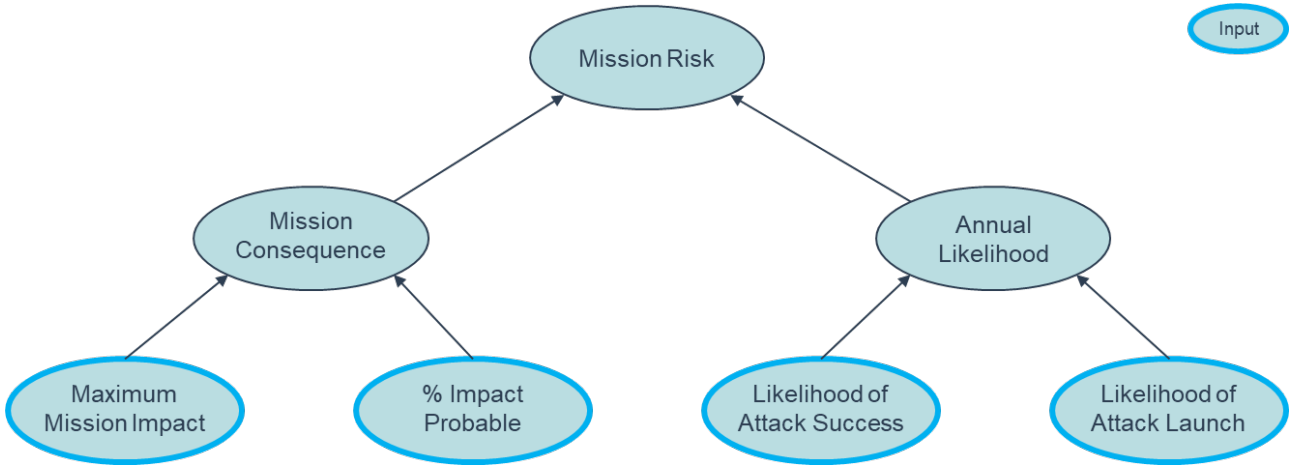




- Much like 2F, 3F requires analysts to accurately assess high-level abstract factors
  - TSN analysis has some tools to help with this

# 4-Factor Risk Model (4F)

- From experience, 4F bases consequence on two factors
  - How bad the attack could be
  - Multiplied by the percentage of that maximum impact expected

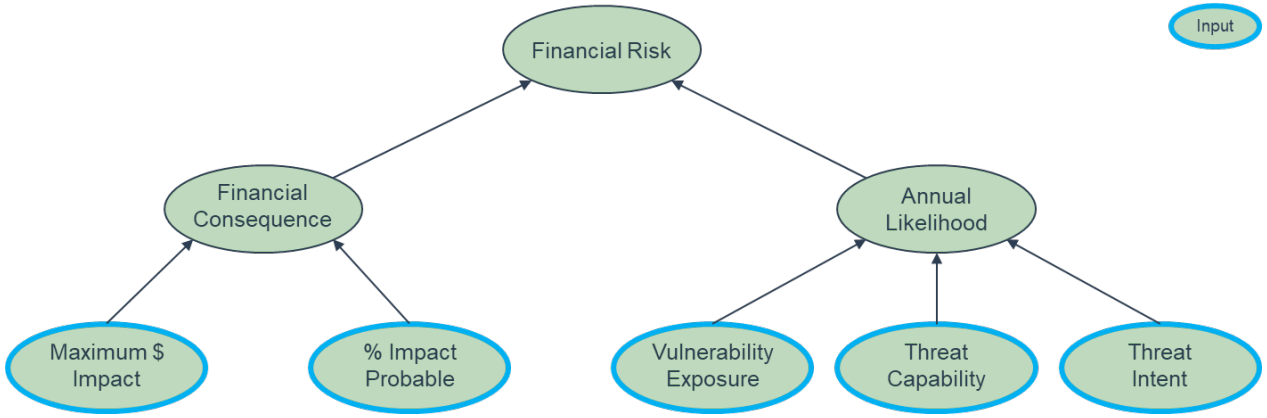


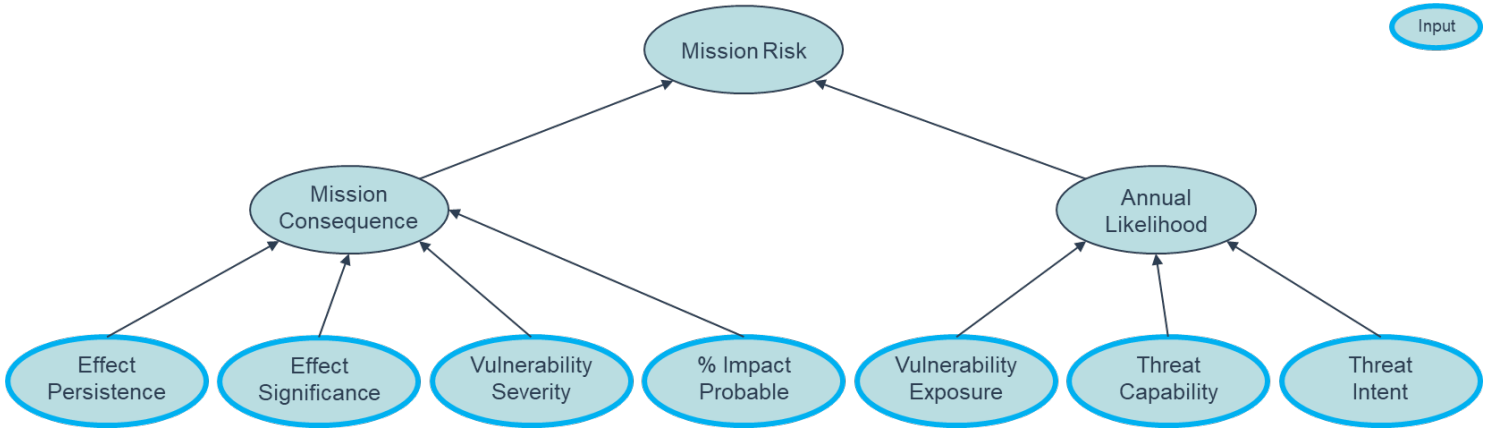




- Annual likelihood combines:
  - The likelihood of attack launch
  - The likelihood of success if it is launched
- Likelihood of attack launch should ideally come from Intel

# 7-Factor Risk Model (7F)

- 7F uses the same concepts of 4F but adds two critical assumptions
  - Fleet mission consequence equals effect persistence x effect significance x vulnerability severity
  - Likelihood equals vulnerability exposure x threat capability x threat intent

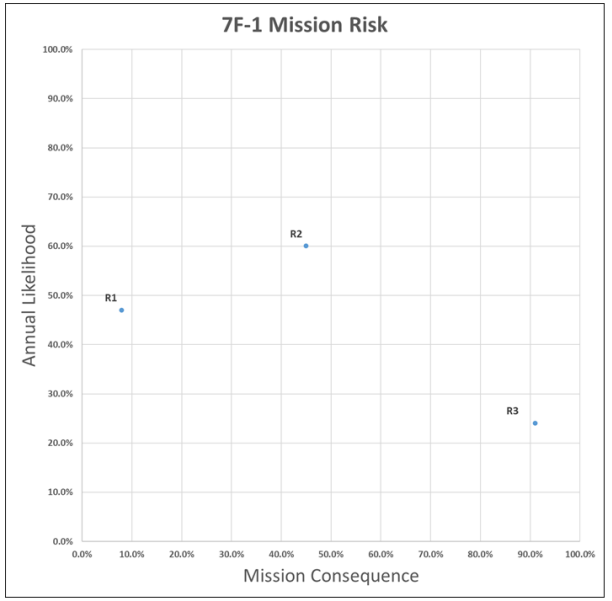


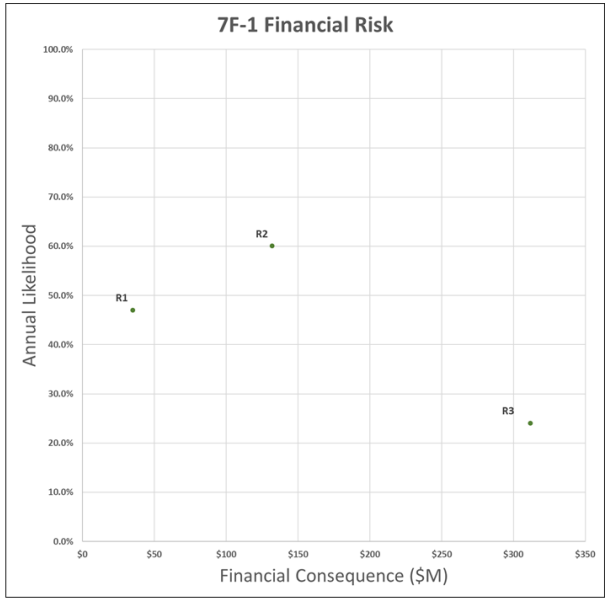




- 7F provides more support to analysts by analytic decomposition
- However, increased assumptions may mean less accuracy

# Single Point Estimation (-1)

- Any of the risk models can be scored using any of the potential input types
- Single point estimation is the most common where a single value is provided for each input
  - Must be from 0.0 – 1.0
- Output looks very similar to a traditional risk cube
- No assessment of uncertainty is provided



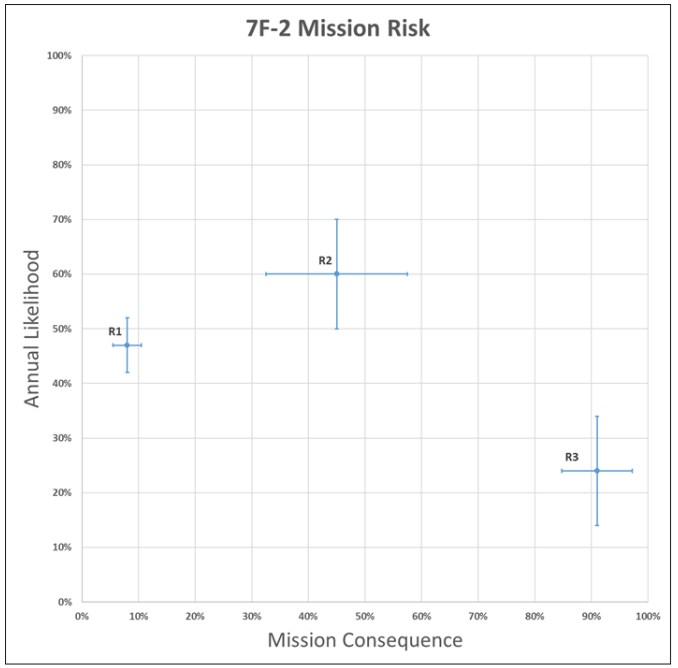



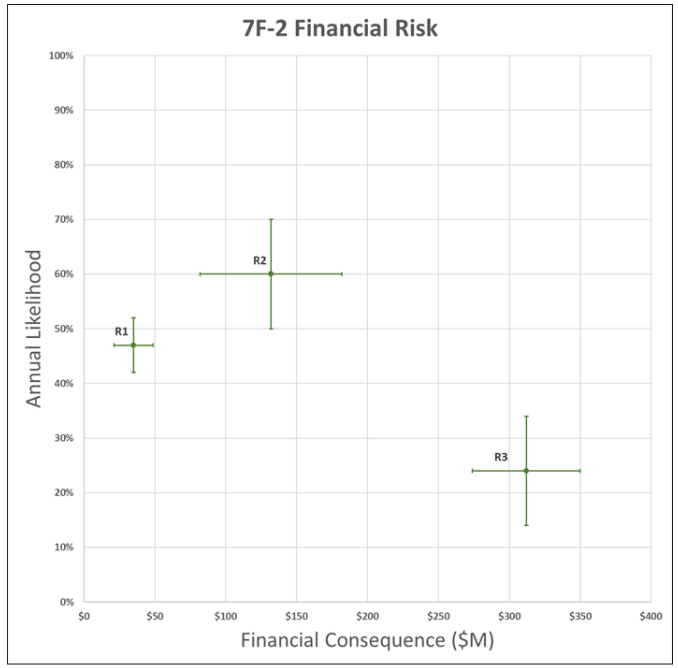

| Risk Scenario | Short Description | Expected Mission Loss (EML) Expected |
|---|---|---|
| R1 | Exfiltrate Mission Data | 0.0358 |
| R2 | Denial of Service | 0.2568 |
| R3 | Command Injection | 0.2077 |

| Risk Scenario | Short Description | Expected Financial Loss (EFL) Expected |
|---|---|---|
| R1 | Exfiltrate Mission Data | $16.5 |
| R2 | Denial of Service | $79.2 |
| R3 | Command Injection | $74.9 |

# Single Point Plus Confidence (-2)

- -2 adds in a qualitative score provided by the assessor that gives a level of confidence in the inputted score
- This can then be carried through the calculations and provides a visual “error bar” that shows comparative uncertainty
  - Qualitative only



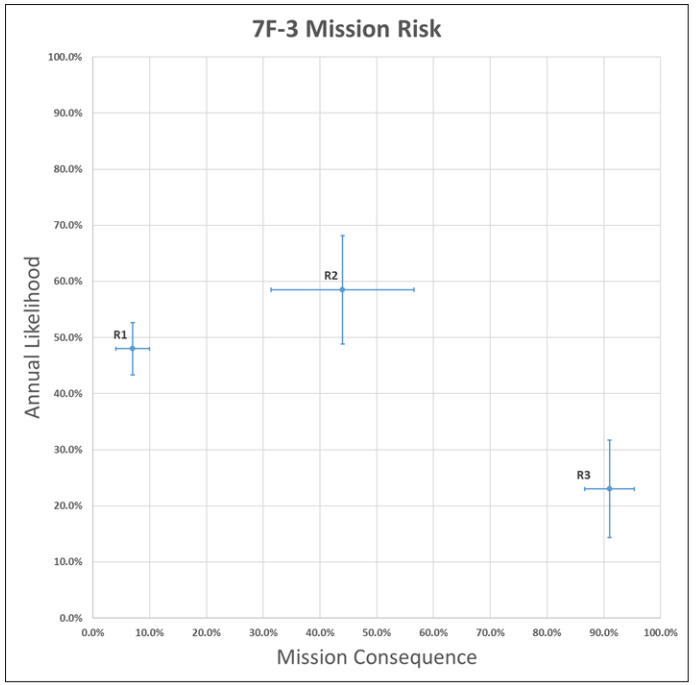



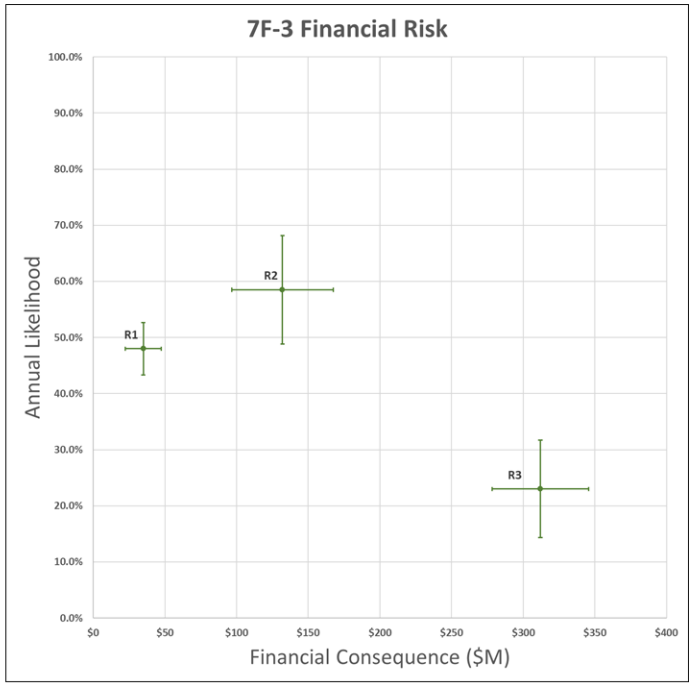

| | | Expected Mission Loss (EML) | |
|---|---|---|---|
| Risk Scenario | Short Description | Expected | Confidence |
| R1 | Exfiltrate Mission Data | 3.4% | 95.0% |
| R2 | Denial of Service | 25.7% | 75.0% |
| R3 | Command Injection | 20.9% | 87.5% |

| | | Expected Financial Loss (EFL) | |
|---|---|---|---|
| Risk Scenario | Short Description | Expected | Confidence |
| R1 | Exfiltrate Mission Data | $16.8 | 93.1% |
| R2 | Denial of Service | $77.2 | 75.0% |
| R3 | Command Injection | $71.8 | 81.0% |

# Three Point Estimation (-3)

- -3 utilizes three-point estimation with an expected-, best-, and worst-case value for each risk model input
- With the added assumption that risk is a Gaussian distribution, 90% confidence intervals can be created
  - Still a qualitative assessment of uncertainty



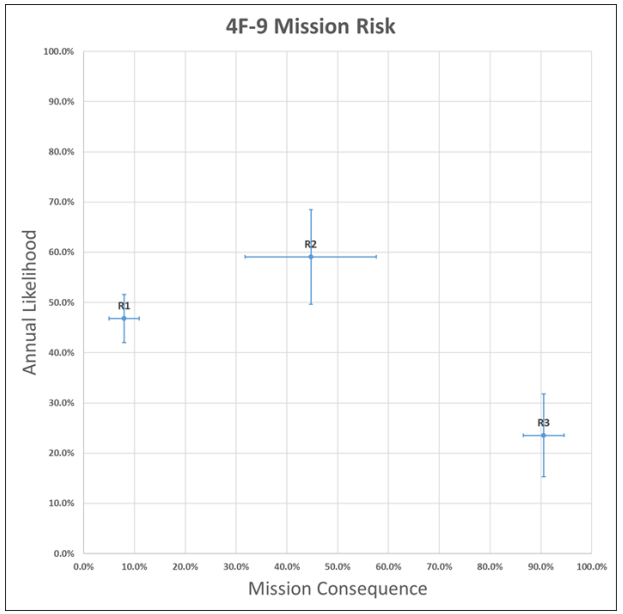



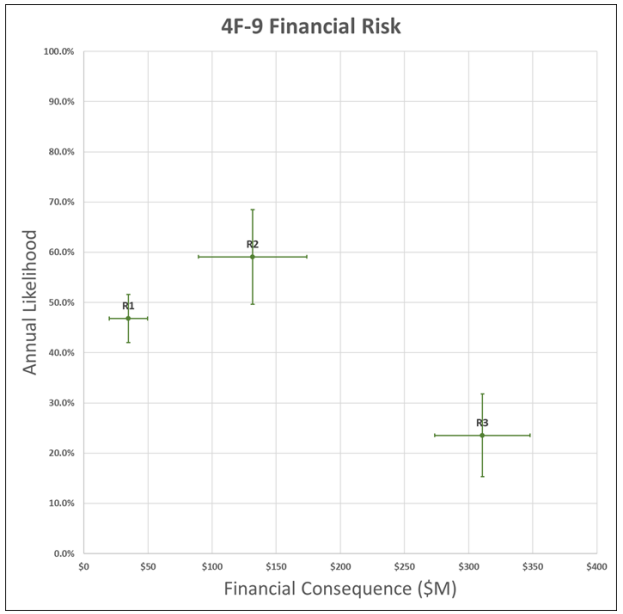

| | | Expected Mission Loss (EML) | | |
|---|---|---|---|---|
| Risk Scenario | Short Description | Expected | 90CI Low | 90CI High |
| R1 | Exfiltrate Mission Data | 3.4% | 1.6% | 5.1% |
| R2 | Denial of Service | 25.7% | 13.9% | 37.6% |
| R3 | Command Injection | 20.9% | 12.1% | 29.8% |

| | | Expected Financial Loss (EFL) | | |
|---|---|---|---|---|
| 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 |

# 90% Confidence Intervals (-9)

- -9 takes all inputs in the form of a 90% confidence interval (90CI)
  - e.g. the SME is 90% confident that the answer lies between 30% and 60% instead of providing the point value of 45%
- Research clearly shows that calibration is required for accurate 90CI assessment
  - ~85% can be calibrated in ½ day
  - Qualitative without calibration



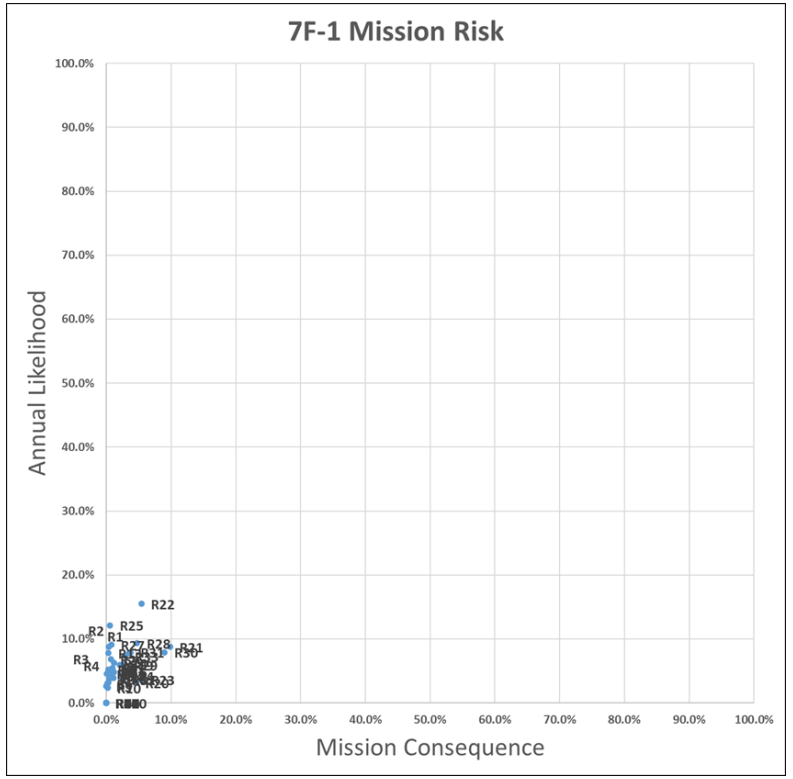




| | | Expected Mission Loss (EML) | | |
|---|---|---|---|---|
| Risk Scenario | Short Description | Mean | 90CI Low | 90CI High |
| R1 | Exfiltrate Mission Data | 3.7% | 2.3% | 5.2% |
| R2 | Denial of Service | 26.5% | 17.8% | 35.3% |
| R3 | Command Injection | 21.4% | 14.0% | 28.8% |

| | | 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 Example 7F-1

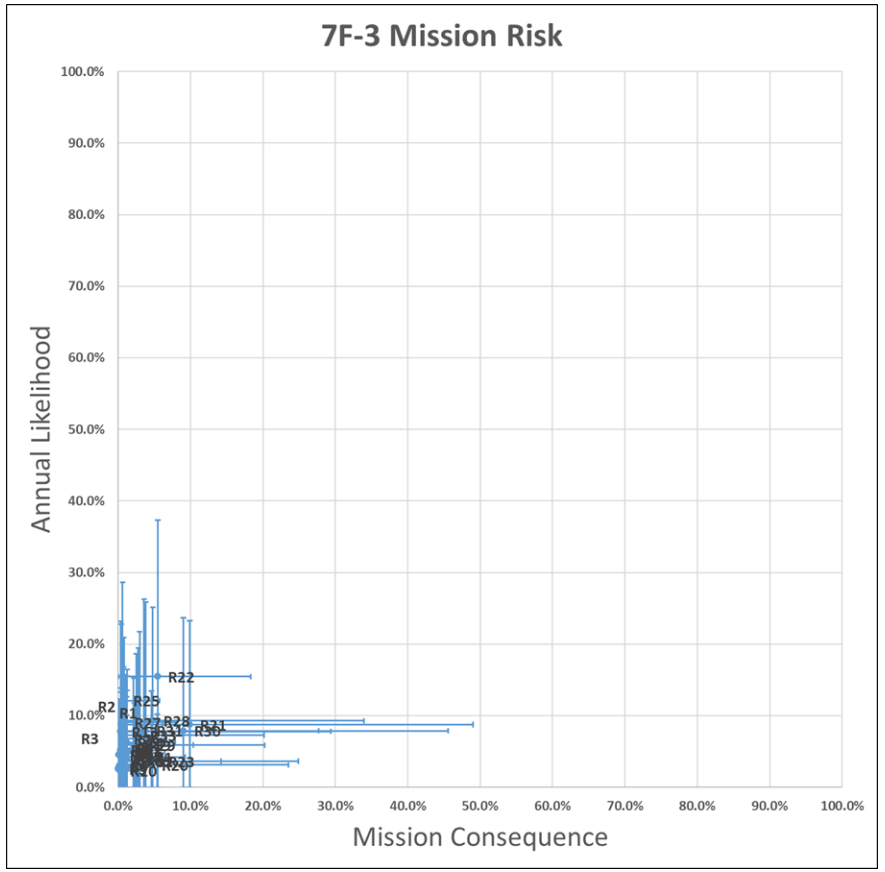
- 33 risk scenarios were scored with results clustering in the lower left
- MQ-99 was probably “overdesigned”




| 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 Example 7F-3

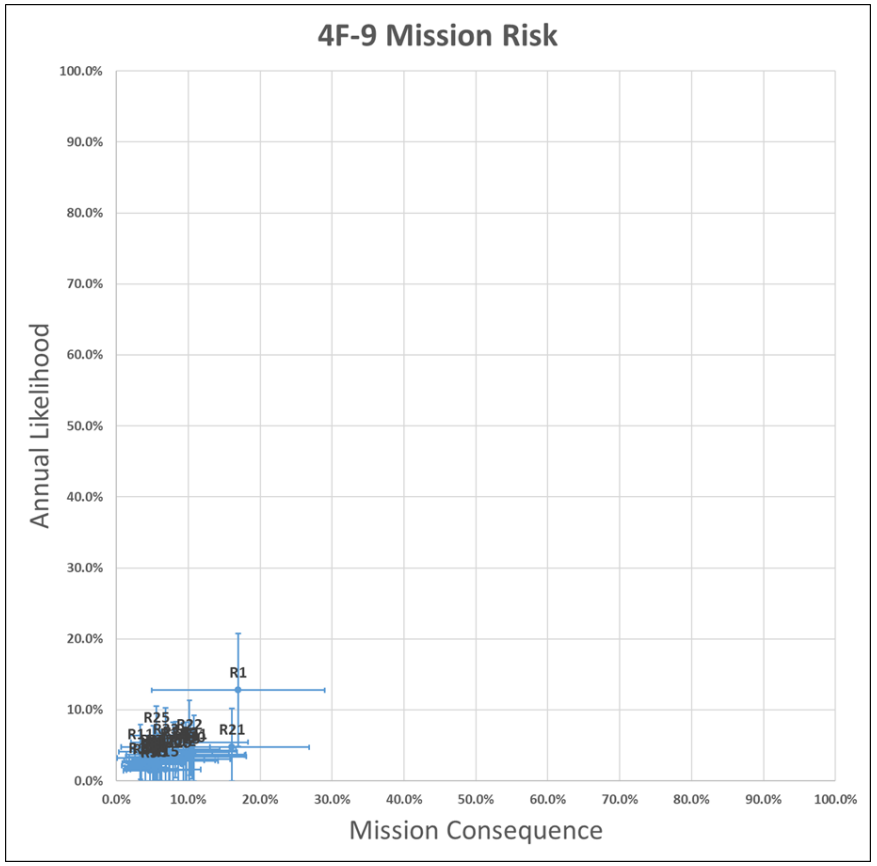
- Results show a significant amount of uncertainty in the assessments of risk




| 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 Example 4F-9

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



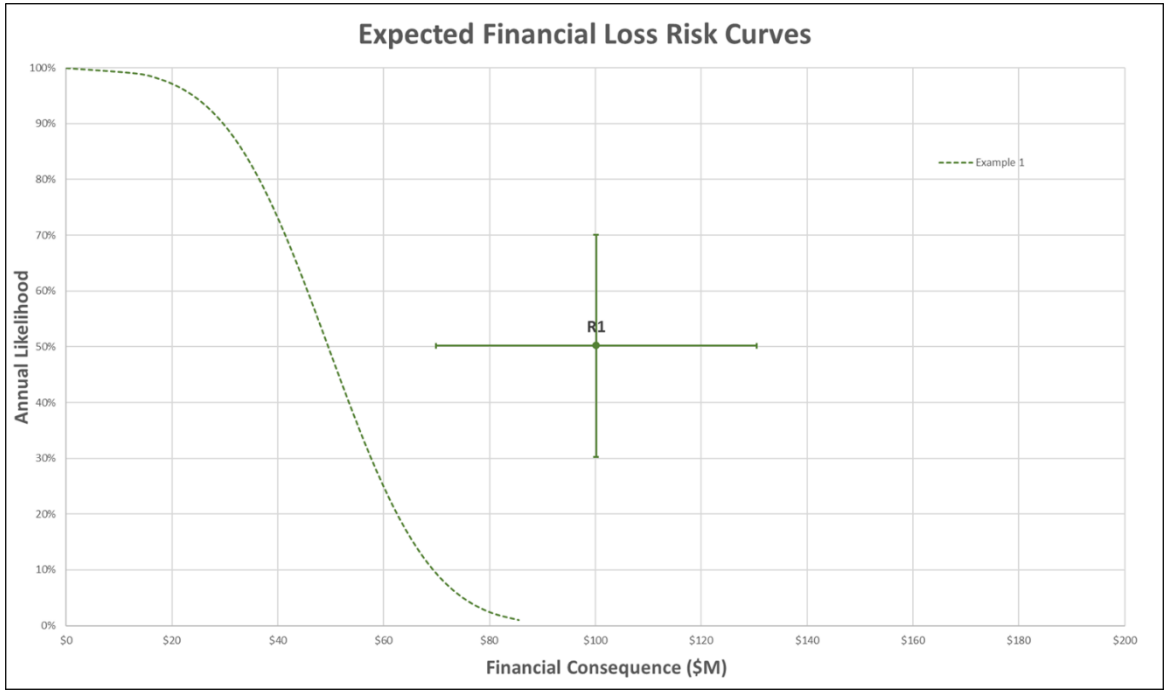

| Risk Scenario | Short Description | EML | Standard Deviation |
|---|---|---|---|
| R1 | GCS supply chain soft production/transmission | 2.140% | 1.273% |
| R21 | Mission computer supply chain OFP adversary control | 0.754% | 0.661% |
| R22 | MX system via Internet tampering load OFPs | 0.561% | 0.476% |
| 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% |

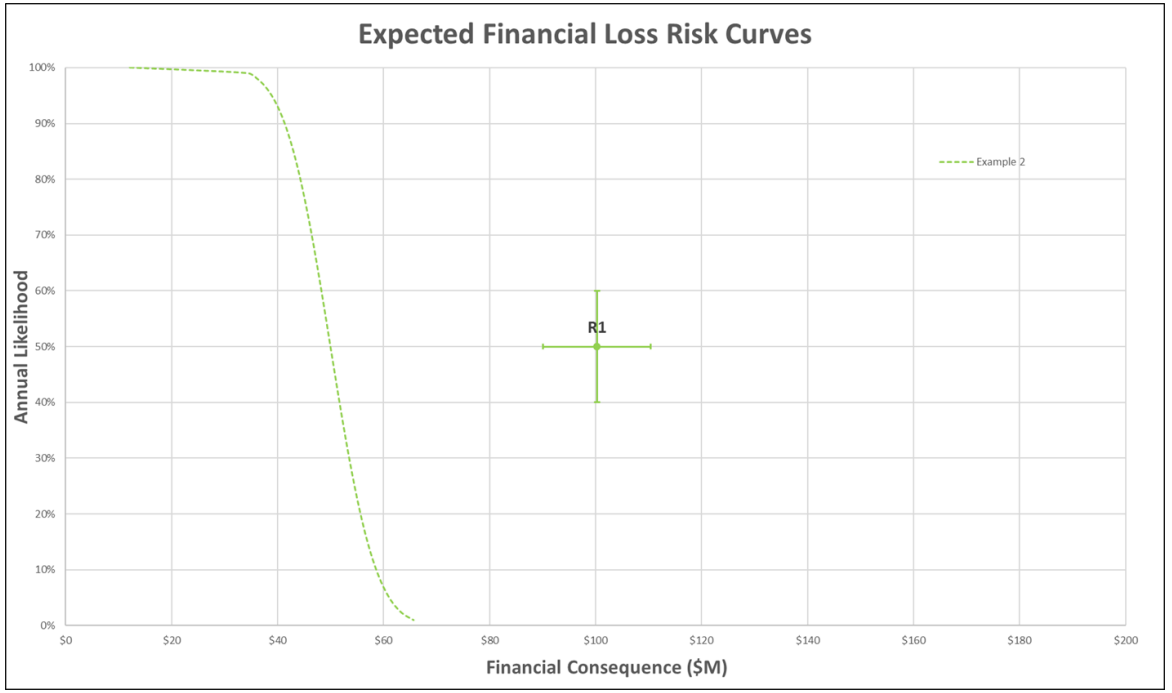
# Combining Risks

- Ordinal risk scoring systems do not have a legitimate way to combine risks to understand overall risk to a system or mission
- With a clear risk model and ratio scoring instead of ordinal (0-1.0) risks can be combined 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 or 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

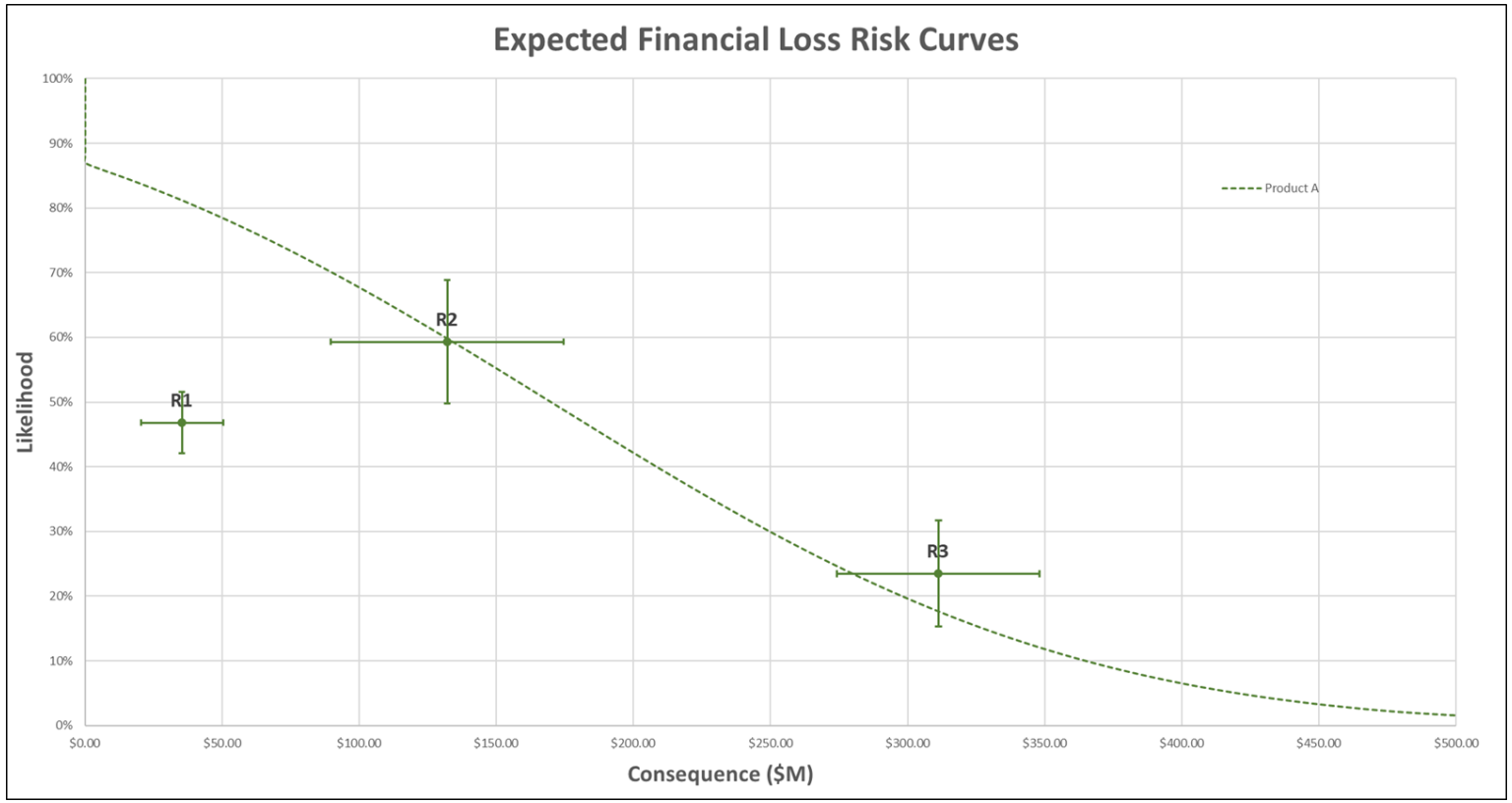



- Total area under the curve equals risk, shallower slope equals more uncertainty

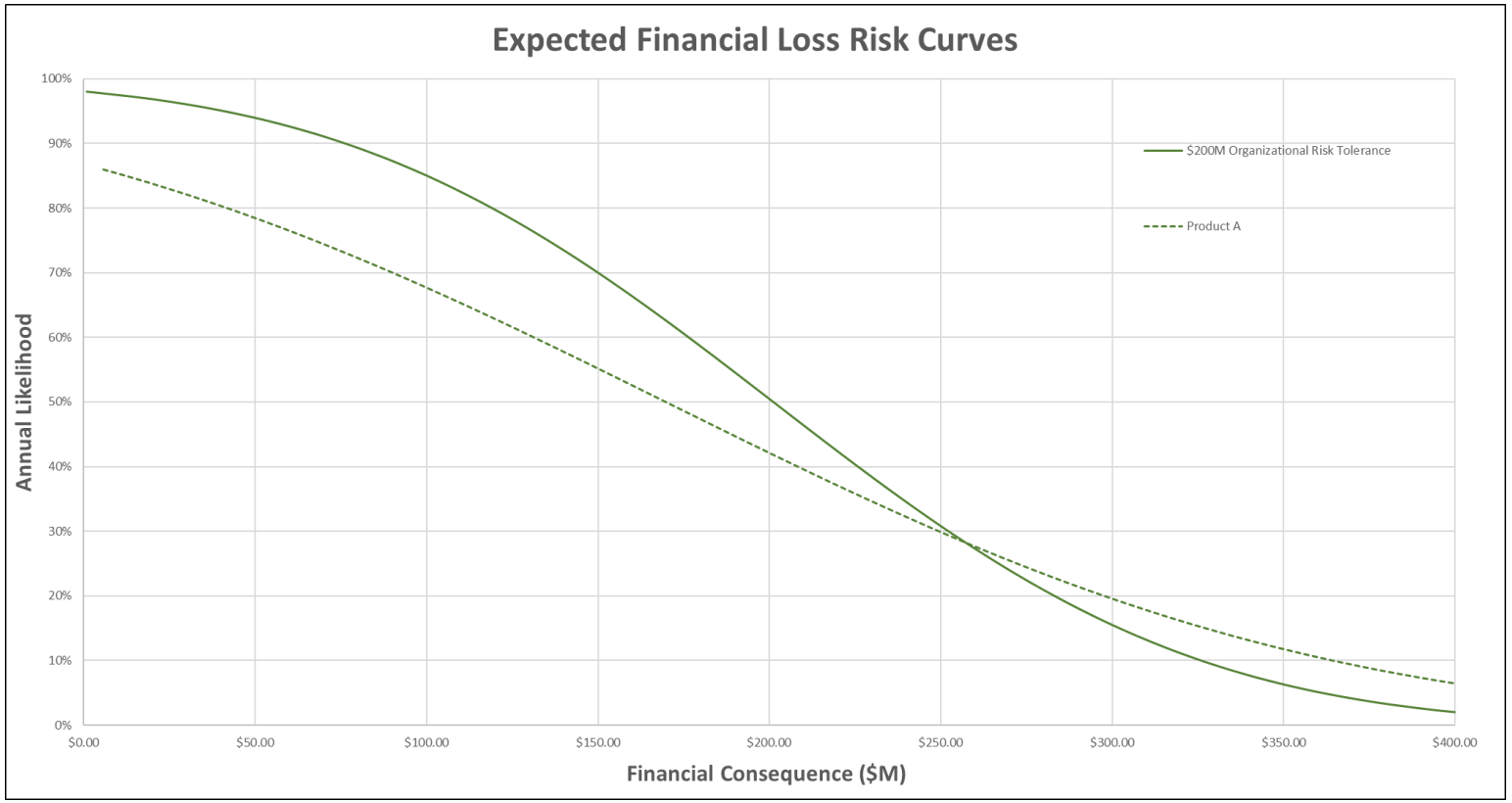
# Simple UAS Example Risk Curve

- 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



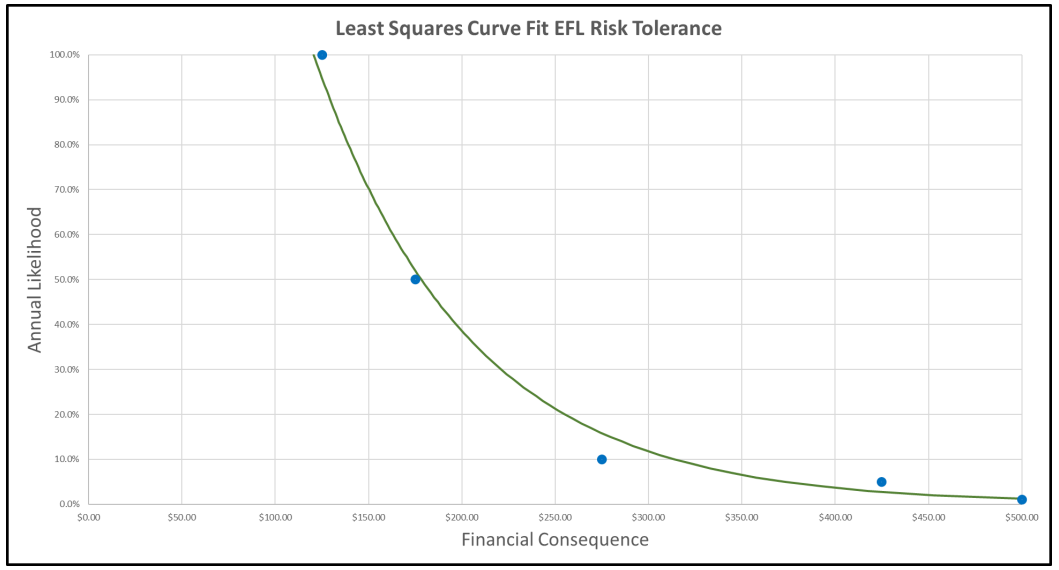
# Risk Tolerance

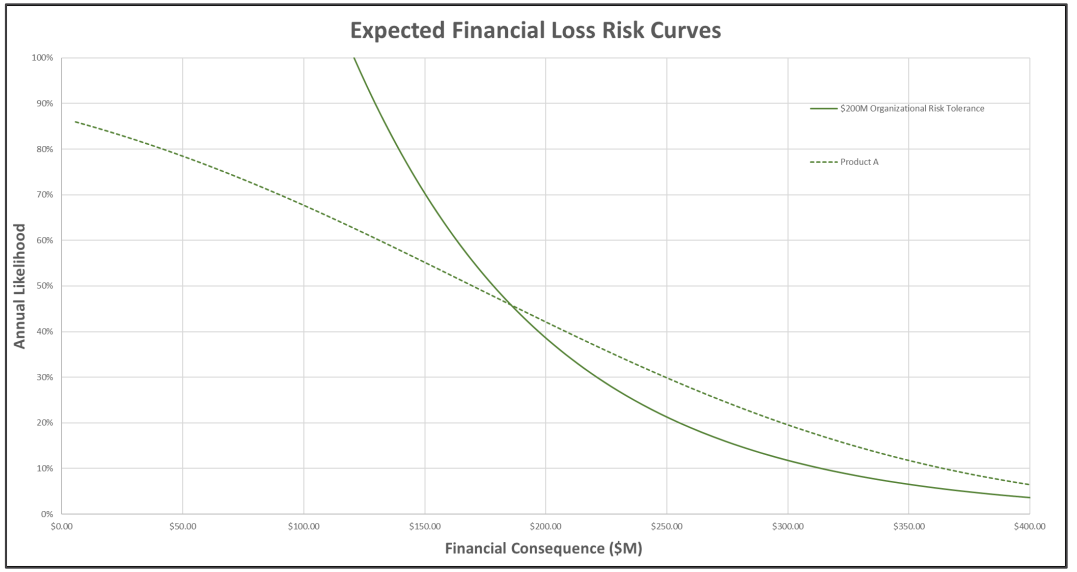
- The amount of risk an organization is willing to take on is its risk tolerance or risk acceptance
- Can be expressed as a point value, a confidence interval, or a risk curve
- A simple “risk neutral” risk tolerance curve can be created by a single 90CI pair of values



# Risk Tolerance 2

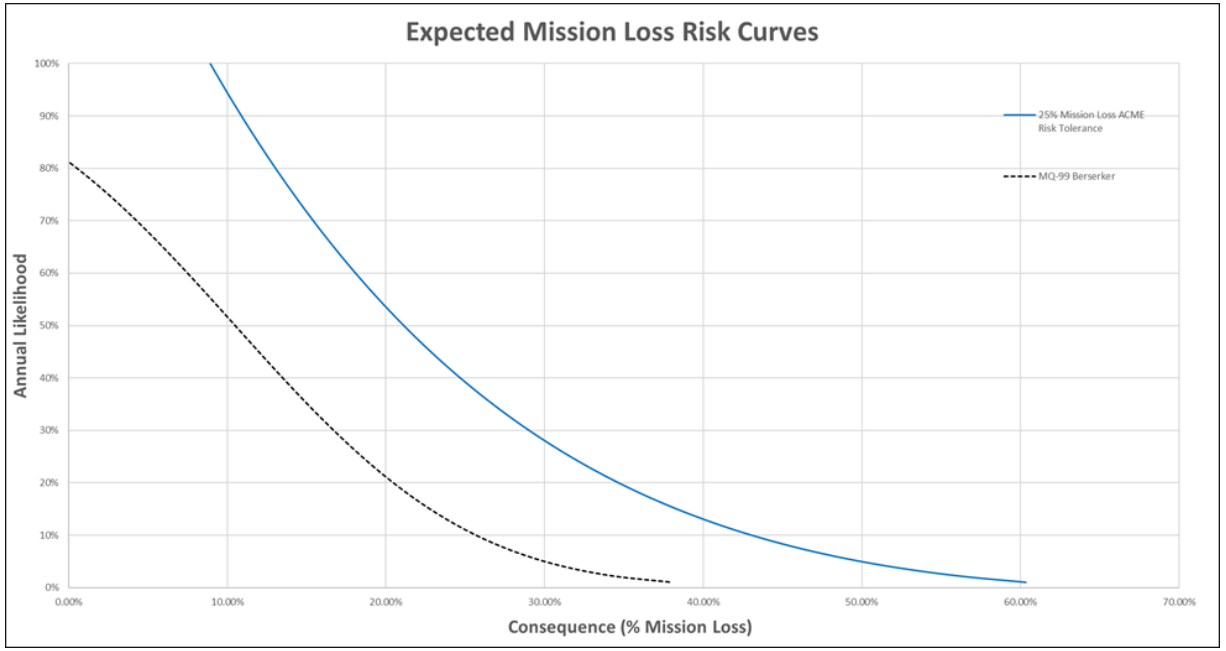
- However, most people are not “risk neutral” and would rather accept a 90% chance of losing $100 than a 0.9% chance of losing $10,000 despite their identical expected loss of $9
- To build a more accurate risk tolerance, determine with senior leaders how much risk they would be willing to accept at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

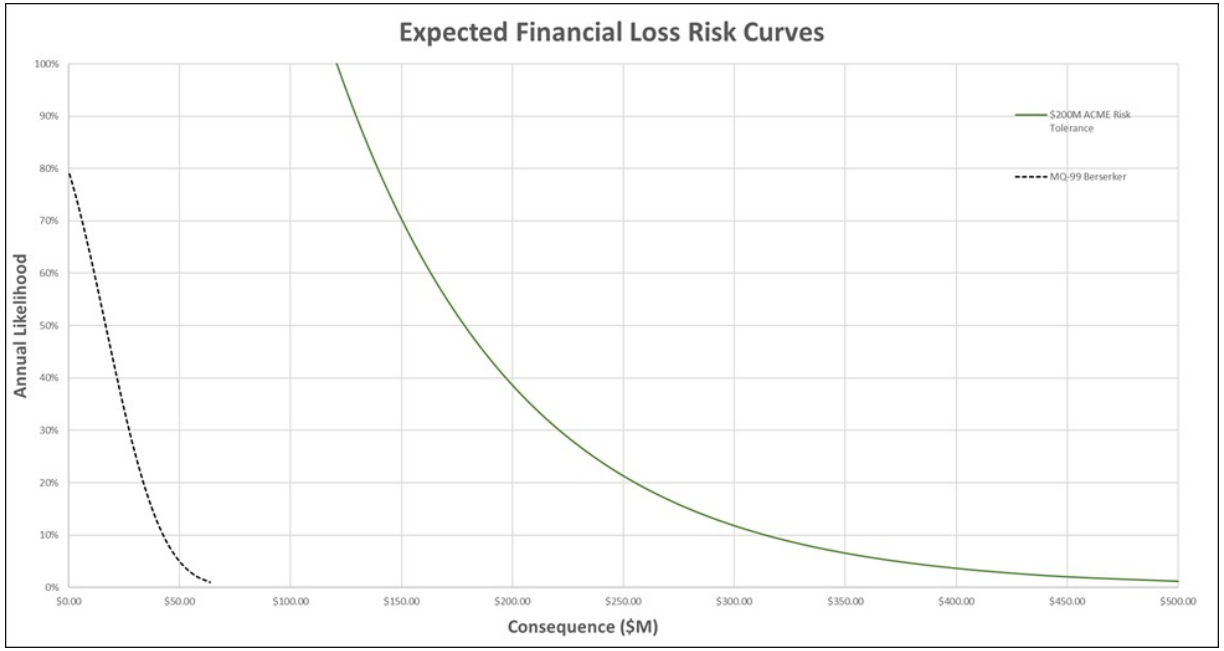


# MQ-99 4F-9 Risk Curves

- 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

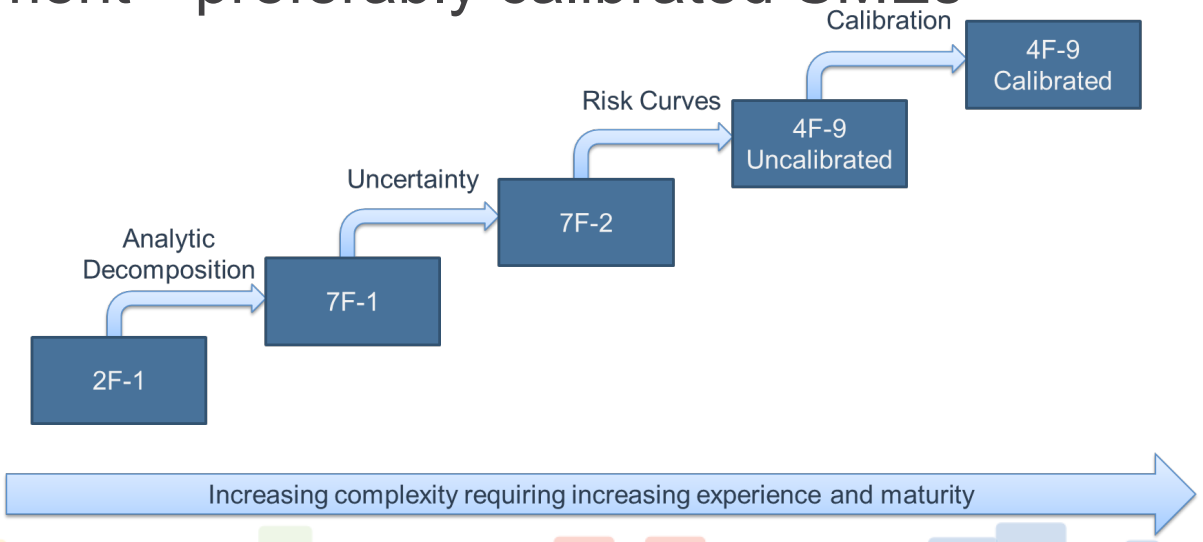



- Security features could be removed to reduce cost, or additional "security margin" could be banked against future adversary capability increases

# Scoring Summary

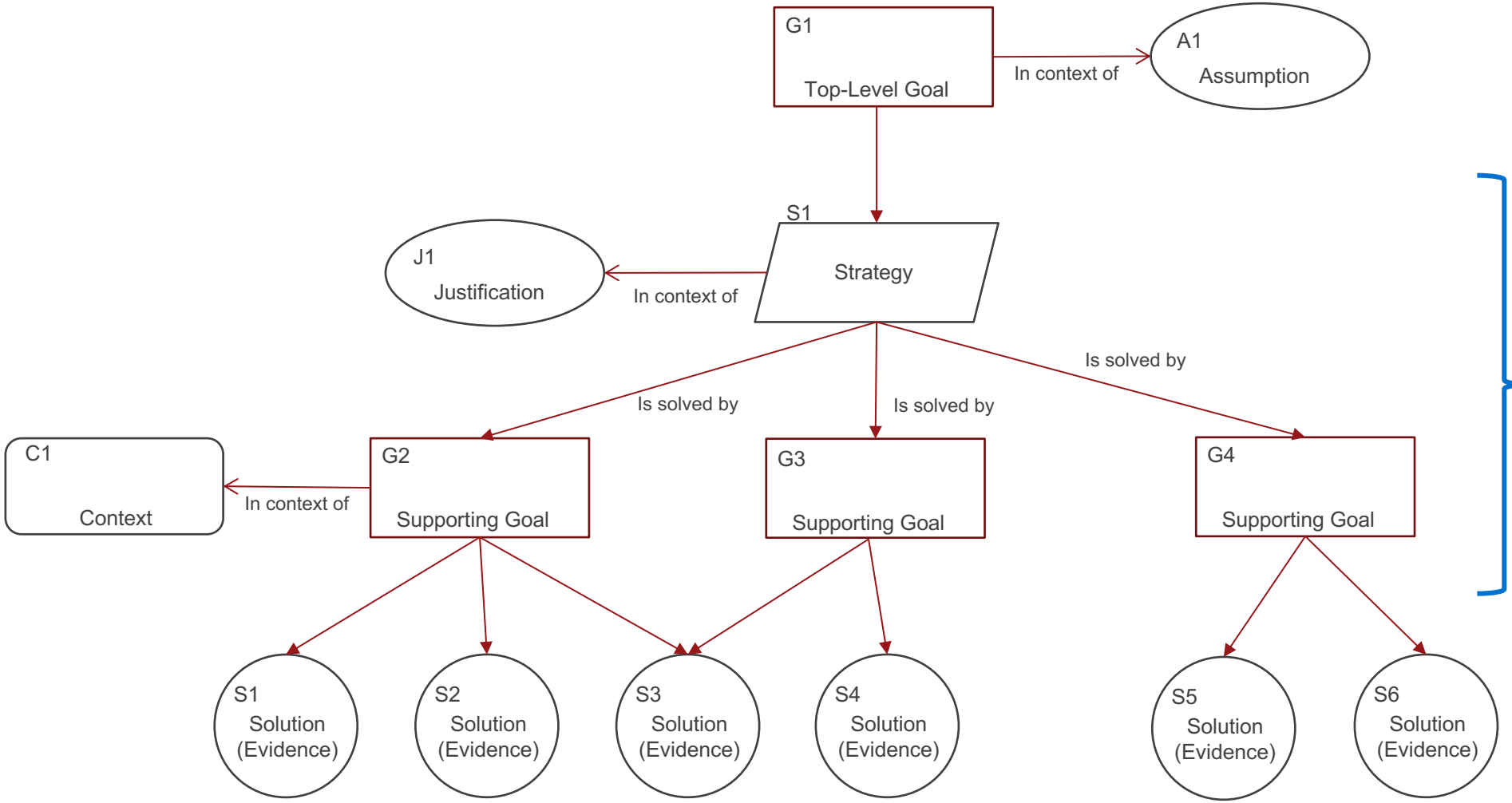
- URAMS can incorporate many different scoring approaches
  - Not all scoring approaches are equal and some have a higher workload
  - Personal preference:
    - 4F as it makes the most sense to me as a probabilistic risk model
    - -2 for a quick high-level assessment
    - -9 for a more rigorous assessment—preferably calibrated SMEs
- Getting away from ordinal (1-5) scoring allows the legitimate calculation of overall risk utilizing expected mission/financial loss



# Decide—Assurance Cases

- An assurance case is a structured argument that demonstrates that a stated claim is or will be satisfied
  - Widely used in the safety world (NASA, Europe, 5-Eyes)
  - Safety has many similarities with security as a property
- Assurance cases are not mathematical proofs and do not provide guarantees; they do provide a structured way of thinking about achievement of an objective
- Assurance cases can help analysts determine the extent to which all relevant concerns have been addressed
  - Can help engineers to deliver adequately secure systems
- Assurance cases can identify areas that provide significant opportunities to improve overall security

# Assurance Case Goal Structuring Notation (GSN)




**Mission Goal**

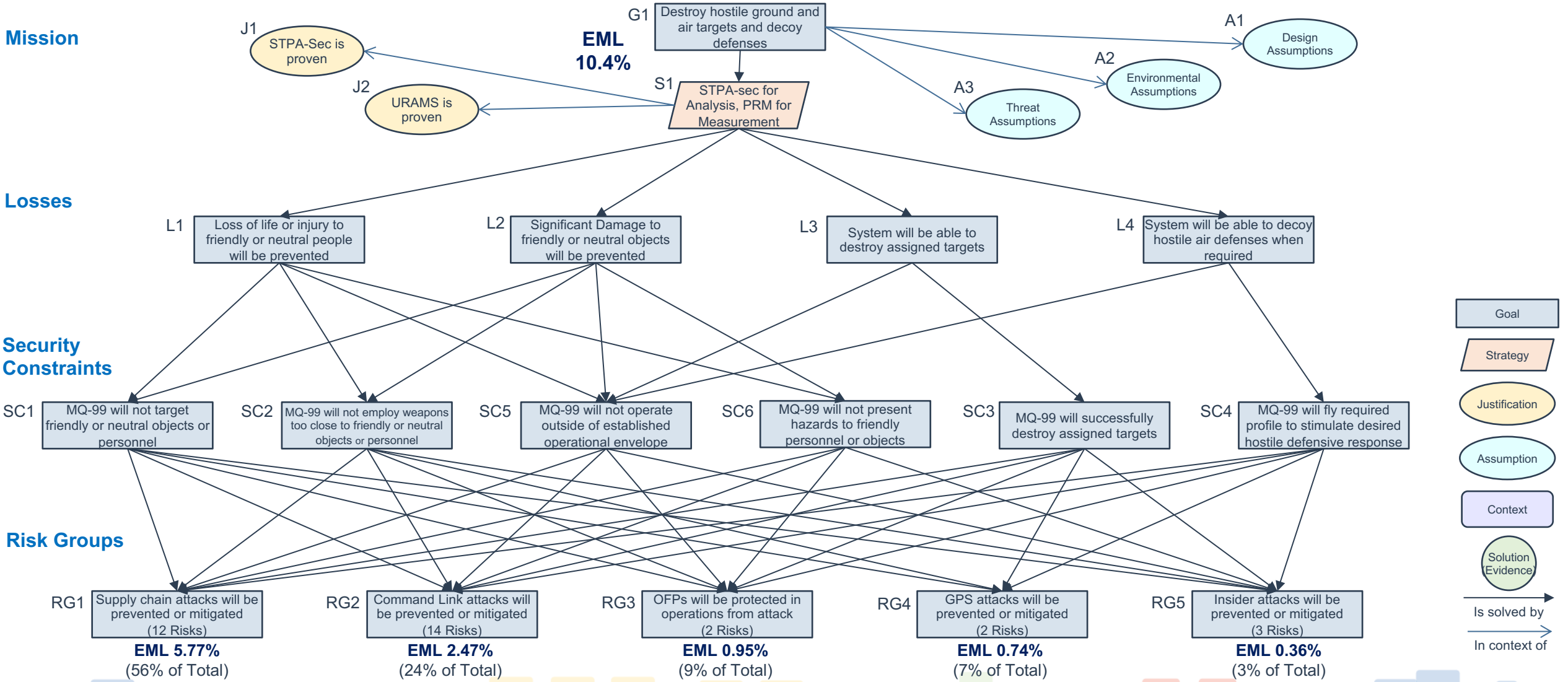
**Mission Structure**

**Evidence**

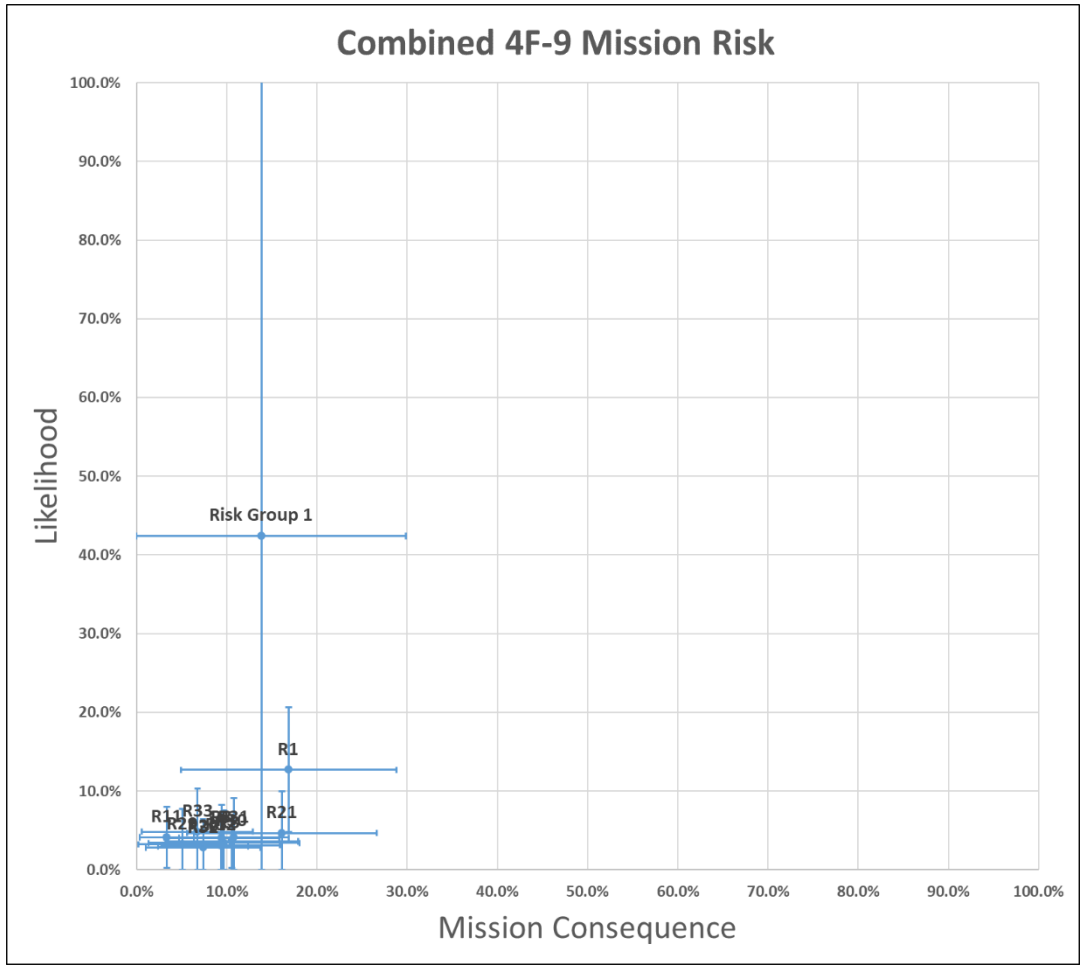
# Assurance Case Strengths

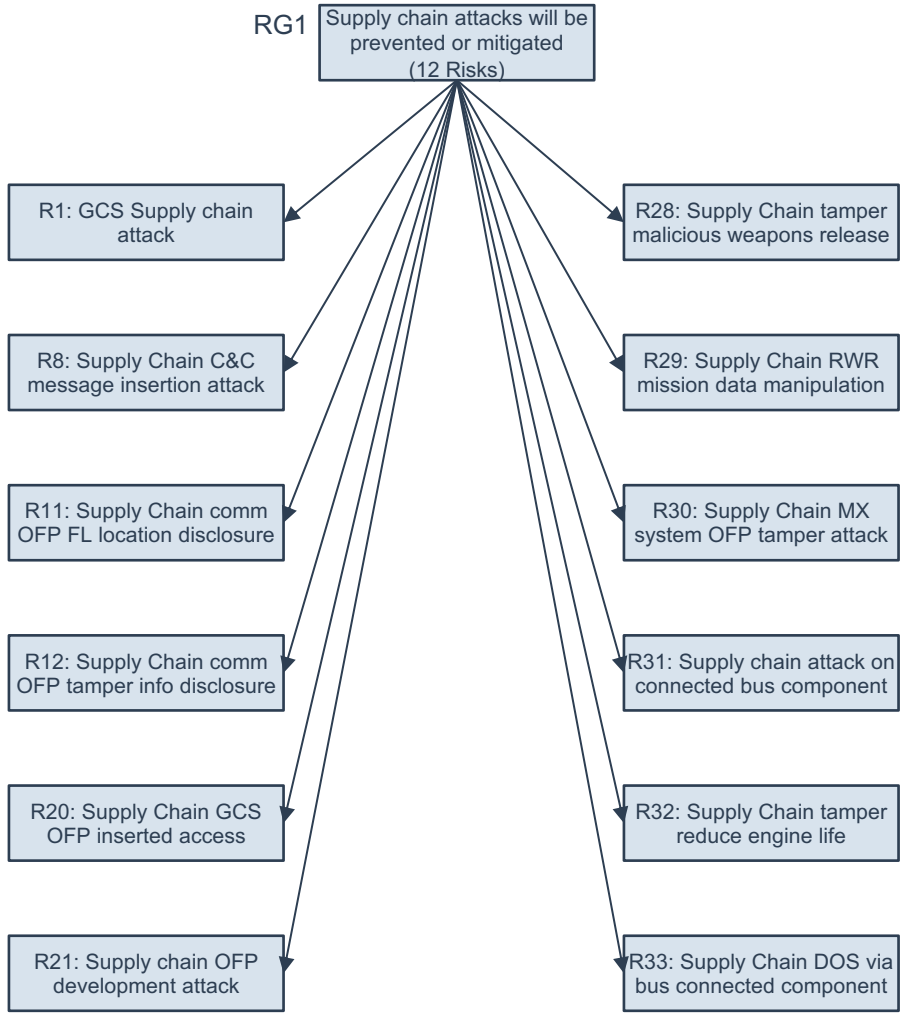
- Tool agnostic
  - Different tools can be used to create the mission structure as well as score risks
- All evidence can be collected in a single structure from different communities
- Traceability throughout
  - If scoring in a particular area feels “off” an assessor can easily trace back to the evidence that supports that scoring
- Enables clear communication of risk in an established standard format

# MQ-99 Overall Assurance Case



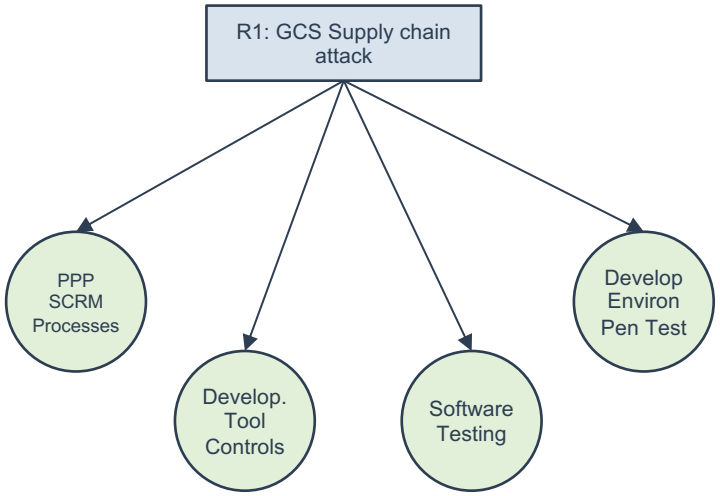
# RG1: Supply Chain Attacks



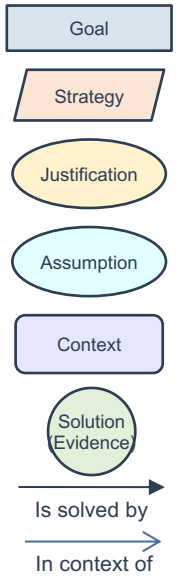
# R1: GCS Supply Chain Attack

- 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]




| Factor | Score |
|---|---|
| EML | 2.1% |
| Likelihood | 12.7% |
| Mission Consequence | 17.0% |

Link to Calculation Spreadsheet

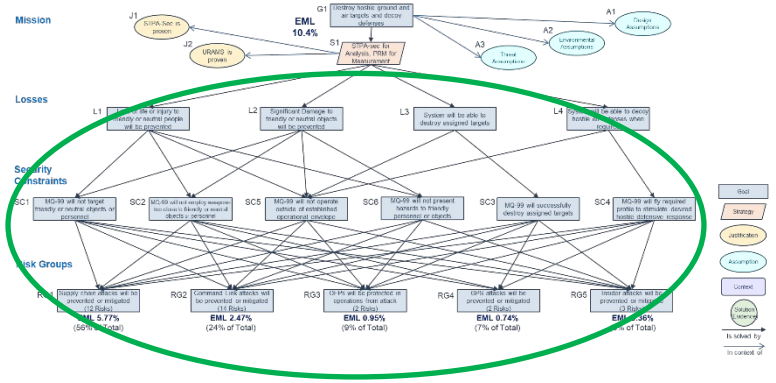


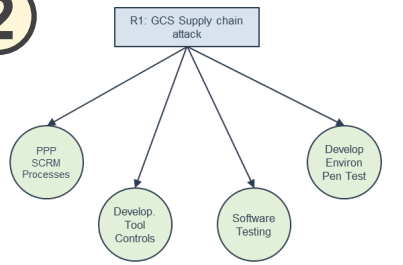
# Using an Assurance Case to Assess Risk

- An assurance case for a complex system may at first seem overwhelming to analyze in depth, but it can easily be broken down into logical steps

**1. Validate mission structure**
**2. Verify individual risk scenario scores by examining evidence**
**3. Flow risk up and compare to risk tolerance**

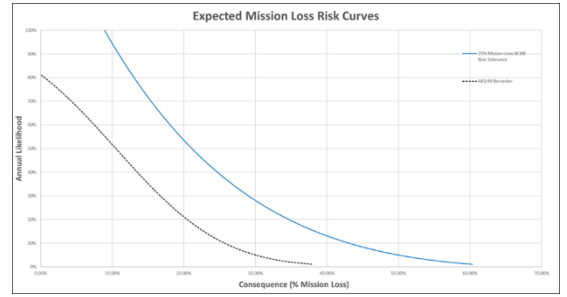
① ② ③




| Factor | Score |
|---|---|
| EML | 2.1% |
| Likelihood | 12.7% |
| Mission Consequence | 17.0% |

Risk Tolerance > Risk?

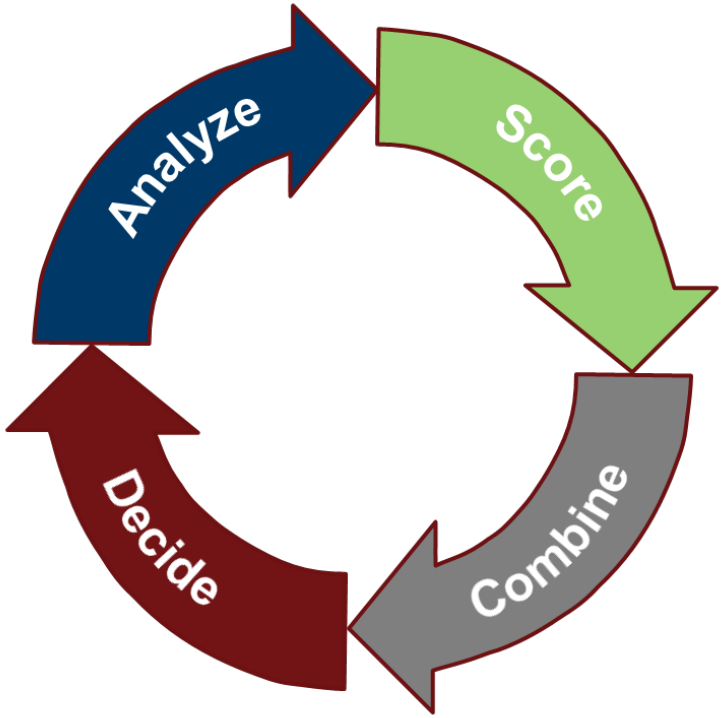


# Decide—Return on Investment (ROI)

- If risk > risk tolerance, then URAMS provides an excellent way to understand ROI on different potential mitigations
  1. Calculate total risk without the mitigation
  2. Re-calculate risk with the mitigation in place
- If scoring financial risk, then the comparison is direct $→$, on the mission side it becomes mission gain/$
- Can also be used to determine what combination of mitigations yields the greatest benefit within a fixed budget
- Rescoring for an already created model tends to be much easier

# Conclusions

- The lack of a widely accepted way of assessing and measuring risk hampers creating secure and resilient systems
- URAMS provides an overall framework that includes multiple tools manage cybersecurity risk to cyber-physical systems
  - Mission focused
  - As quantitative as possible
  - Clear picture of the risk and links to supporting evidence through the use of structured assurance cases



32nd Annual INCOSE international symposium

hybrid event

Detroit, MI, USA

June 25 - 30, 2022

www.incose.org/symp2022