Mission Based Risk Assessment (MBRA)

Ryan Brunton
Randy Saunders

Purpose and Desired Outcomes

What is the Purpose of this Discussion?

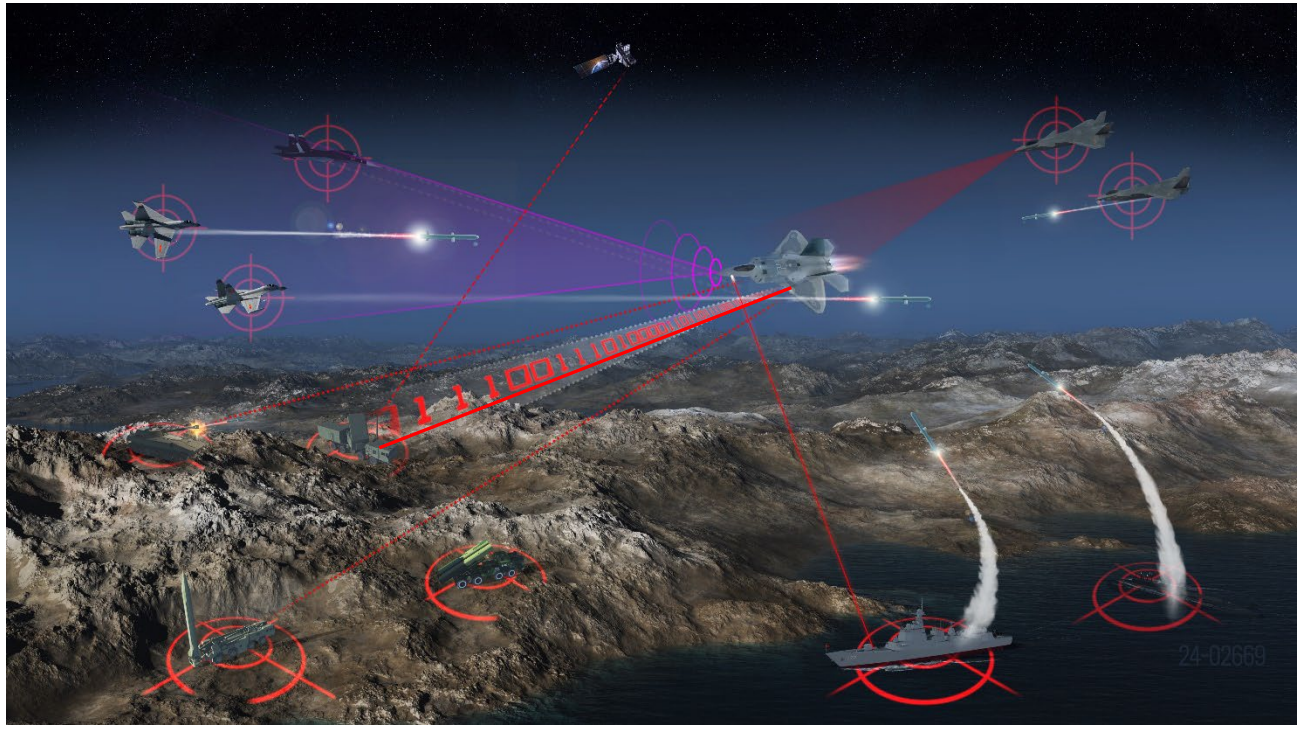
1. Describe MBRA's role: what it is and gaps it fills

What are the Desired Outcomes of this Discussion?

1. Align on the intent and the approach of the Mission Based Risk Assessment.
2. Discuss a specific baseline MBRA implementation: Full-Spectrum Risk Analysis for Mission-based Evaluation of Resiliency and Survivability (FRAMERS)

What Motivates the Need for Mission-Based Risk Assessments?

Complex systems and missions + full spectrum operating environments require: Structured, top down approach to identify **mission critical functions** that are vulnerable to operationally relevant threats. Traditional, bottom up, approach is not scalable to address full spectrum questions.

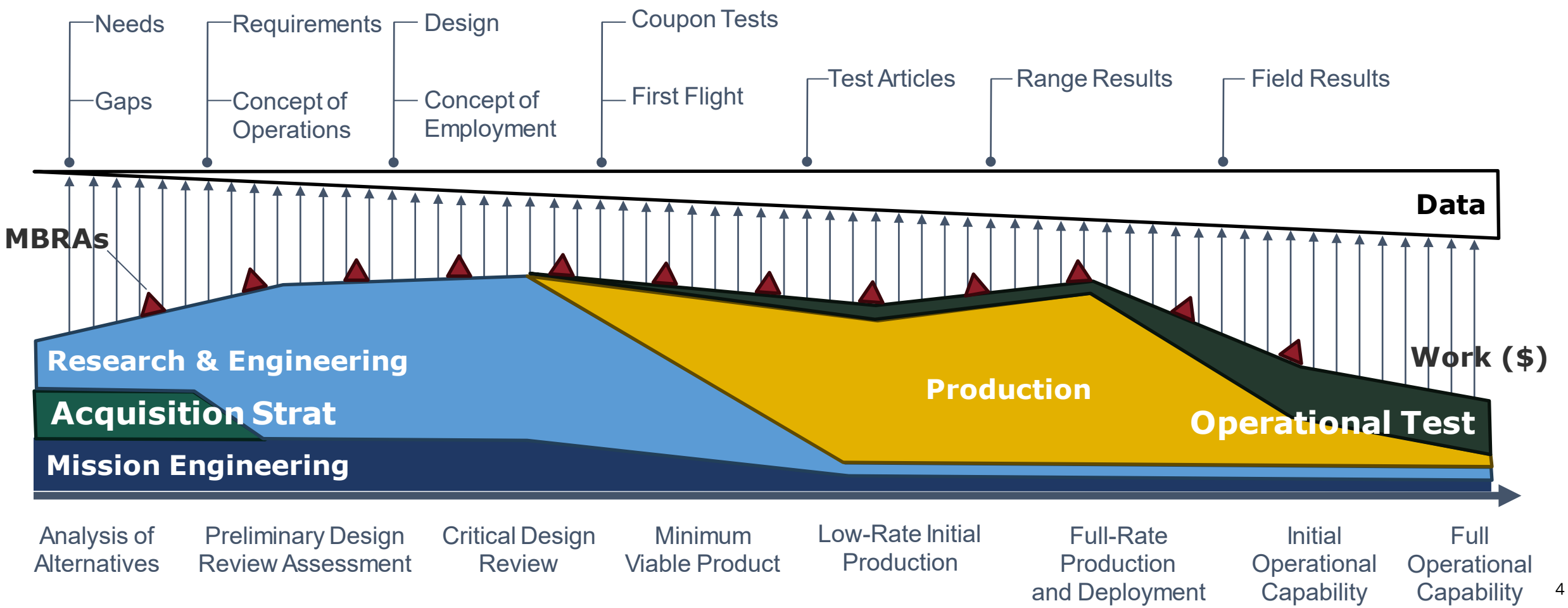


1. How might full spectrum conditions an affect system operation?
2. What are the potential mission critical functions and how could they be exploited by adversaries?
3. How do these factors impact the system's ability to complete its mission?
4. What scope of Operational Test will be required to verify survivability, suitability, and effectiveness?

Ensures systems are not only technically capable but survivable and adaptable in the face of diverse and evolving threats

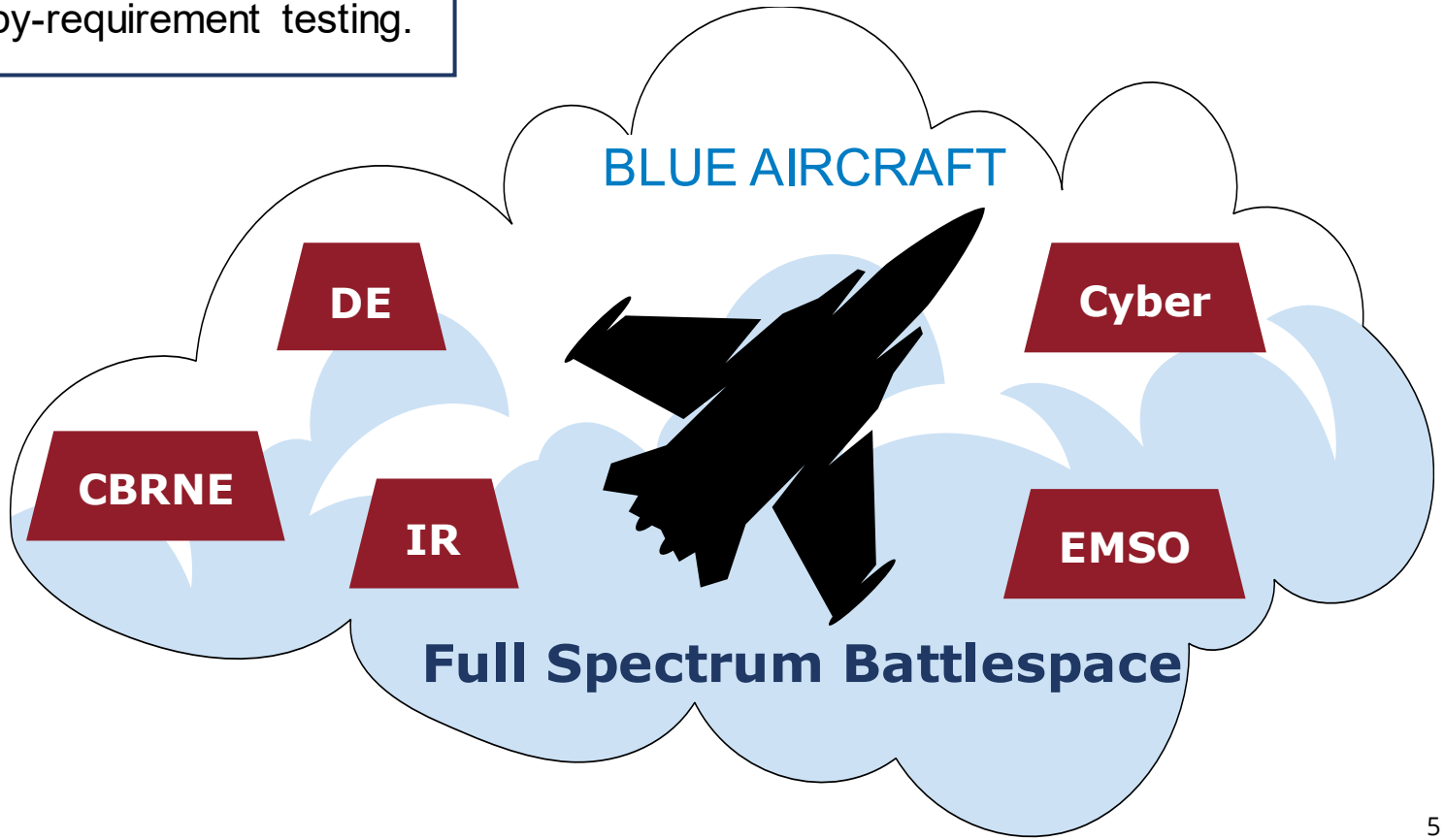
Project Life-Cycle

MBRAs enhance program data gathered by identifying risks to mission and results that reduce risk.



MBRA – Full Spectrum Assessment

- Just as we plan full spectrum attacks, we need to assess systems against full spectrum attacks.
- Critical area for Operational Test because it depends on the whole operational environment interacting with the system under test, and can't be easily aggregated from requirement-by-requirement testing.

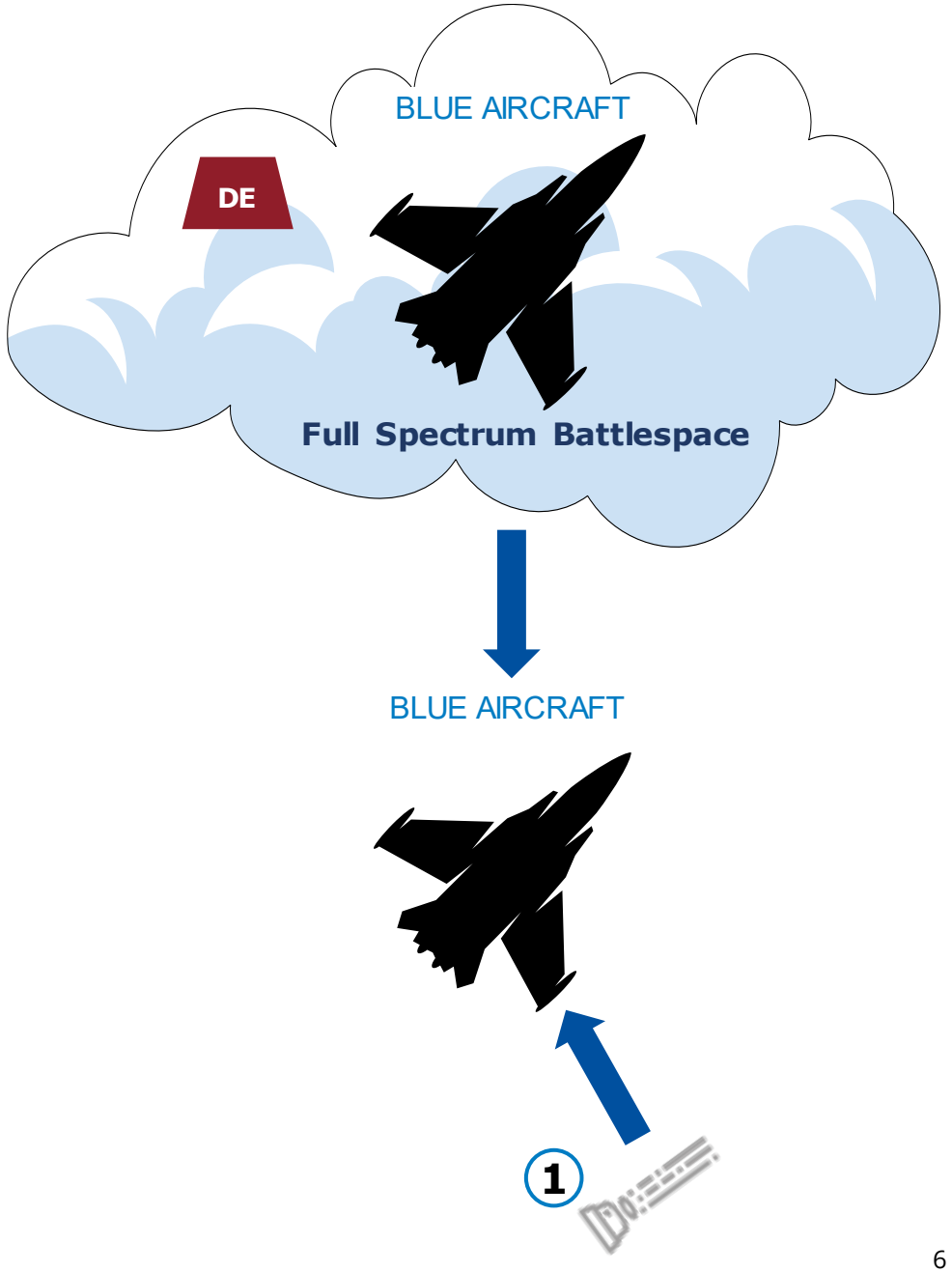


MBRA – Full Spectrum Assessment

- Just as we plan full spectrum attacks, we need to assess systems against full spectrum attacks.
- Critical area for Operational Test because it depends on the whole operational environment interacting with the system under test, and can't be easily aggregated from requirement-by-requirement testing.
  - For example:

1 A directed energy weapon might not harm the vehicle, but it might make the skin hotter than normal.

Risk = Low

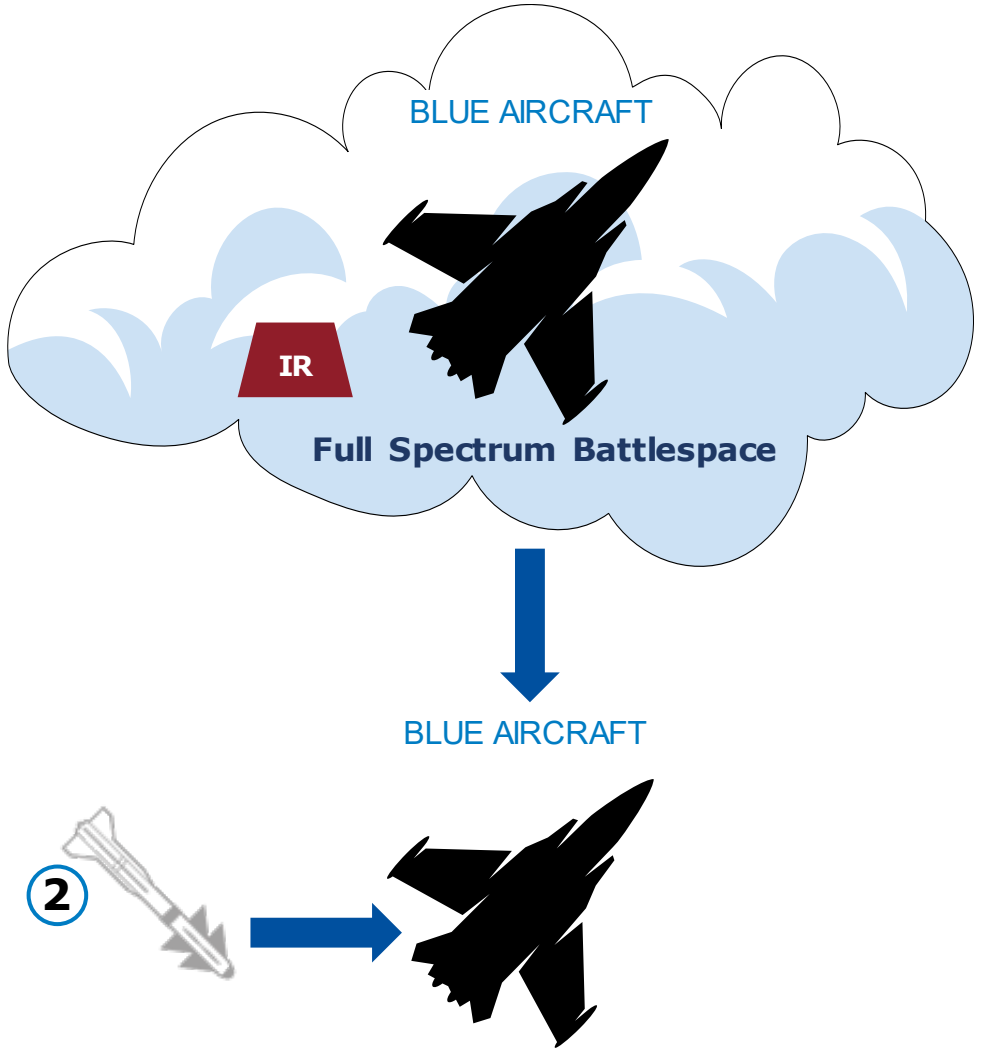


MBRA – Full Spectrum Assessment

- Just as we plan full spectrum attacks, we need to assess systems against full spectrum attacks.
- Critical area for Operational Test because it depends on the whole operational environment interacting with the system under test, and can't be easily aggregated from requirement-by-requirement testing.
  - For example:

2 An IR seeking missile might be unlikely to lock onto the vehicle, unless there was an unusually hot spot.

Risk = Low

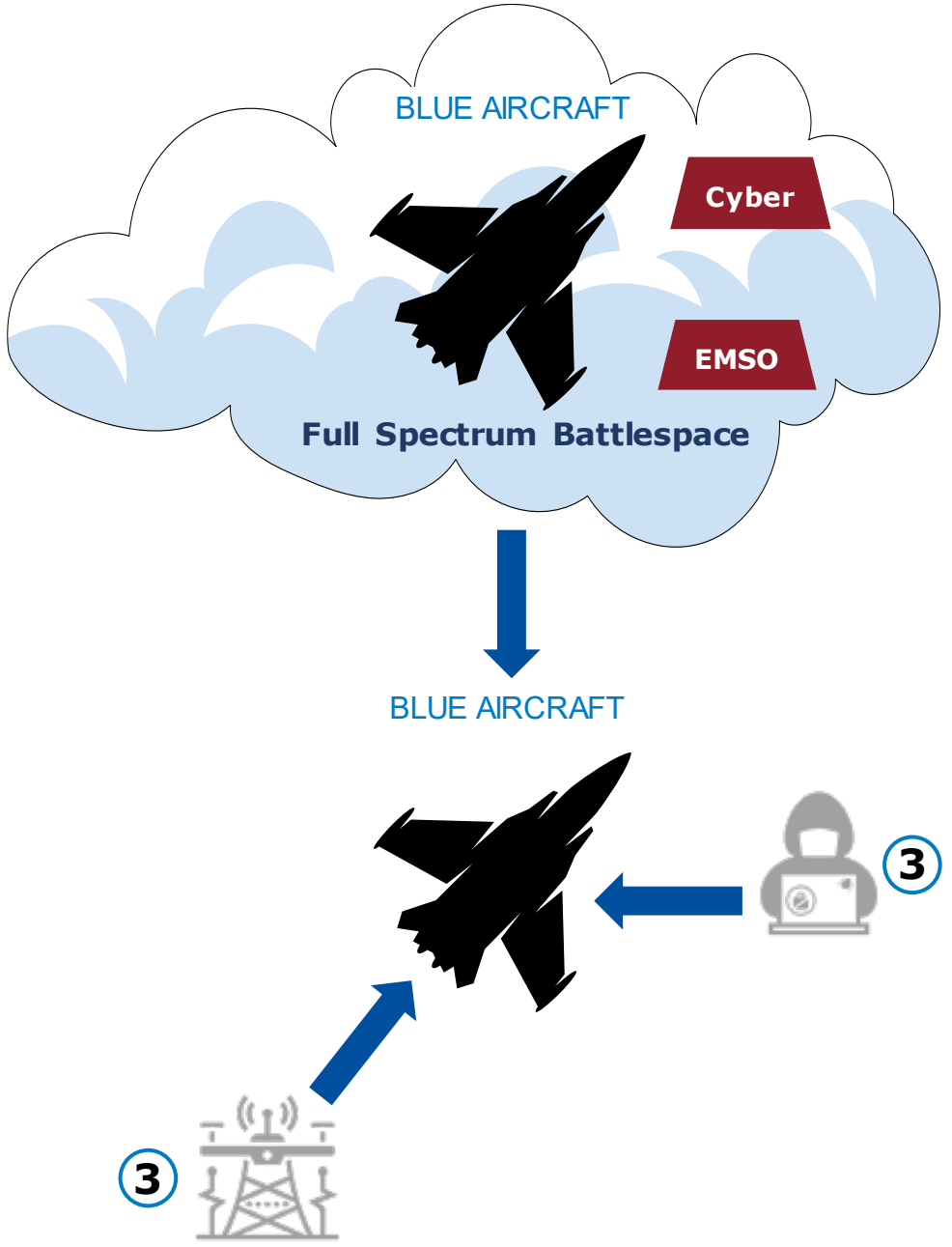


MBRA – Full Spectrum Assessment

- Just as we plan full spectrum attacks, we need to assess systems against full spectrum attacks.
- Critical area for Operational Test because it depends on the whole operational environment interacting with the system under test, and can't be easily aggregated from requirement-by-requirement testing.
  - For example:

3 A cyber/EW flood attack might be unlikely to disrupt communication within the vehicle for more than a second.

Risk = Low

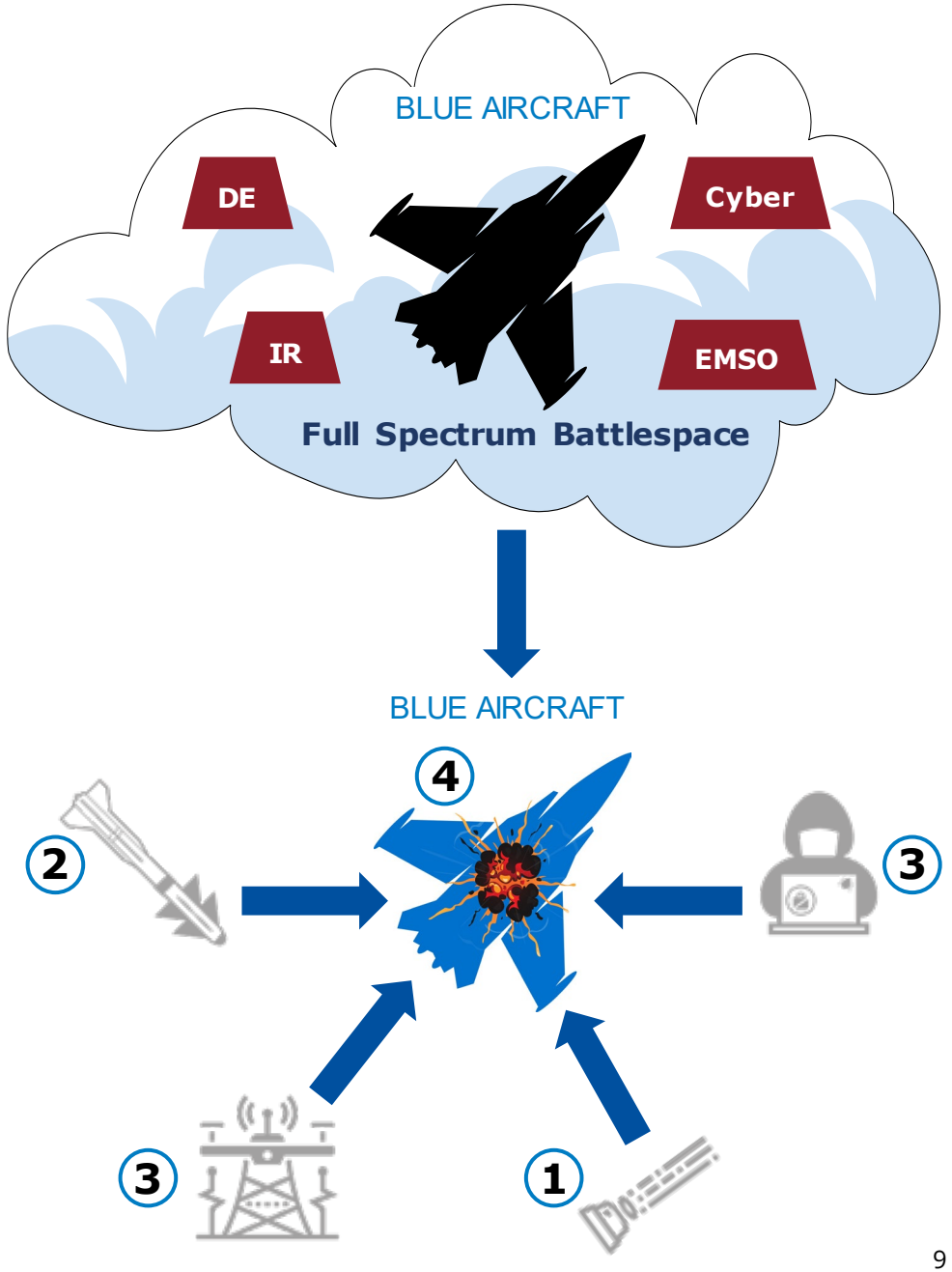


MBRA – Full Spectrum Assessment

- Just as we plan full spectrum attacks, we need to assess systems against full spectrum attacks.
- Critical area for Operational Test because it depends on the whole operational environment interacting with the system under test, and can't be easily aggregated from requirement-by-requirement testing.
  - For example:

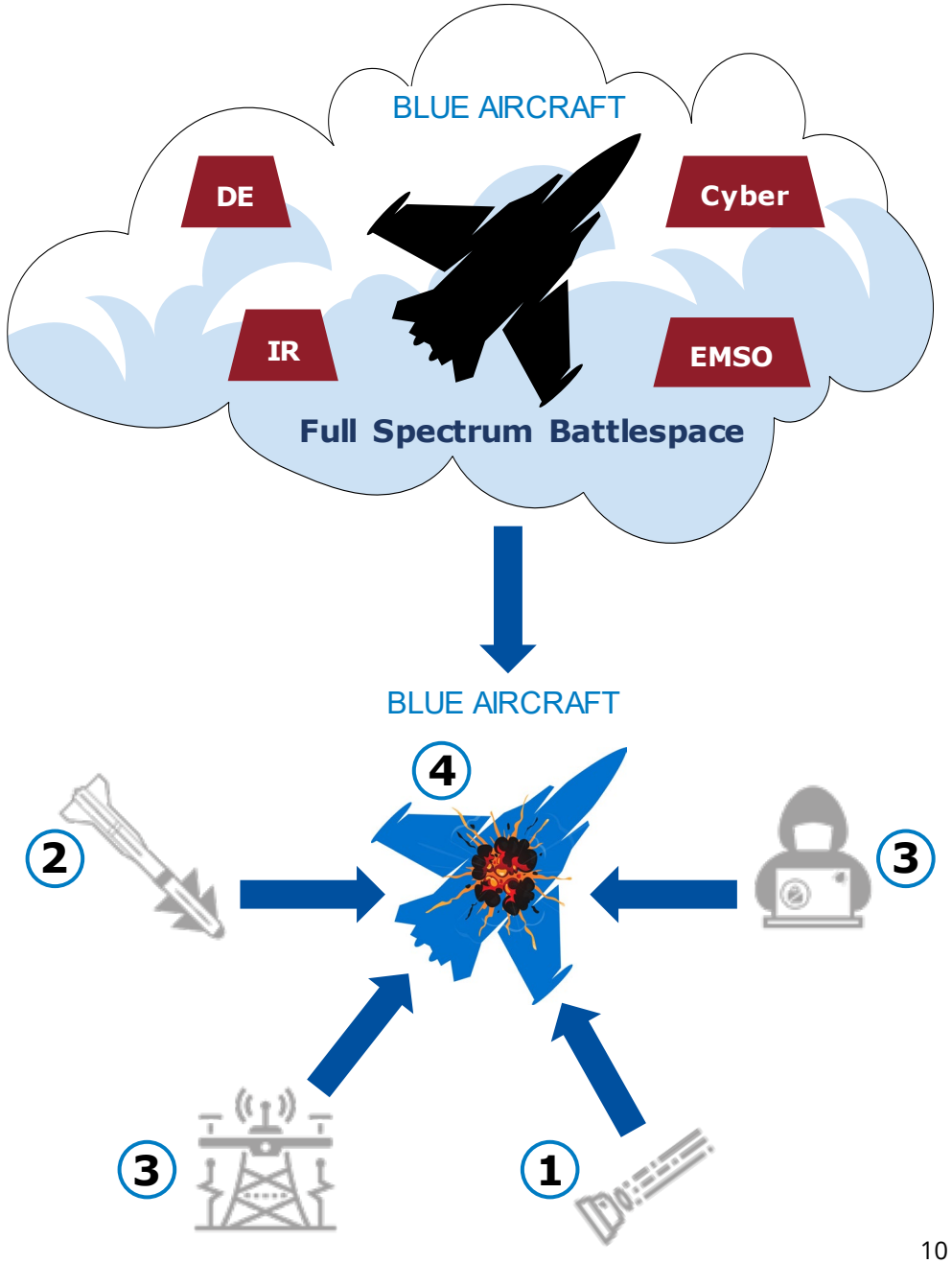
1. A directed energy weapon might not harm the vehicle, but it might make the skin hotter than normal. Risk = Low
2. An IR seeking missile might be unlikely to lock onto the vehicle, unless there was an unusually hot spot. Risk = Low
3. A cyber/EW flood attack might be unlikely to disrupt communication within the vehicle for more than a second. Risk = Low
4. But if that 1s delay causes the missile to get 1s closer to the vehicle than normal and that hot spot allows the missile to track better than expected it might cause a vehicle to be destroyed when independent assessments suggest it would not.

Risk = High

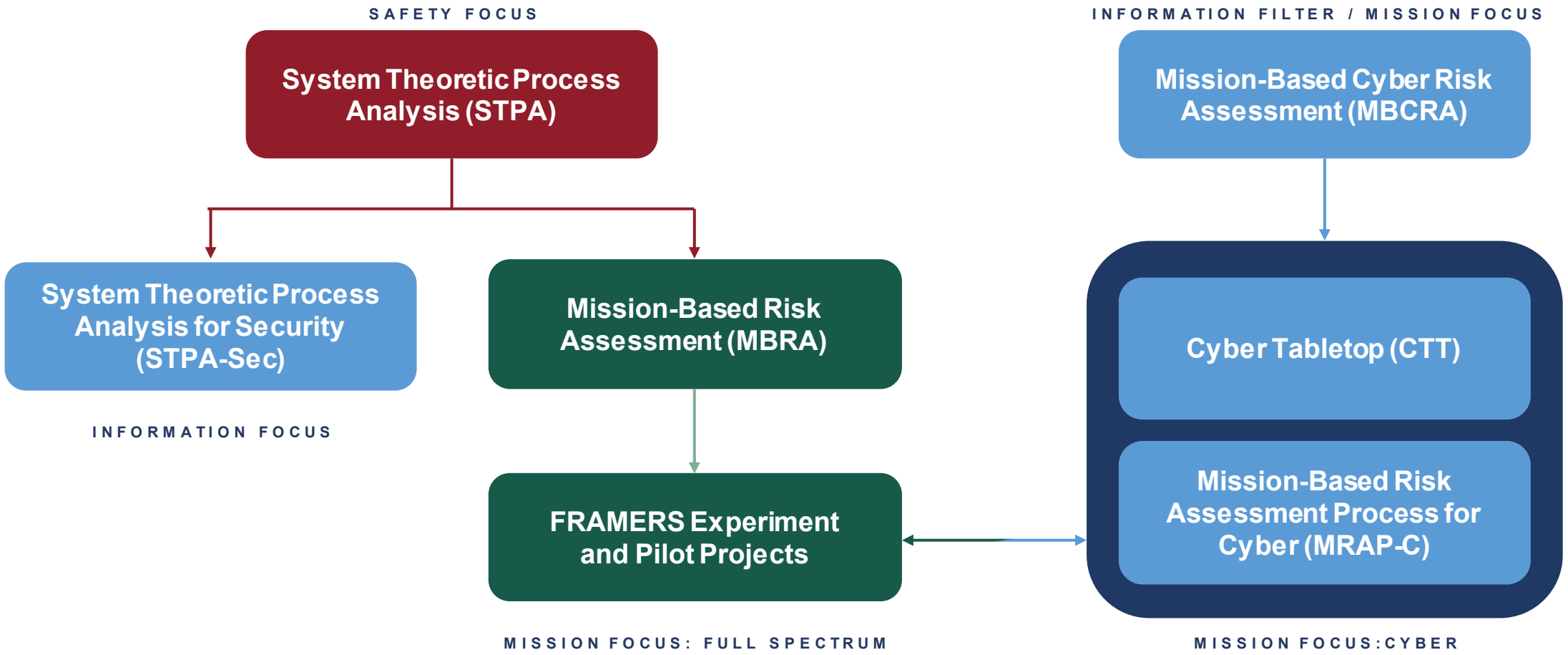


MBRA – Full Spectrum Assessment

- Just as we plan full spectrum attacks, we need to assess systems against full spectrum attacks.
- Critical area for Operational Test because it depends on the whole operational environment interacting with the system under test and can't be easily aggregated from requirement-by-requirement testing.
  - For example:
    1. A directed energy weapon might not harm the vehicle, but it might make the skin hotter than normal.
    2. An IR seeking missile might be unlikely to lock onto the vehicle, unless there was an unusually hot spot.
    3. A cyber/EW flood attack might be unlikely to disrupt communication within the vehicle for more than a second.
    4. But if that 1s delay causes the missile to get 1s closer to the vehicle than normal and that hot spot allows the missile to track better than expected it might cause a vehicle to be destroyed when independent assessments suggest it would not.
  - The absence of intelligence showing an adversary has planned this attack does not negate the risk.
    - Likelihood in the risk calculation becomes a Bayesian analysis of the of the individual component threats existing on a contested battlefield



Full-Spectrum Risk Analysis for Mission-based Evaluation of Resiliency and Survivability (FRAMERS)



FRAMERS is derived from STPA with a Mission Focus

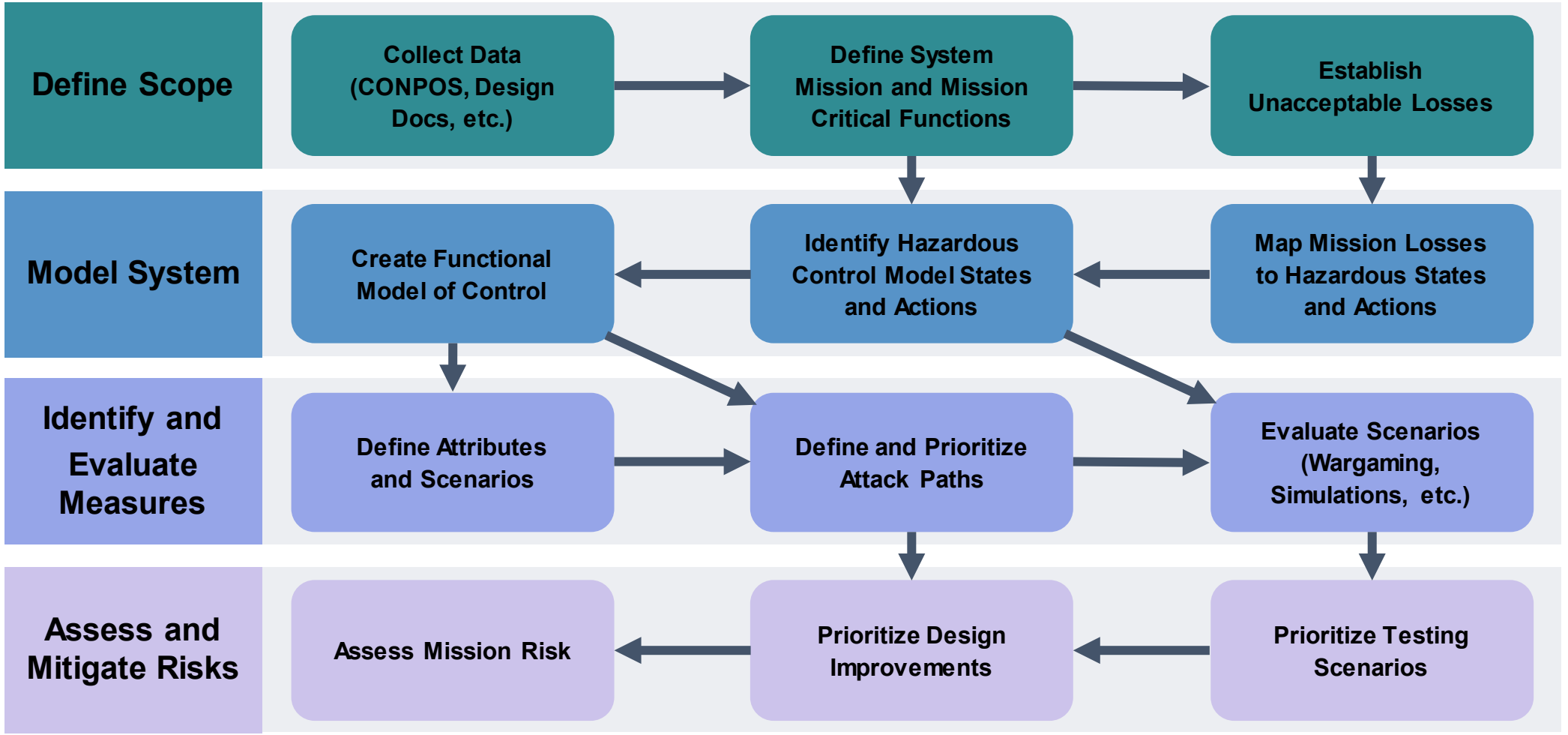
The FRAMERS Process

Proactive and based on systems theory – where every system has causal boundaries, is influenced by its context, defined by its structure, function and role, and expressed through its relations with other systems.

Define Scope	Collect Data (CONPOS, Design Docs, etc.)	Define System Mission and Mission Critical Functions	Establish Unacceptable Losses
Model System	Create Functional Model of Control	Identify Hazardous Control Model States and Actions	Map Mission Losses to Hazardous States and Actions
Identify and Evaluate Measures	Define Attributes and Scenarios	Define and Prioritize Attack Paths	Evaluate Scenarios (Wargaming, Simulations, etc.)
Assess and Mitigate Risks	Assess Mission Risk	Prioritize Design Improvements	Prioritize Testing Scenarios

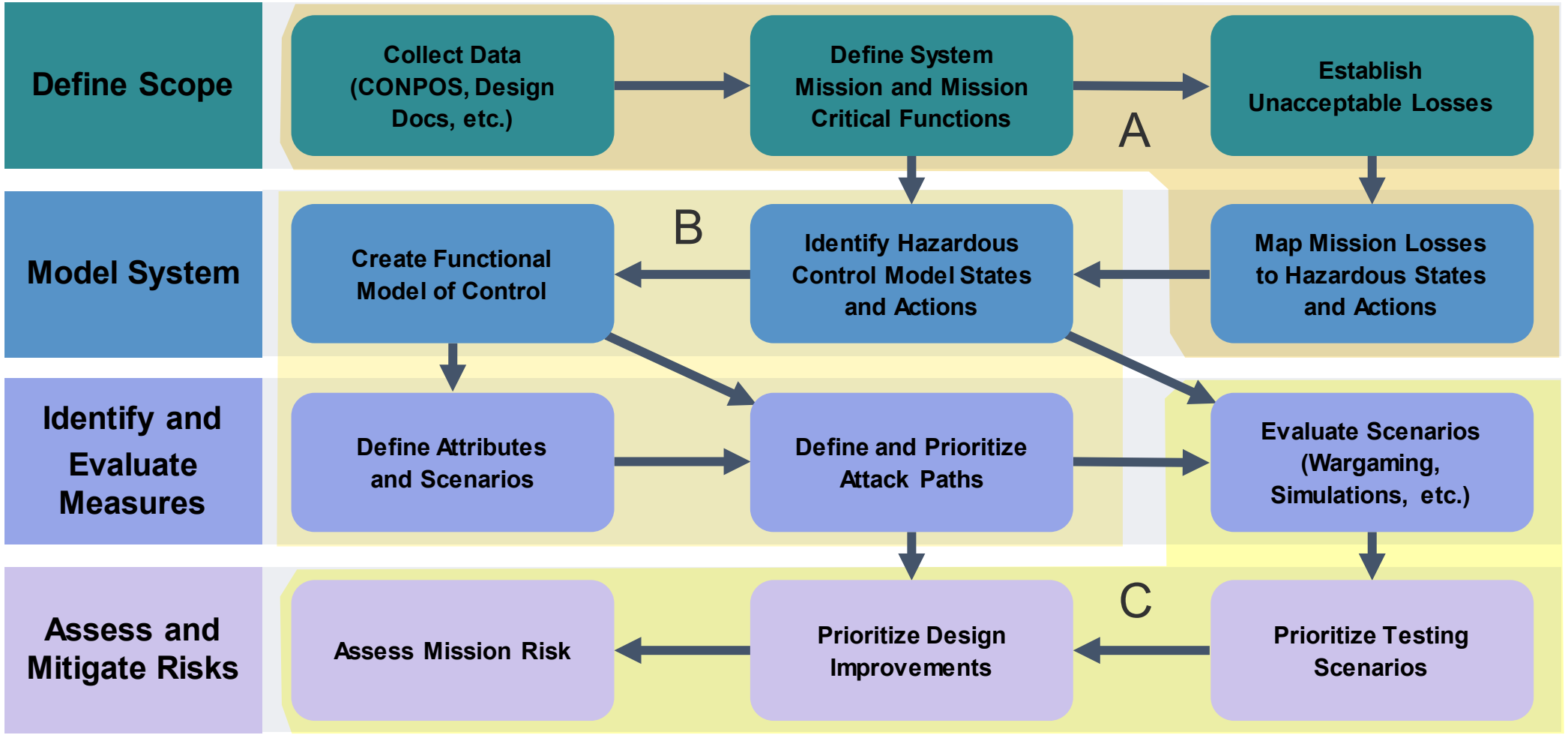
The FRAMERS Process

Proactive and based on systems theory – where every system has causal boundaries, is influenced by its context, defined by its structure, function and role, and expressed through its relations with other systems.



The FRAMERS Process

Proactive and based on systems theory – where every system has causal boundaries, is influenced by its context, defined by its structure, function and role, and expressed through its relations with other systems.



Questions?

Ryan Brunton Ryan.Brunton@jhuapl.edu
Randy Saunders Randy.Saunders@jhuapl.edu