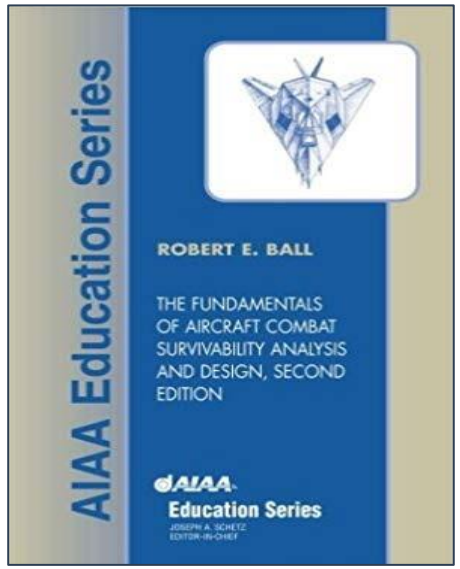
Aircraft Cyber Combat Survivability (ACCS)

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

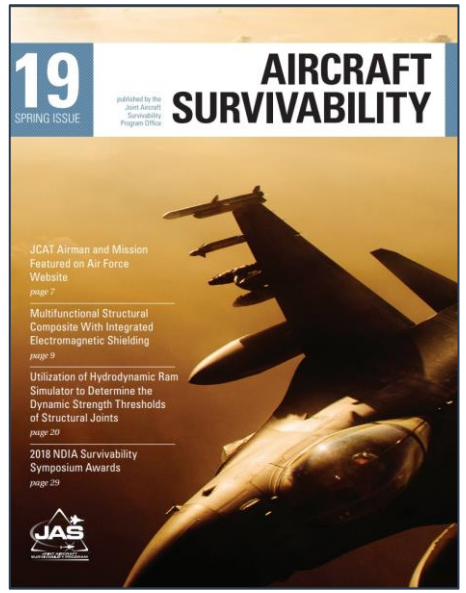
AIRCRAFT COMBAT SURVIVABILITY (ACS) INTRODUCTION

- **Aircraft Combat Survivability** is the capability of an aircraft to *Avoid* or *Withstand* a man-made hostile environment
- **Susceptibility** = How likely an aircraft is to get hit
- **Vulnerability** = How likely an aircraft is to be killed after getting hit
  - Killed can mean different things
    - "Attrition kill" means the aircraft is permanently dead (smoking hole)
    - "Mission kill" means the mission wasn't completed successfully, but the aircraft lives to fight another day



AIRCRAFT CYBER COMBAT SURVIVABILITY (ACCS) INTRODUCTION

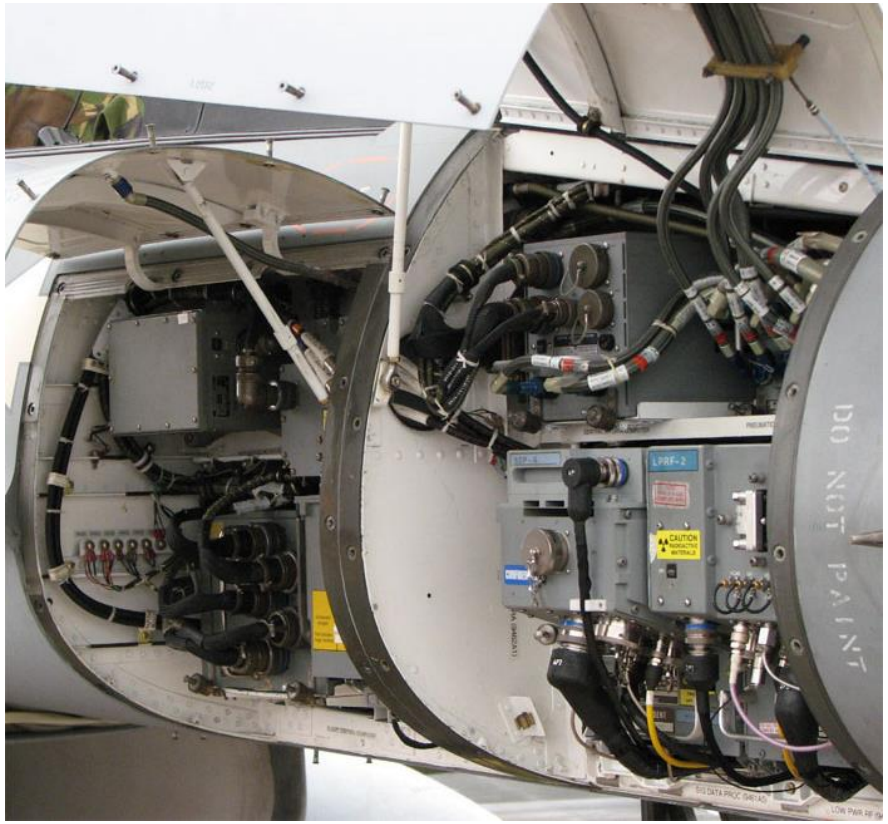
- **Aircraft Cyber Combat Survivability** focuses solely on "cyber antiaircraft weapons" that affect the aircraft in flight
  - Leverages ACS framework
    - Kinetic weapons generate physical destruction
    - Cyber weapons generate component dysfunction or functional damage
    - Can end up creating the same effects
  - Most successful cyber attacks will result in "mission kills"
    - ACCS prioritizes addressing attacks that can result in permanent, or "attrition kills"



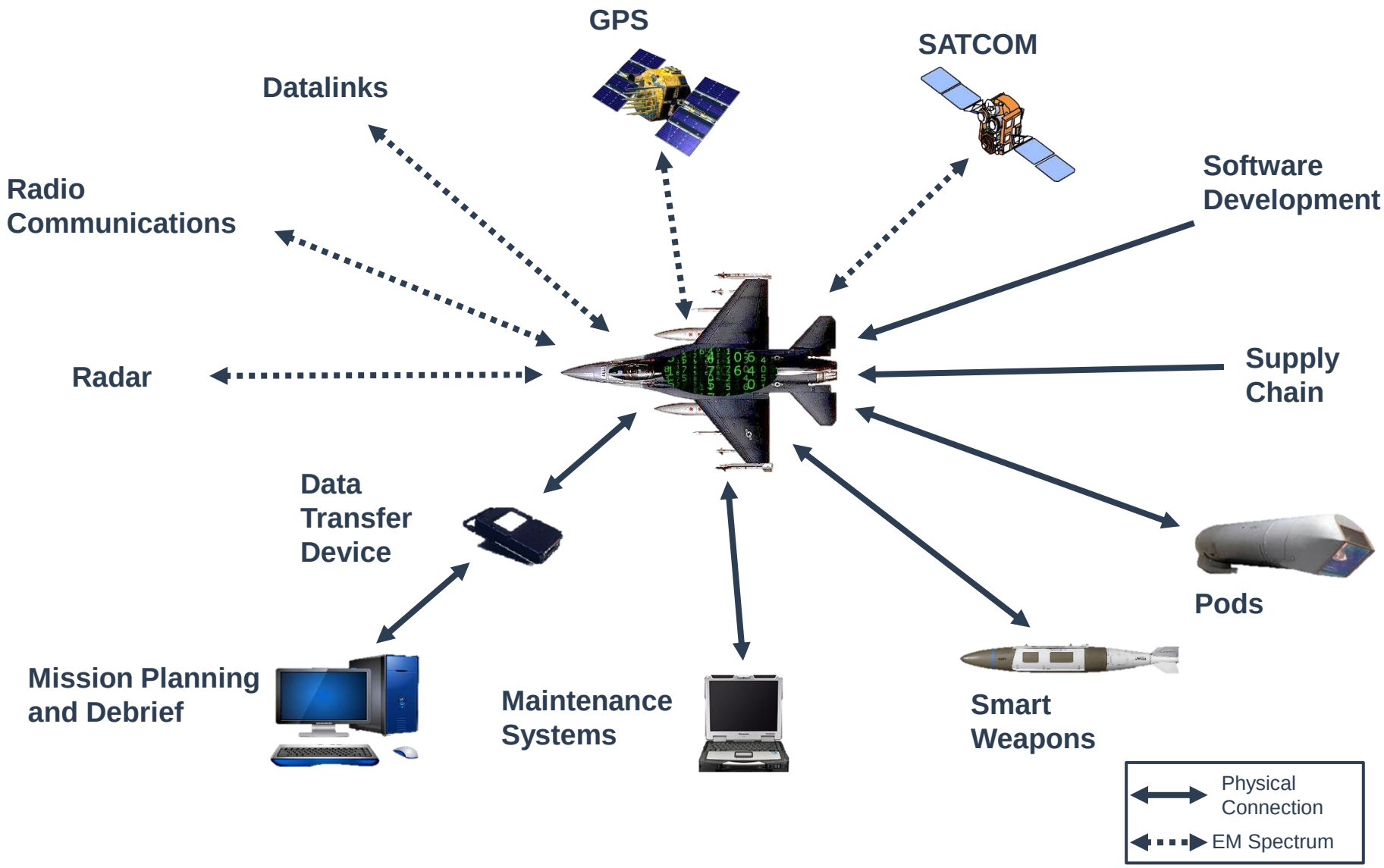
But it's an Airplane, not a Computer…





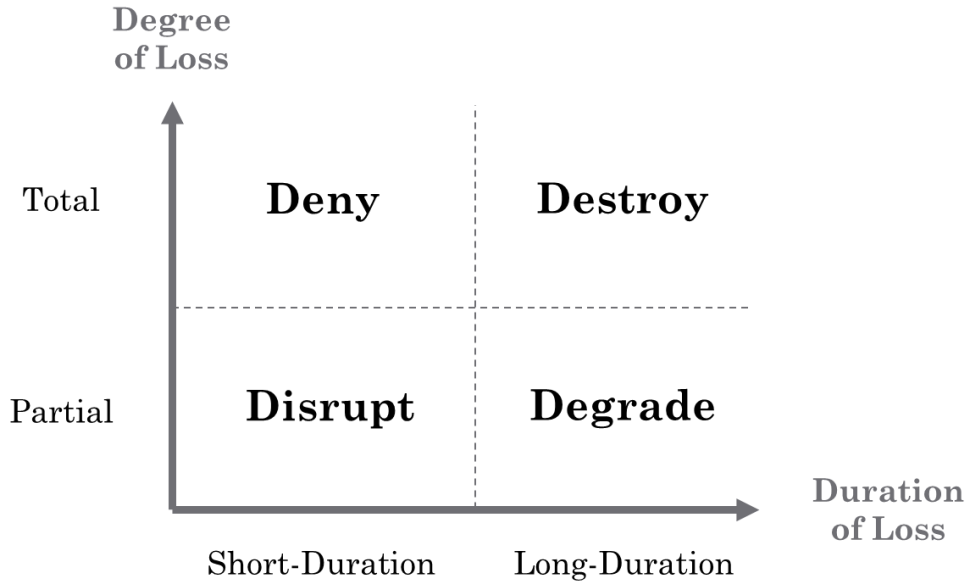


TYPICAL AIRCRAFT CYBER-ATTACK SURFACE



ACCS "Cyber-Weapons"

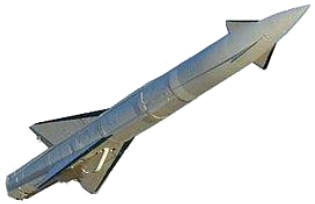
- **Creates functional damage** (or malfunction) versus physical damage
  - Can Disrupt, Degrade, Deny, or Destroy aircraft system functionality
  - Depends on Degree and Duration of loss
- **"Aimed" at aircraft systems** (inside the skin) versus off-board supporting systems
  - May use supporting systems as an attack path



- **Targets mission critical or flight critical components**
  - Mission critical is easier to target, flight critical tends to be more challenging to attack
  - Use of ACS two tier criticality with permanent kill critical more important than mission kill critical

KINETIC VS. CYBER WEAPONS





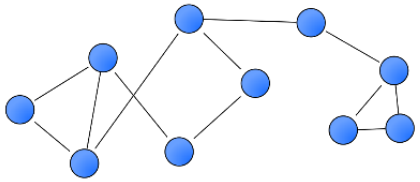
Attempted Trigger



Susceptibility

Vulnerability

	Detection and Tracking Subsystem	Warhead Transporter Subsystem	Warhead
Kinetic	System of systems to identify, find, fix, and track the target: e.g. C2, Radar, missile launcher	Propelled by chemical rocket, guided missile homes in on the target	Detonates using a chemical reaction to produce blast, fragmentation and incendiaries
Cyber	System of systems to hide the weapon's origin and get to a connection point on the aircraft	Package of code that homes in on the targeted system location and implants payload code	Executes computer code when triggered to create the adversary's desired system dysfunctions





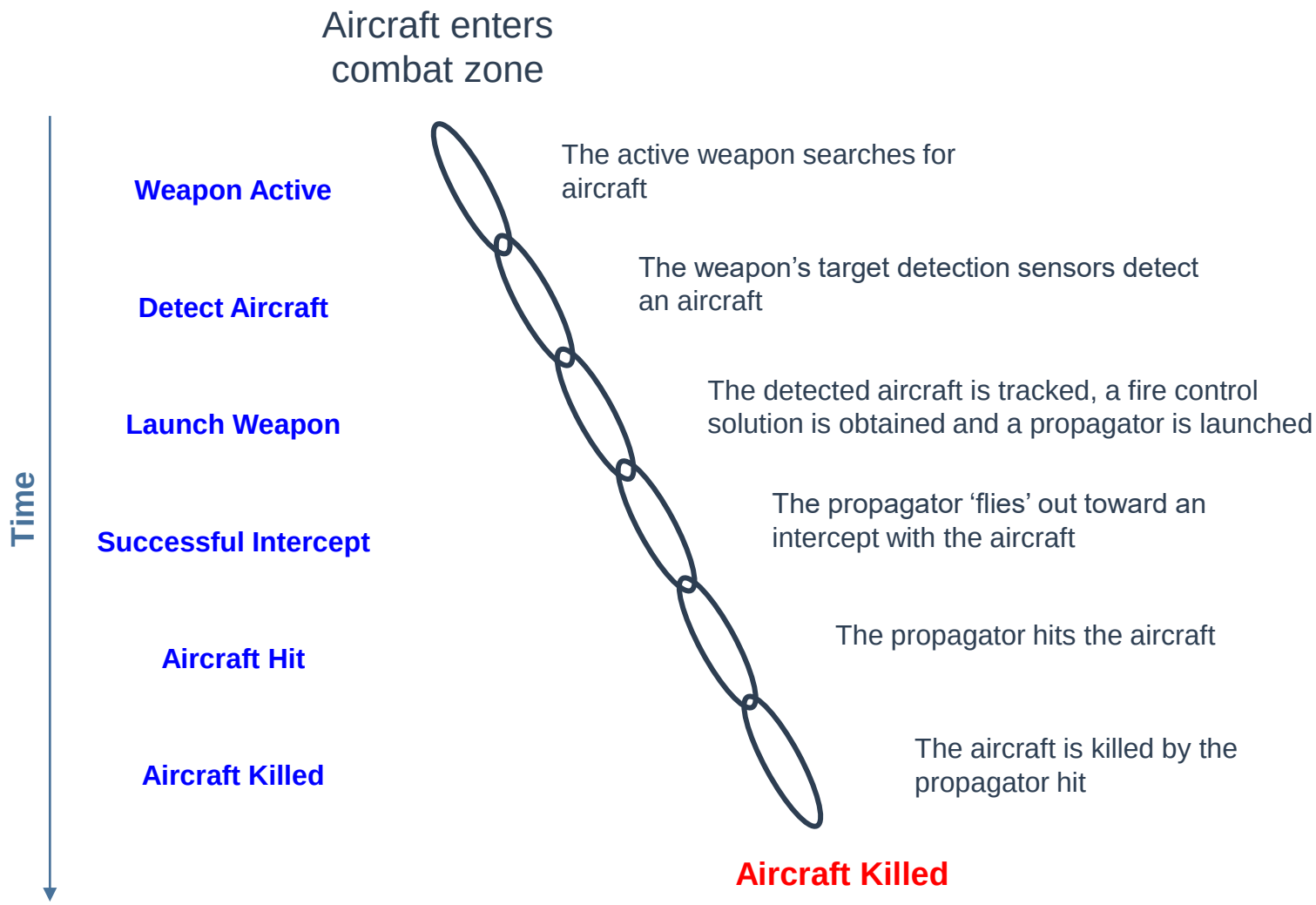


KINETIC VS. CYBER WEAPONS

	Kinetic Weapon	Cyber Weapon
Damage	Physical damage	Functional damage
Observability	Easily observed, repeatable in a lab	Hard to observe, hard to predict
History	More than 100 years combat history to build models and theories	Limited-to-no history; not yet in use in large scale
Range	Limited range Can affect anything within range	Unlimited range (with connection) Can affect only specific systems
Obfuscation	Low, generally obvious	High, purposefully hidden
Lethality	Known kinetic weapons can still be lethal	Known cyber weapons are relatively easy to render harmless

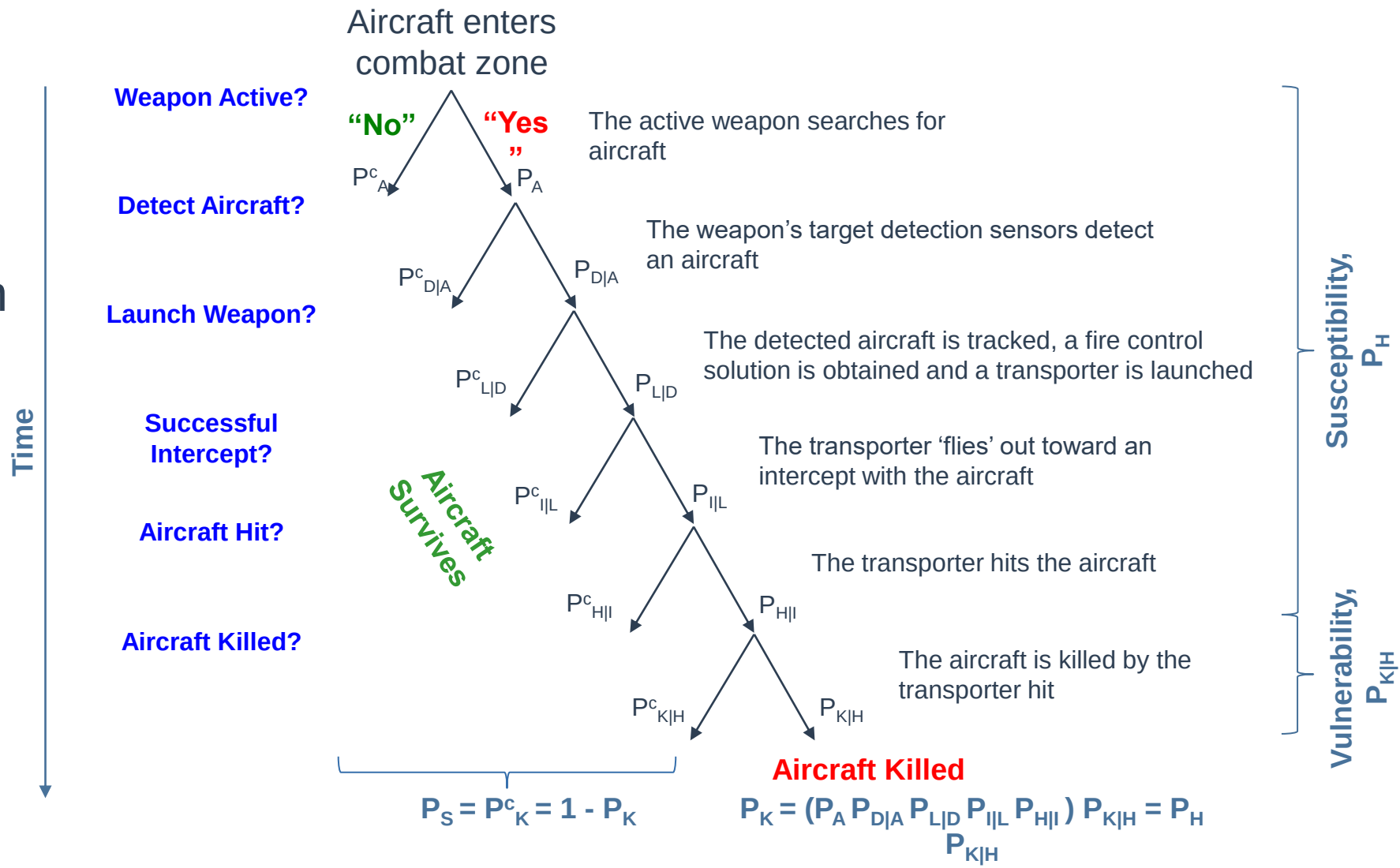
KINETIC ACS KILL CHAIN

- Time-wise sequence of the weapon's actions
- Each step must be completed successfully by the weapon for the aircraft to be killed
- Therefore, most of practical aircraft survivability engineering consists of finding ways to "break the chain"



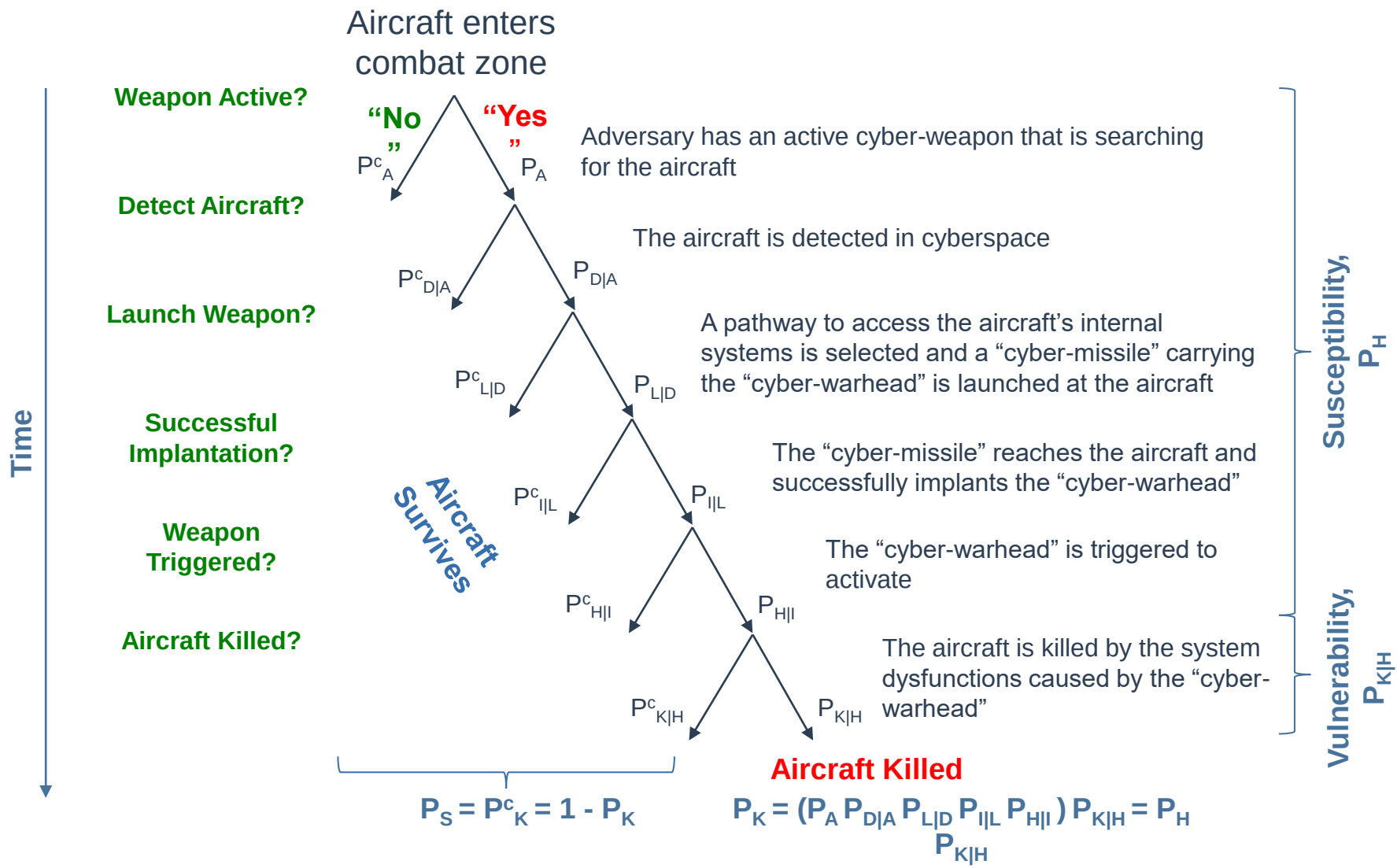
KINETIC ACS PROBABILISTIC KILL CHAIN

- We need a way to measure how well a mitigation improves survivability
- One method is to assign probabilities to each step in the kill chain
- This can be used to model the expected losses during a campaign
- A tool for determining the best mitigations, not a prediction



CYBER ACCS PROBABILISTIC KILL CHAIN

- Developing kinetic probabilities is hard—cyber probabilities are much worse
- Can still help point engineers to the points where changes can have the most impact
- Can also be used with caution in modeling and simulation to connect changes to mission and campaign level impacts



SURVIVABILITY ENHANCEMENT

- Concepts are broad categories of enhancements
- Functions are the specific implementation of a concept
- Each is split into susceptibility and vulnerability

Aircraft Combat Survivability (ACS)	Aircraft Cyber Combat Survivability
Survivability Enhancement Concept (SEC)- general functions or concepts fundamental to survivability enhancement and reducing either the susceptibility or the vulnerability of the aircraft.	***Cyber Survivability Enhancement Concept (CSEC) -*** general functions or concepts fundamental to cyber survivability enhancement and reducing either the cyber susceptibility or the cyber vulnerability of the aircraft.
Survivability Enhancement Feature (SEF) - any particular characteristic of the aircraft, specific piece of equipment, design technique, armament, or tactic that reduces either the susceptibility or the vulnerability of the aircraft and thus has the potential for increasing survivability.	***Cyber Survivability Enhancement Feature (CSEF) -*** Any particular characteristic of the aircraft, specific piece of equipment, design technique, design of supporting systems, or operational procedures that reduces either the cyber susceptibility or the cyber vulnerability of the aircraft and thus has the potential for increasing cyber survivability.

Susceptibility Reduction Concepts

- Survivability CSECs focus on avoiding the cyber weapon
- Several changes between kinetic and cyber due to the "physics" of cyberspace

Kinetic Energy Weapons: Survivability Enhancement Concept (SEC)	Cyber Weapons: Cyber Survivability Enhancement Concept (CSEC)
Situational Awareness	Situational Awareness
Signature Control	Signature Management
Electronic Noise Jamming and Deceiving	Deception
Expendables	Cybersecurity Hardening
Threat Suppression and Offensive Weapons	Threat Suppression
Mission Planning, Tactics, Flight Performance, and Crew Training and Proficiency	Training and Tactics

VULNERABILITY REDUCTION CONCEPTS

- Vulnerability CSECs focus on system resiliency, being able to "fight hurt" and still get the mission done
- Kinetic SECs all have functional equivalent CSECs

Kinetic Energy Weapons: Survivability Enhancement Concept (SEC)	Cyber Weapons: Cyber Survivability Enhancement Concept (CSEC)
Component Location	Component Location and Logical Separation
Component and System Redundancy (with effective separation)	System Redundancy (with effective separation and diversity)
Passive and Active Damage Suppression	Malfunction Suppression (passive and active)
Component and System Capability Recovery	System Capability Recovery
Component Elimination or Replacement	Component Elimination or Replacement
Component Shielding	Component Shielding

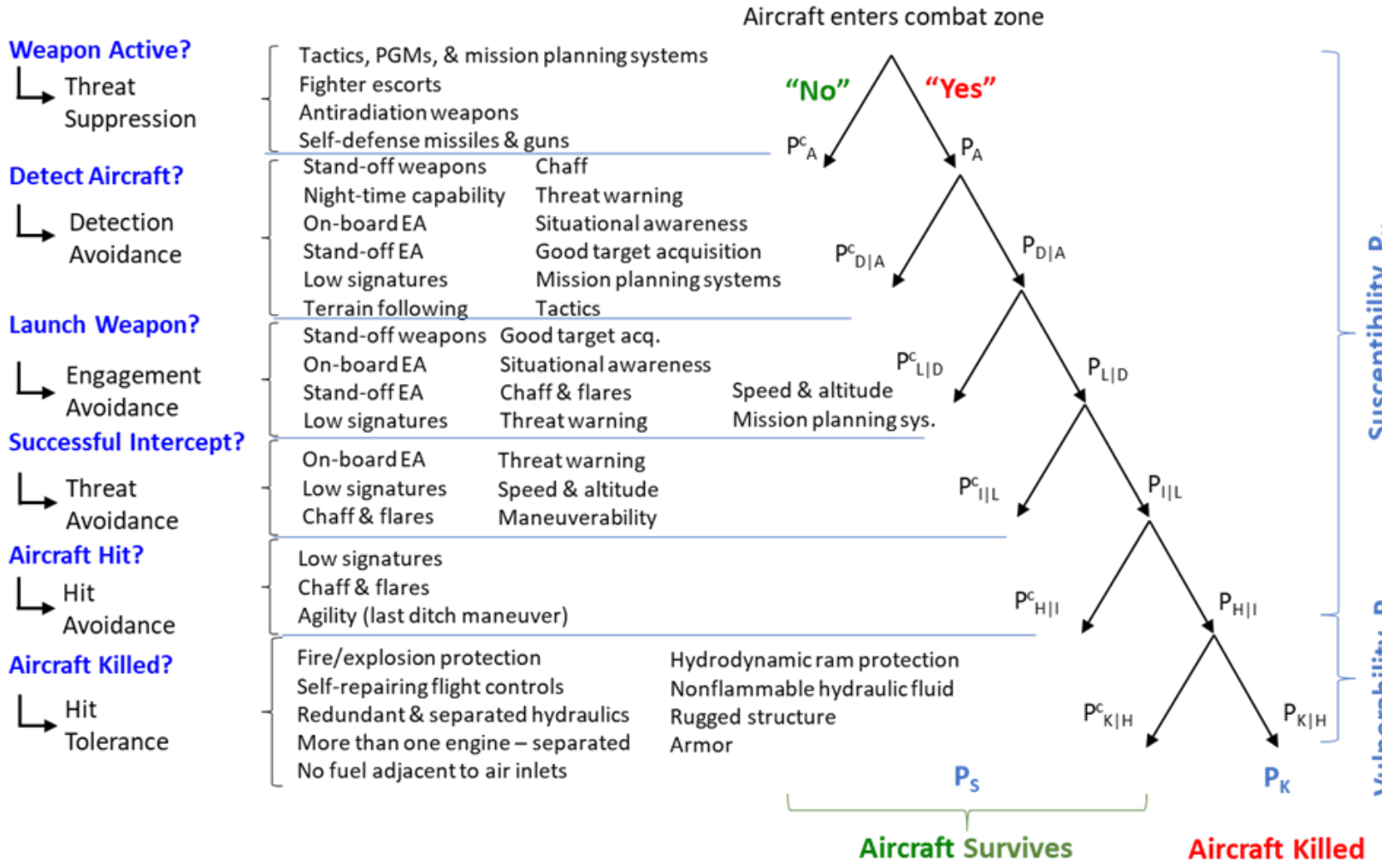
SURVIVABILITY ENHANCEMENT FEATURES

- While concepts are broad, features are specific to a particular platform and implementation
- How then do we determine what CSEFs to use?

Aircraft Combat Survivability (ACS)	Aircraft Cyber Combat Survivability
Survivability Enhancement Concept (SEC)- general functions or concepts fundamental to survivability enhancement and reducing either the susceptibility or the vulnerability of the aircraft.	***Cyber Survivability Enhancement Concept (CSEC) -*** general functions or concepts fundamental to cyber survivability enhancement and reducing either the cyber susceptibility or the cyber vulnerability of the aircraft.
Survivability Enhancement Feature (SEF) - any particular characteristic of the aircraft, specific piece of equipment, design technique, armament, or tactic that reduces either the susceptibility or the vulnerability of the aircraft and thus has the potential for increasing survivability.	***Cyber Survivability Enhancement Feature (CSEF) -*** Any particular characteristic of the aircraft, specific piece of equipment, design technique, design of supporting systems, or operational procedures that reduces either the cyber susceptibility or the cyber vulnerability of the aircraft and thus has the potential for increasing cyber survivability.

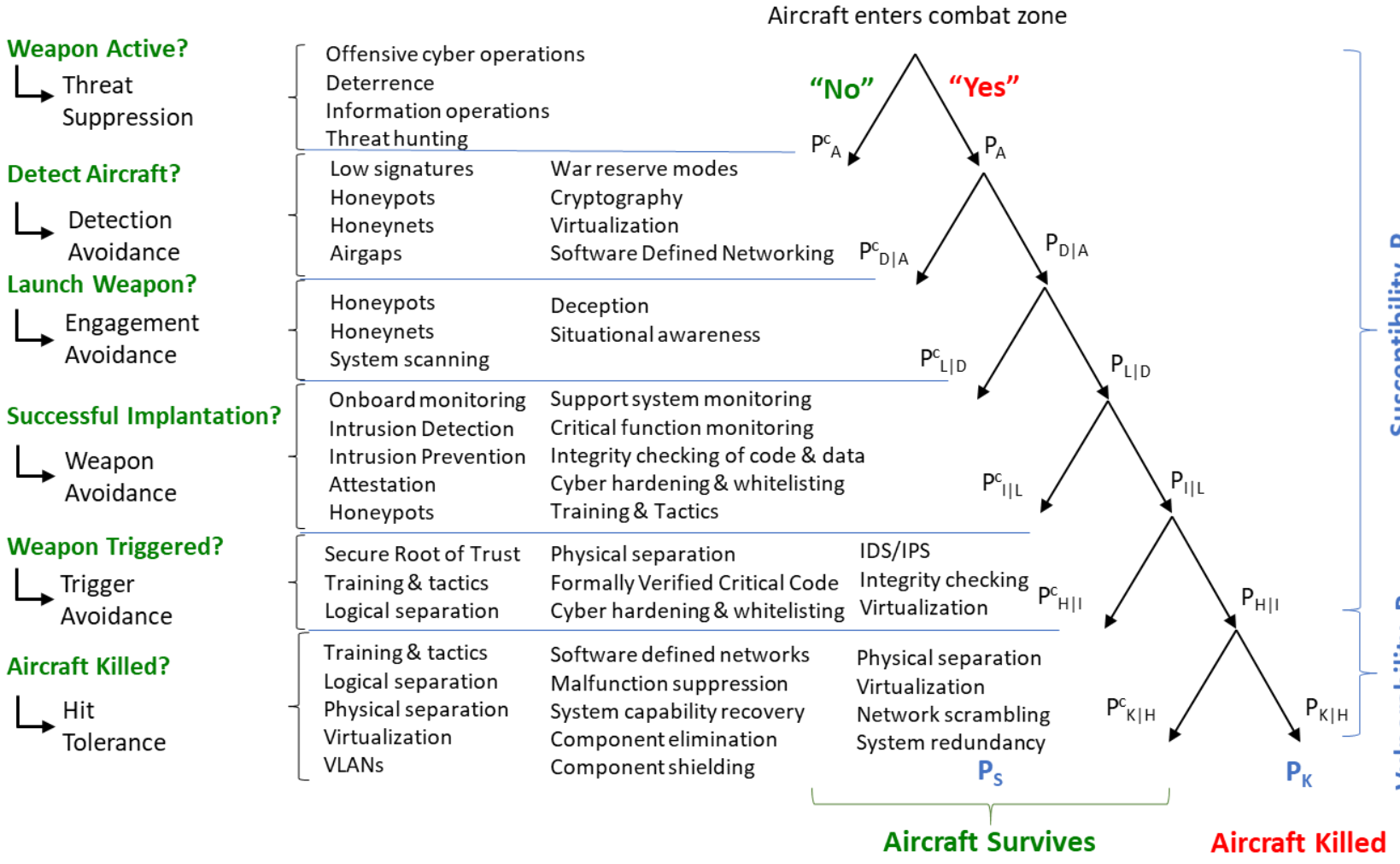
SELECTED KINETIC SEFS

- SEFs should reduce the likelihood that some step of the kill chain is broken
  - Can have performance cost
  - Can be a change in operations
  - Can involve significant design changes



SELECTED CYBER SEFS

- CSEFs should also reduce the likelihood that some step of the kill chain is broken
  - Can also have performance cost
  - Can be a change in operations
  - Can involve significant design changes

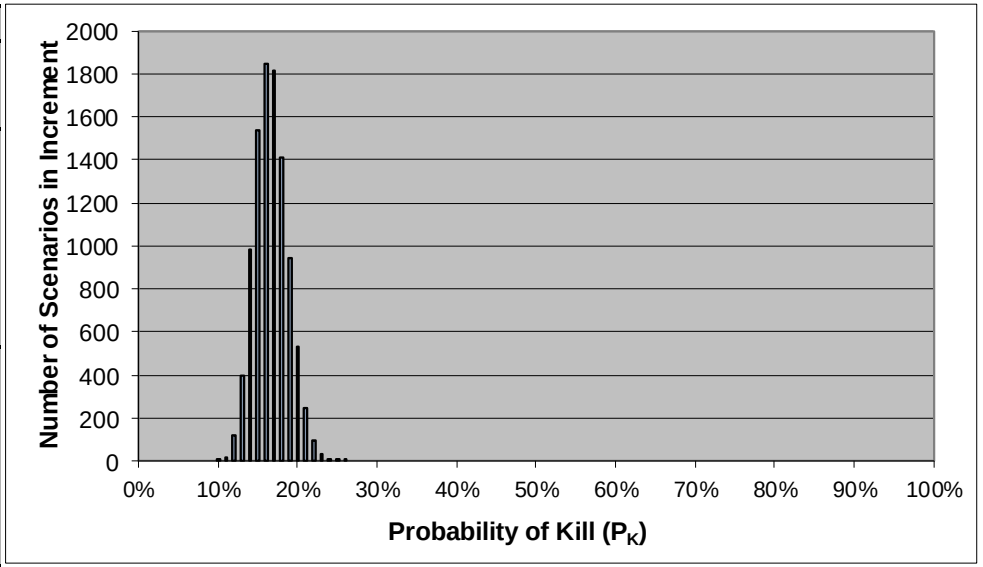


Modeling the Probability of Kill

- The probabilistic kill chain can be utilized to model whether a system will be killed by a particular cyber attack or not
- Utilize 90% Confidence Intervals (CI) instead of point values
- Can use different distributions
- Provides uncertainty

Inputs	Probability adversary has active cyber weapon and is searching for the aircraft (P_A)	Probability adversary detects aircraft in cyberspace ($P_{D|A}$)	Probability adversary determines path and launches cyber trasnsporter ($P_{L|D}$)	Probability the cyber warhead is successfully implanted ($P_{I|L}$)	Probability the cyber warhead is triggered ($P_{H|I}$)	Probability the aircraft is killed by the system malfunctions caused by the cyber warhead ($P_{K|H}$)
90%CI Upper	85.4%	70.8%	71.7%	73.0%	88.0%	93.2%
90% CI Lower	72.8%	58.0%	58.1%	59.7%	75.9%	86.8%
Mean	79.1%	64.4%	64.9%	66.3%	81.9%	90.0%

Outputs	Probability that the Aircraft/Mission will be killed (P_K)	Probability that the Aircraft/Mission will survive (P_S)
90%CI Upper Bound	19.57%	87.28%
90%CI Lower Bound	12.72%	80.43%
Standard Deviation	0.0208	0.0208
Mean	16.15%	83.85%

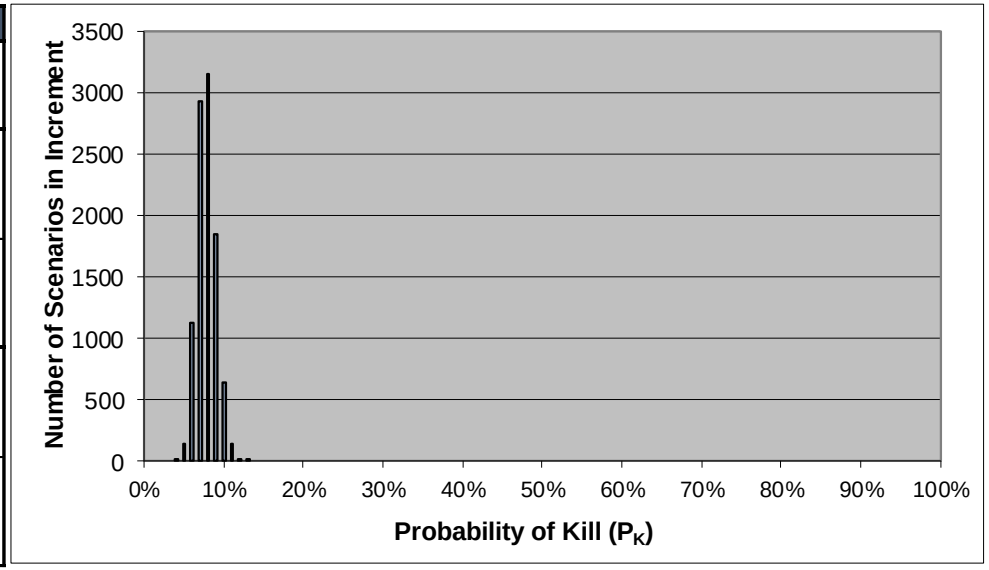


ACCOUNTING FOR MITIGATIONS

- To illustrate a simple mitigation, the cyber experts who scored the previous scenario, rescored with a design mitigation
- Added an IDS to the main aircraft avionics bus
- Significantly reduced $P_{I|L}$
- No major effects elsewhere in the kill chain

Inputs	Probability adversary has active cyber weapon and is searching for the aircraft (P_A)	Probability adversary detects aircraft in cyberspace ($P_{D|A}$)	Probability adversary determines path and launches cyber trasnsporter ($P_{L|D}$)	Probability the cyber warhead is successfully implanted ($P_{I|L}$)	Probability the cyber warhead is triggered ($P_{H|I}$)	Probability the aircraft is killed by the system malfunctions caused by the cyber warhead ($P_{K|H}$)
90%CI Upper	85.4%	70.8%	71.7%	35.6%	88.0%	93.2%
90% CI Lower	72.8%	58.0%	58.1%	24.4%	75.9%	86.8%
Mean	79.1%	64.4%	64.9%	30.0%	81.9%	90.0%

Outputs	Probability that the Aircraft/Mission will be killed (P_K)	Probability that the Aircraft/Mission will survive (P_S)
90%CI Upper Bound	9.22%	94.61%
90%CI Lower Bound	5.39%	90.78%
Standard Deviation	0.0116	0.0116
Mean	7.30%	92.70%



MODERN TECHNOLOGY SOLUTIONS, INC.

USING MODELING AND SIMULATION

- Estimating the P_K of a single weapon versus a single aircraft is interesting, but not compelling
- Mission owners need to know the mission impact
- Utilizing P_K's calculated using the previously discussed methods, cyber weapons can then be modeled in campaign level simulations
- This then gives decision-makers the "so what" in various scenarios they care about of the effect of cyber weapons
- Also provides the mission gains of various potential mitigation strategies on both the engineering and operational fronts

CONCLUSIONS

- The fundamental principles and approach used in Aircraft Combat Survivability (ACS) provide a useful framework for Aircraft Cyber Combat Survivability (ACCS)
- Cyber weapons have an analogous probabilistic kill chain to kinetic weapons that can model the P_K of an engagement
- That P_K can then be used in a campaign level simulation to express the mission impact of a cyber weapon
- The same campaign level model provides an excellent way to understand the return on investment for a particular mitigation approach or cyber survivability enhancement feature

MODERN TECHNOLOGY SOLUTIONS, INC.®

Questions?

FUNDAMENTAL ACS AND ACCS DEFINITIONS

Aircraft Combat Survivability (ACS)	Aircraft Cyber Combat Survivability
Aircraft Combat Survivability = The capability of an aircraft to avoid or withstand a man-made hostile environment, where: • to avoid means the aircraft avoids being physically hit by one or more warhead damage mechanisms; and • to withstand means the aircraft eventually functions, while in flight, at a useful or acceptable level after being hit by one or more warhead damage mechanisms.	*Aircraft Cyber Combat Survivability* = The capability of an aircraft to avoid or withstand a man-made hostile cyber environment, where: • to avoid means the aircraft's internal cyber systems avoid being accessed and modified and having one or more implanted malfunction mechanisms activated; and • to withstand means the aircraft eventually functions, while in flight, at a useful or acceptable level, after the activation of one or more implanted malfunction mechanisms.
Aircraft Susceptibility = The inability of an aircraft on a mission to avoid being physically hit by one or more warhead damage mechanisms. The more likely an aircraft is hit by one or more warhead damage mechanisms, the more susceptible is the aircraft.	*Aircraft Cyber Susceptibility* = The inability of an aircraft on a mission to avoid having its internal cyber system's code accessed and modified and one or more implanted malfunction mechanisms activated. The more likely an aircraft's internal cyber systems are accessed and modified and one or more implanted malfunctions are activated, the more cyber susceptible is the aircraft
Aircraft Vulnerability = The inability of an aircraft to eventually withstand, while in flight, one or more hits by warhead damage mechanisms. The more likely an aircraft is killed by the hits, the more vulnerable is the aircraft.	*Aircraft Cyber Vulnerability* = The inability of an aircraft to eventually withstand, while in flight, the activation of one or more implanted malfunction mechanisms. The more likely an aircraft is killed by the activation of one or more implanted malfunction mechanisms, the more vulnerable is the aircraft.

MODERN TECHNOLOGY SOLUTIONS, INC.

SITUATIONAL AWARENESS

- If a cyber attack happened how would the pilot know?
  - Systems failure may be extremely common without cyber attacks
  - Standard maintenance procedures may be spoofed
- Education and reporting systems
  - Abnormal operation reports
  - Will only happen if operators know cyber is a “thing”
- Exterior IT-based monitoring systems
  - Numerous commercial tools available—relatively easy to implement
  - Clever attackers will stay hidden all the way to the aircraft
- Monitoring Systems built into design baseline
  - Watching key files that shouldn’t change, monitoring for communications traffic that shouldn’t be there
  - Very difficult and expensive given unique architectures, safety, and airworthiness

SIGNATURE MANAGEMENT

- Making the system harder to find and access, analogous to stealth
- Airgaps are a traditional defense for weapon systems
  - How air gapped are you really?
  - Have you had a red team look?
  - Strengthening an airgap can be a very affordable and effective approach
- More advanced techniques can include software based networks that constantly reconfigure so an adversary has trouble figuring out what is where
  - Can be very challenging, but a one time pre-planned shift akin to Electronic Warfare's War Reserve Modes may be more achievable
- Numerous high-quality honeypots can make it harder for an adversary to determine what is real—equivalent to jamming

DECEPTION

- Making an adversary believe they are successfully attacking you when either they are attacking a decoy, or you have inoculated your system
  - Just like other types of deception, you may want to appear stronger, or weaker depending on what you are trying to accomplish
  - Battle damage assessment is a tremendous problem with cyber weapons because it is so easy to provide false data back if the attack is known
  - Fool the enemy successfully once and now everything else they think they have is suspect as well
- Honeypots and Honeynets
  - Fake systems that confuse the attacker
  - Can be very simple or elaborate depending on the defender's resources and what they are trying to accomplish
  - Also has an early warning function

CYBERSECURITY HARDENING

- Focus of traditional Cybersecurity
- Harden the traditional-IT systems that interconnect and interact with the aircraft such as maintenance and mission planning systems
- Restrict access—Strengthen your airgap, check for unexpected communication pathways and control the pathways that do exist
- Secure code signing and checking—make sure what is loaded on the system is what you think it is and wasn't tampered with
- Whitelisting—Only allow "known good" software to execute on your system
- Attestation—Techniques to verify that software and hardware on the aircraft have not changed
  - Very similar to hashing in the traditional IT world where a "hash" is created via a mathematical algorithm that is unique to that code or data
  - Verifies the system hasn't changed, not that it is good

MODERN TECHNOLOGY SOLUTIONS, INC.

THREAT SUPPRESSION

- Cyber equivalent of Suppression of Enemy Air Defenses (SEAD)
- Disrupting enemy cyber-attack capabilities and infrastructure
- Cyber-ninjas *love* talking about this and while I think it can be useful, I see it as a niche capability
  - Think of it much like strategic bombing in WWII, an independent mission that validates organizations
  - It is really hard to do, and even harder to know that you really got everything
  - Remember, the infrastructure required to launch an attack can be very modest, and can generally be hijacked from other people you don't want to attack
  - Feeding the information discovered back to the defenders might actually be more useful than the disruption itself…but they likely won't be told about it

MODERN TECHNOLOGY SOLUTIONS, INC.

TRAINING AND TACTICS

- Teaching both pilots and maintainers how cyber attacks work and how their actions can enable enemy cyber attacks
- This is potentially tremendously valuable, and very inexpensive, but not happening on a large scale
- Annual “cyber training” isn’t going to cut it
  - Needs to be carefully targeted and focused
  - Needs to be delivered from credible sources
- To achieve the largest effect, flow cyber attacks into training and exercises

Component Location and Logical Separation

- Just like in kinetic ACS, you don't want multiple components to be taken out with a single "hit"
- Separate networks is one (albeit expensive) possibility
- Virtualization offers many other opportunities to have multiple versions of the same software operating in multiple "locations"
  - Could have multiple "voting" schemes much like is common in flight controls
  - Likely will be a challenge initially with airworthiness
- Virtualization has an "Achilles heel" in the hypervisor, if the adversary gets to it, they own all the virtualized machines

MODERN TECHNOLOGY SOLUTIONS, INC.

System Redundancy

- It isn't enough to have multiple of the same exact component as the same cyber-attack could take them all out
- Ideally, you would want different hardware and software, but that obviously will be prohibitively expensive in most cases
- One potentially reasonably cheap approach is to have multiple different versions of software on one avionics box
  - Could be older versions or stripped-down basic versions
  - Could automatically load if a failure or attack is detected
  - Need to ensure attackers can simply easily overwrite the backup software
- Virtualization enables a number of powerful defensive techniques
  - Have multiple computers that all do the same math and check each other's outputs
  - "Throw away" bad or infected computers and build new ones seamlessly while still airborne

Malfunction Suppression

- Passive
  - Systems should be designed to respond securely to unexpected, malformed, or malicious data and commands
  - Buffer overflows
  - Radar altimeter should likely never reprogram the stores management system
- Active
  - Misbehaving sub-systems should be cut off from the network, ignored, or shut down
  - Requires situational awareness and control mechanism
- In specialized situations cyber defenders may have a role
  - UAS that require a communications link for mission capability
  - Large command and control aircraft where cyber defender can be on the platform
  - Do we want a communications link to cyber defenders?—probably not

MODERN TECHNOLOGY SOLUTIONS, INC.

System Capability Recovery

- Restore to a previous state before the cyber attack
  - Unlike most physical damage, cyber damage can be repaired in flight
- Could be done at pilot command, or automatically when an attack is detected
- Could load new software over compromised avionics
  - Can be done from within avionics or from the outside via a security component
  - Clean software
  - Previous version
  - Software with only basic functionality as a “get home” mode
  - Memory is relatively inexpensive and the switching mechanism doesn’t have to be overly complex
  - Virtualization could allow the backup systems to be “hot” and running all the time

Component Elimination or Replacement

- Something that isn't there can't be an attack pathway
- Some functionality may be inherently un-defensible
  - Do you ever want to have an open cyber connection to a combat aircraft in flight?
  - Is it worth downloading your maintenance data before landing?
- Are the extra "bells and whistles" worth the increased risk that you will lose the entire mission and/or aircraft?
- This CSEC can save you substantial amounts of money, but only if you do it early in the lifecycle

MODERN TECHNOLOGY SOLUTIONS, INC.

COMPONENT SHIELDING

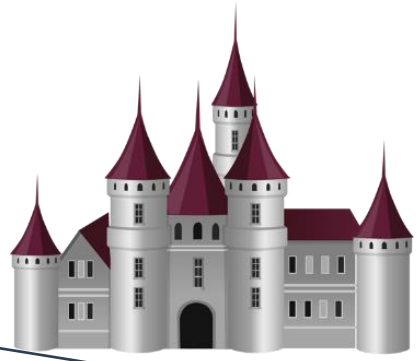
- Helps components resist functional damage after a cyber warhead has been triggered
  - Protect non-infected components from infected ones
  - Limit the ability of infected components to infect others
- Hardware root of trust
  - Makes it hard for adversaries to get their malicious software to run
- Physical loading switches
  - Prevents adversaries from remotely loading software, if well implemented can be very hard to get around
  - Discrete switches are better, messages on a bus can be spoofed

DEFINITIONS

- Mission Assurance (MA) A process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DoD mission-essential functions in any operating environment or condition. (DoDD 3020.40)
- System A functionally, physically, and/or behaviorally related group of regularly interacting or independent elements; that group of elements forming a unified whole. (JP 3-0)
- Assurance Confidence or certainty in one's own abilities. (Oxford Dictionary)
- Survivability The capability of a system or its crew to avoid or withstand a manmade hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission. (DAU Glossary); All aspects of protecting personnel, weapons, and supplies while simultaneously deceiving the enemy. (JP 3-34)
- Cybersecurity Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DODI 8500.01)
- Cyber resiliency The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources regardless of the source. (NIST SP 800-160 vol 2); The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources. (MITRE)
- Cyberspace defense Actions normally created within DoD cyberspace for securing, operating, and defending the DoD information networks. Specific actions include protect, detect, characterize, counter, and mitigate (DoDI 8500.01).
- Defensible Capable of being defended. (Merriam-Webster Dictionary)

EXAMPLE 1 - CASTLE

Mission: Keep the people inside alive and safe



Mission Assurance
Making sure the system can still accomplish its mission despite attack

Hardening
Making the system hard to attack and keeping adversaries out

- Walls
- Moat
- Drawbridge
- Protection of critical assets (people)

Resiliency
Making the system still function well enough after enemies get in

- Protected keep to inside the walls
- Additional layers of walls
- Cleared areas to trap attackers between walls

Defensibility
Making the system easy to defend by human defenders

- Rampart for soldiers to walk on and observe enemy
- Towers
- Holes in the walls to shoot from

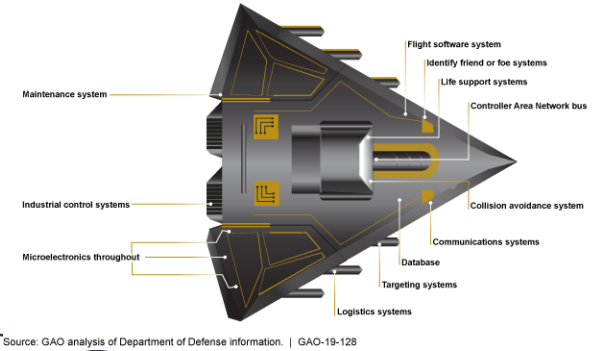
Recoverability
Making the system easy rebuild after a successful attack

- Building materials to rebuild walls
- Skilled Craftsmen such as masons and carpenters
- Building tools

EXAMPLE 2 – F-99

Mission: Neutralize enemy targets

Mission Assurance
Making sure the system can still accomplish its mission despite attack



Hardening
Making the system hard to attack and keeping adversaries out

- Minimize attack surface
- Code signing and verification
- Harden MX loaders and mission planning systems
- Stealth

Resiliency
Making the system still function well enough after enemies get in

- Active damage suppression
- Component redundancy with diversity
- Secure partitioning
- Backup systems

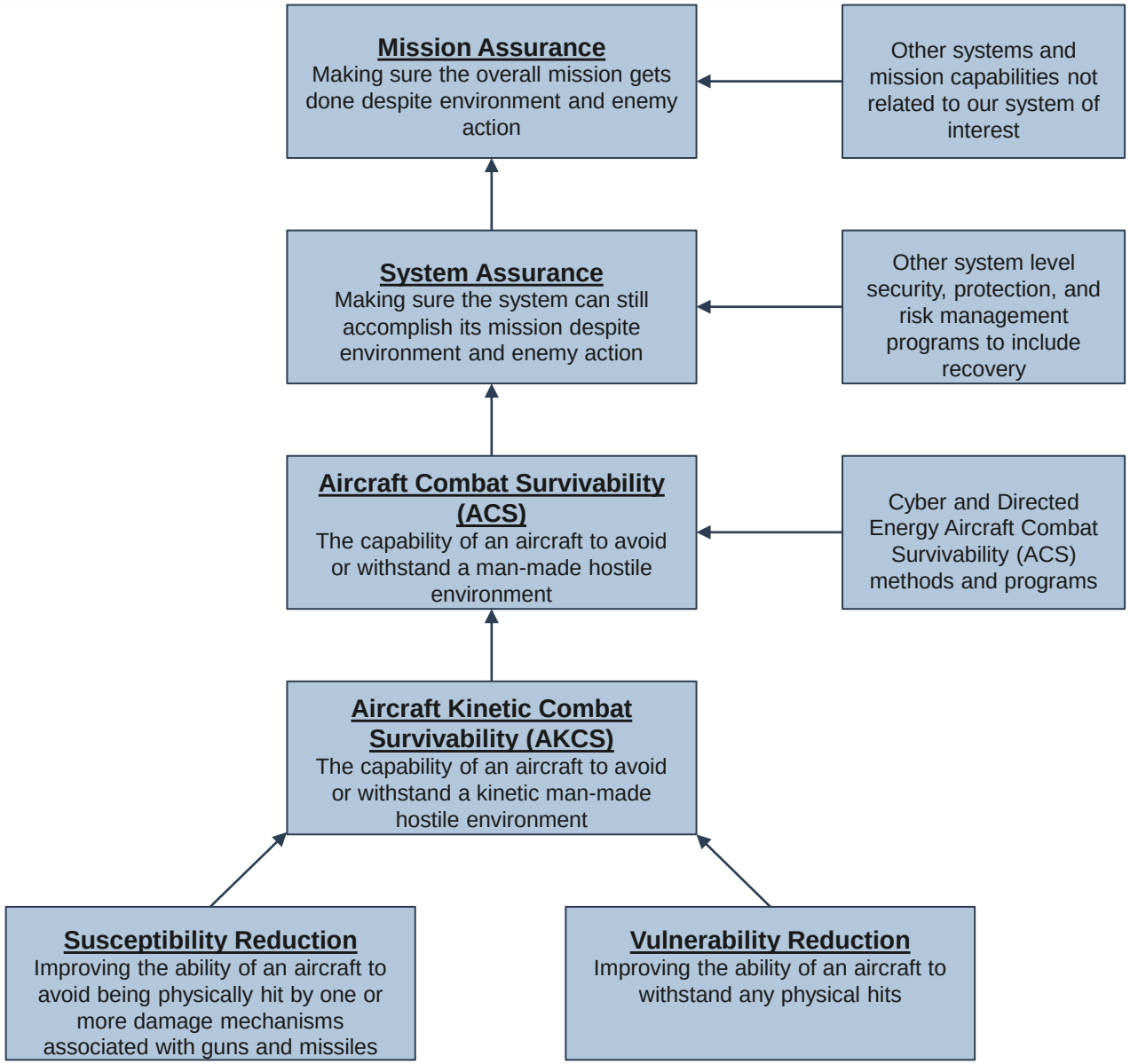
Defensibility
Making the system easy to defend by human defenders

- Support system monitoring
- Logging tools built into baseline
- Honeypots and honeynets
- Intrusion Prevention Systems (IPS)

Recoverability
Making the system easy rebuild after a successful attack

- Forensics capability
- Rapid software loading
- War reserve modes
- Rapid software development & test
- Vulnerability management

KINETIC ACS TAXONOMY



ACCS TAXONOMY

