P5

Air Vehicle Design

AOE 4065 – 4066

III. Project Management Topics

Course Module P5

Project Risk Management

Kevin T. Crofton Department of Aerospace and Ocean Engineering
Blacksburg, VA

13 August 2024

AOE 4065-4066:
Capstone Air Vehicle Design (AVD) Course Modules (CMs)

Overview of AVD Courses

I. Foundational Elements

F1. Design: *An Engineering Discipline*

F2. Systems and Systems Thinking

F3. Basics of Systems Engineering

F4. Decision Making with Ethics and Integrity

II. Air Vehicle Design Fundamentals

A1. Purpose & Process

Conceptual Design

A2. Understand the Problem

A3. Solve the Problem

A4. Initial Sizing: *Takeoff Weight Estimation*

A5. Initial Sizing: *Wing Loading and Thrust Loading Estimation*

A6. Cost Considerations

A7. Concept to Configuration: *Key Considerations*

A7A. Configuration Layout: *Drawings & Loft*

Conceptual & Preliminary Design

A8. Trade Studies

A9. Use of Software Tools

A10. Preliminary Design: *Baseline Design Refinement & Validation*

III. Project Management Topics

P1. Basics of Project Management and Project Planning

P2. Project Organization

P3. Roles & Responsibilities of Team Members

P4. Project Execution: *Teamwork for Success*

P5. Project Risk Management

P6. Delivering Effective Oral Presentations

P7. Writing Effective Design Reports

Disclaimer

Prof. Pradeep Raj, Aerospace and Ocean Engineering, Virginia Tech, collected and compiled the material contained herein from publicly available sources solely for educational purposes.

Although a good-faith attempt is made to cite all sources of material, we regret any inadvertent omissions.

CRUCIALLY IMPORTANT

CMs only introduce key topics and highlight some important concepts and ideas…but without sufficient detail.

We must use lots of Reference Material* to add the necessary details!

(*see Appendix in the Overview CM)

Outline

P5. Project Risk Management

NOTE

In this CM, we first discuss *what ‘Risk’ is* and what its sources *are before diving into the specifics of ‘Risk Management’*.

What is Risk?

- **Risk is a normal condition of existence. It is inherent in all activities.**
- **Risk is the *potential* for the occurrence of a future reality that may or may not happen.**
- **If the probability of occurrence is not known, the risk is undefined.**
- **'Risk' and 'Problem' are *<u>not</u>* synonymous. Defining risk helps us understand whether or not a future reality—if it occurs—will be a problem.**
- **Knowledge of risk is an opportunity to avoid a problem.**
- ***Risk Exists* whether you acknowledge it, whether you believe it, whether you write it down, or whether you understand it!**
- **Risk is neither good nor bad; it is just how things are.**
- **In order to make progress, risks must be understood and managed to acceptable levels.**

Source: Adapted from Chapter 15, SE 5

Risk and Some FAQs

- ***What is risk?*** A risk is an uncertain future condition that places some part (or all) of the expected outcomes outside of nominal expectations.
- ***Will risk occur?*** The risk has some *probability* of occurring. (a.k.a. likelihood or certainty)
- ***If risk occurs, what happens?*** A risk may lead to a systemic outcome with positive or negative consequences. This outcome is referred to as an *effect*. (a.k.a. “impact” or “consequence”)
- ***To which risks should we pay attention****?* An effect might not propagate to a consequence at a systemic level. We should distinguish between local and systemic effects and pay first attention to those of greater systemic consequence.
- ***Should we respond?*** Can we? *Exposure* is an aggregate measure of a risk’s criticality. We **mitigate** to modify exposure in a direction that strengthens the project.

Source: Adapted from Lectures by Dr. Bryan Moser, MIT, on Design of Projects

Risk Isn’t a New Idea!

Code of Hamurabi: *Babylonian Legal Text 1755-1750 BC*

- 229. If a builder builds a house for someone, and does not construct it properly, and the house which he builds falls in and kills its owner, then that builder shall be put to death.
- 230. If it [were to] kill the son of the owner, the son of that builder shall be put to death.
- 231. If it [were to] kill a slave of the owner, the he shall pay slave for slave to the owner of the house.

- 232. If it [were to] ruin goods, he shall make compensation for all that has been ruined, and in as much as he did not construct properly this house which he built and it fell, he shall re-erect the house from his own means.
- 233. If a builder [were to] build a house for someone, even though he has not yet completed it; if then the walls seem toppling, the builder must make the walls solid from his own means.

Source: Adapted from Lectures by Dr. Bill Grossmann on Design of Projects

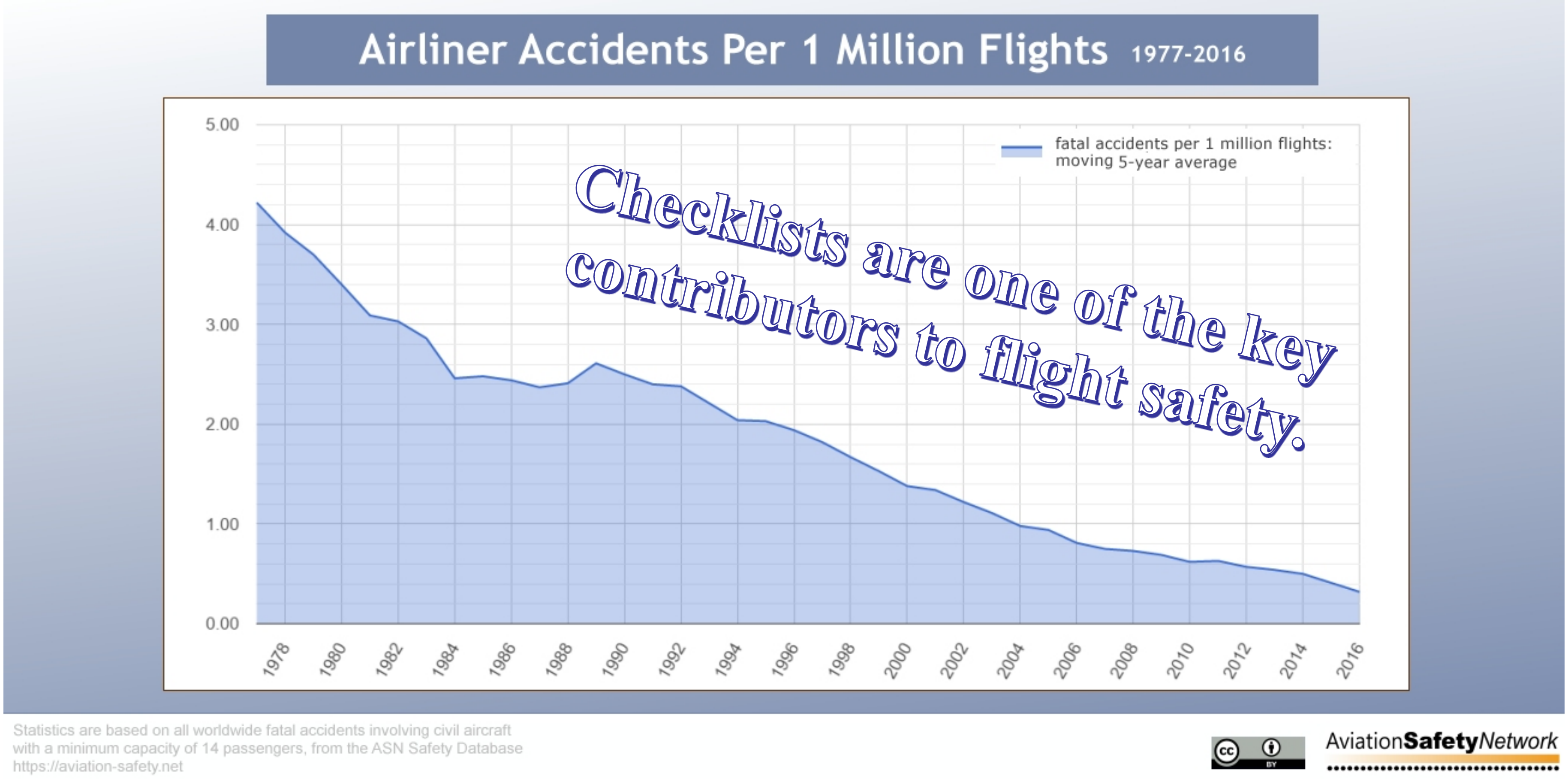
Examples of Risk

Risk of an accident while driving in a car or flying in an airplane-- *Familiar, Everyday Activities!*

- ***National Highway Traffic Safety Administration* data on automobile accidents for 2015**
  - 32,166 fatal motor vehicle accidents with just over 35,000 deaths, or
  - 1.13 fatalities per 100 million vehicle miles traveled, or
  - nearly 11 fatalities for every 100,000 U.S. residents
- ***National Transportation Safety Board* data on U.S. airline accidents for 2015**
  - 27 total accidents—**zero of which was fatal**
  - 0.155 accidents for every 100,000 flight hours
  - 0.0035 airline accidents per one million miles flown
- **According to the *National Safety Council,* Americans have a 1 in 114 chance of dying in a car crash**
- **The odds of dying in air and space transport incidents, which include private flights and air taxis, are 1 in 9,821. *That's almost three times better chance than dying by choking on food.***

Source: https://fortune.com/2017/07/20/are-airplanes-safer-than-cars/amp/

Safety of Flight is No Accident!


Airliner Accidents Per 1 Million Flights 1977-2016

Checklists are one of the key contributors to flight safety.

Statistics are based on all worldwide fatal accidents involving civil aircraft with a minimum capacity of 14 passengers, from the ASN Safety Database https://aviation-safety.net

“2016 was the seventh straight year that nobody died in a crash on a US-certificated scheduled airline operating anywhere in the world.”

Source: https://www.forbes.com/sites/danielreed/2016/12/28/in-the-last-7-years-you-were-more-likely-to-be-run-over-by-a-car-than-to-die-in-an-airline-crash/4/#dfec7d96bd15

We Can Take Actions to Successfully Reduce Risk

Birth of Checklists

- October 30, 1935, Wright Air Field, Dayton, Ohio
- US Army Air Corps flight competition for long-range bomber
- Boeing Model 299 (dubbed “flying fortress”) was supposed to trounce Martin and Douglas designs
- Climbed to 300 ft., stalled, rolled, and crashed
- Two of the five crew died, including the pilot, Maj. Hill
- Crash due to “pilot error,” no mechanical problems
- *“Too much of an airplane for one man to fly”*
- Douglas declared winner; Boeing almost went bankrupt
- Checklist born out of the ashes!
- Test pilots devised a solution: *Not more training but index card checklist*
    - *Simple, brief, and to the point*
    - *Flying this new airplane was too complicated to be left to the memory of any one person, however expert*
- Pilots subsequently flew Model 299 for 1.8 million miles without one accident
- Army ordered almost 13,000 aircraft known as **B-17**—*gave US decisive advantage in WW II*

Checklists Rule!

Risk Associated with Hospital Care

Another Familiar, Everyday Event

"Between 210,000 and 440,000 patients each year who go to the hospital for care suffer some type of *preventable* harm that contributes to their death!"

John T. James

Journal of Patient Safety, Vol. 9, No. 3, Sept. 2013

"…medical errors are third-leading cause of death in America, behind heart disease…and cancer…"

Marshall Allen

ProPublica, Sept. 2013

A Shocking Statistic:

More than One 300-Passenger Airliner Fatal Crash Every Day of the Year! 😳

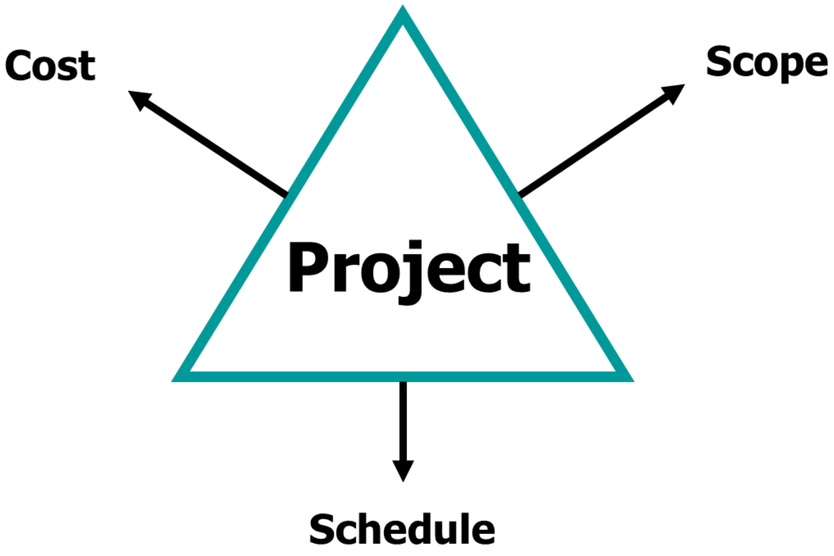
"Checklists can be enormously helpful!"

See Chapter 2, "The Checklist Manifesto" by Dr. Atul Gawande

Risk is an Integral Part of All Projects

- **A project is a set of tasks that relate to each other, and together define the <u>Scope</u> of the project**
  - Each task has a <u>Start</u> and <u>Finish</u>
  - Tasks consume <u>Resources</u> *(Time, Effort, Material)*

The "Iron Triangle"



- **All projects have <u>Cost</u> and <u>Schedule</u> targets**

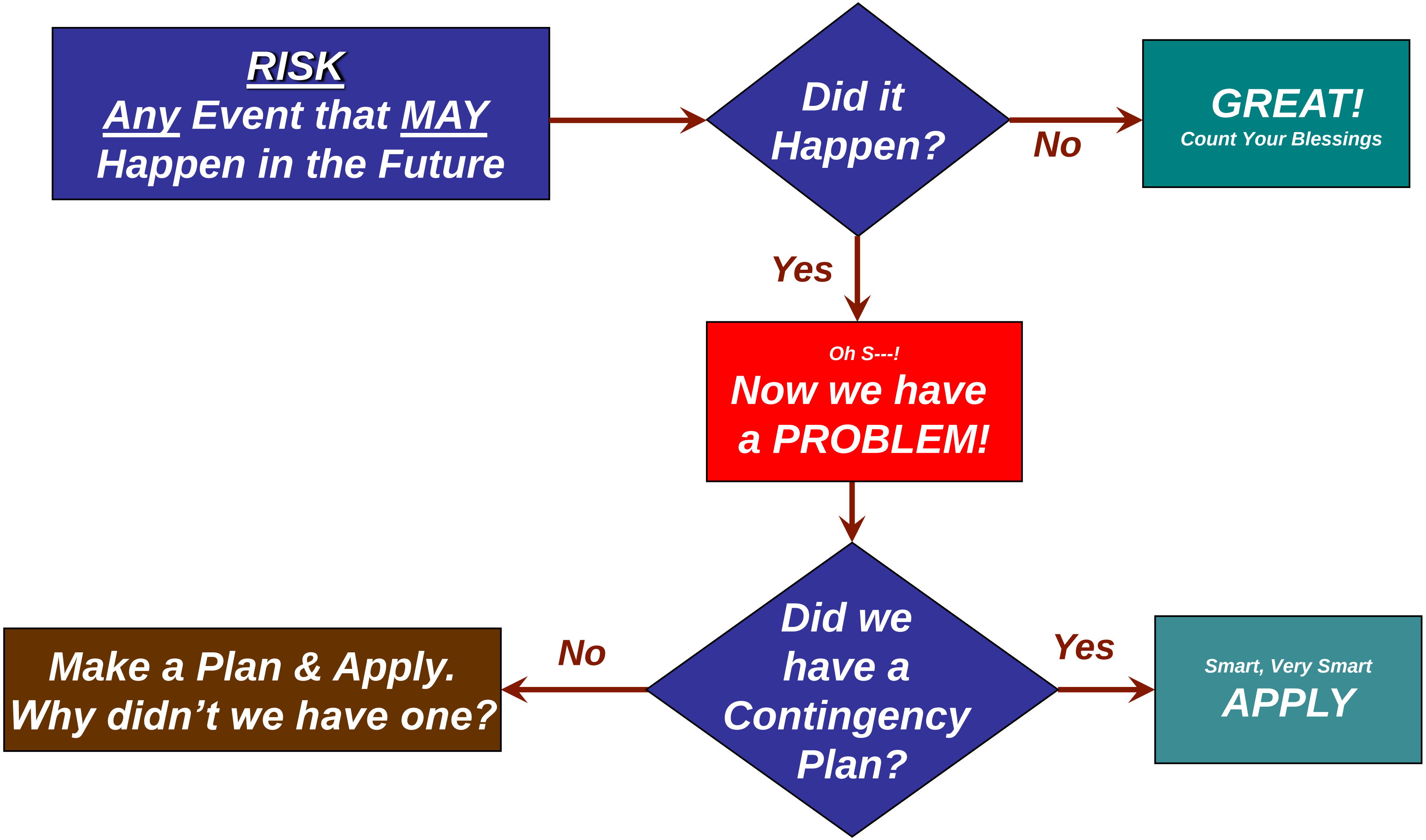
<u>All three cannot be constrained without incurring substantial risk</u>

- **Purpose of the Project is to (*or attempt to*) achieve a set of <u>Objectives</u>**

Confusion Over Risk is the Worst Risk for a Project!

Source: Adapted from AOE-3564 lectures by Dr. Bryan Moser, MIT

Risk and Its Relationship to Your Project



RISK
Any Event that MAY Happen in the Future

Did it Happen?

GREAT!
Count Your Blessings

Oh S---!
Now we have a PROBLEM!

Did we have a Contingency Plan?

Make a Plan & Apply.
Why didn't we have one?

Smart, Very Smart
APPLY

"We don't deal with risk until it's absolutely certain!"

Risk is Inherent in All Design Efforts

"…Understanding failure plays a key role in error-free design of all kinds."

"…Indeed, all successful design is the proper and complete anticipation of what can go wrong."

Henry Petroski

Aleksandar S. Vesic Professor of Civil Engineering
Duke University

Understanding and Managing Project Risks is What Separates Successful Teams from the Rest!

Source: Image from Wikipedia; Internet

Outline

P5. Project Risk Management

P5.1 Understanding Risk

P5.2 Sources of Risk

P5.3 Risk Management

Appendix A: Basics of Fault Tree Analysis

The Main Source of Project Risk: *Uncertainty*

- **Risk comes from uncertainty in the processes used to execute the project**
- **Potential sources of uncertainty include:**
    - Uncertainty in performance, safety, cost, and schedule models
    - Uncertainty/changes in customer requirements
    - Uncertainty in integration effects on performance
    - Uncertainty in manufacturing variation/tolerances
    - Uncertainty in test results
    - Uncertainty in operating environment (temperature, pressure, etc.)
    - Uncertainty in response to operating environment/ failure modes
    - Uncertainty in reliability of components or subsystems or system
    - Human errors in design, development, production or operation

No Uncertainty…No Risk!
Reduce Uncertainty…Reduce Risk!

Risk Event (Uncertainty) Drivers

Generic Drivers

- Complexity exceeds experience
- Unknown or unclear requirements
- Unstable or changing requirements
- Performance criteria or failure mechanisms cannot be measured
- Availability and/or capability of key resources
- Safety

Flavors of Uncertainty

- **Variation:** small changes in project paths compound to cause variation in cost and schedule; may be compensated through buffers at key locations in project plan (e.g., see Goldratt's Critical Chain)
- **Foreseen Uncertainty:** compensation through contingency plans
- **Unforeseen Uncertainty:** project teams must flexibly build responsive contingency plans throughout the project's duration
- **Chaos:** continuous re-planning required based on incremental learning; medium-to-long-term contingencies cannot be planned

Source: Adapted from AOE-3564 Lectures by Dr. Bill Grossmann

Impact of Drag Prediction Uncertainty

C-141 Cruise Drag (early 1960s)

- **Predicted drag based on wind-tunnel tests within *One Count of flight data…***

  …but good agreement fortuitous!
  - Minimum Profile Drag: *Underpredicted*
  - Compressibility Drag: *Overpredicted*

- **DoD Aeronautical Test Facilities Assessment Team (1997)**
  - *Question*: **Can we do better with improved wind-tunnel test techniques combined with CFD?**
  - *Answer*: **Cruise drag would be Underpredicted by 3.5%**
    - *Considering only Reynolds Number Scaling*
      - *Minimum Profile Drag Underprediction—about Eight counts*
      - *Compressibility Drag Overprediction—eliminated*

Erroneous Predictions would Increase Fuel Cost by $688M (FY96 dollars) for Entire Fleet over Service Life

Impact of Drag Prediction Uncertainty

C-5 Cruise Drag (mid 1960s)

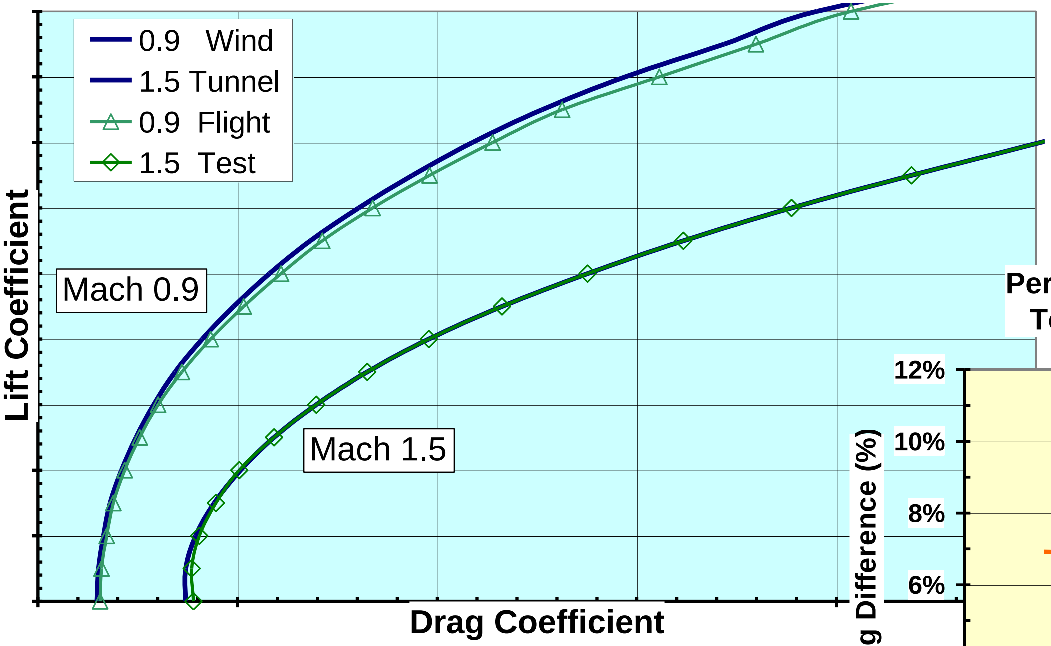
- **Total drag overpredicted by 2.5% based on wind-tunnel tests**
  - Minimum Profile Drag*: Underpredicted by one scale-up method and correctly predicted by another*
  - Compressibility Drag*: Overpredicted*

- **DoD Aeronautical Test Facilities Assessment Team (1997)**
  - *Question*: **Can we do better with improved wind-tunnel test techniques combined with CFD?**
  - *Answer:* **Cruise drag would be Underpredicted by 1.5%**
    - *Considering only Reynolds Number Scaling*
      - Minimum Profile Drag Underprediction—*1% to 3%*
      - Compressibility Drag Overprediction—*eliminated*

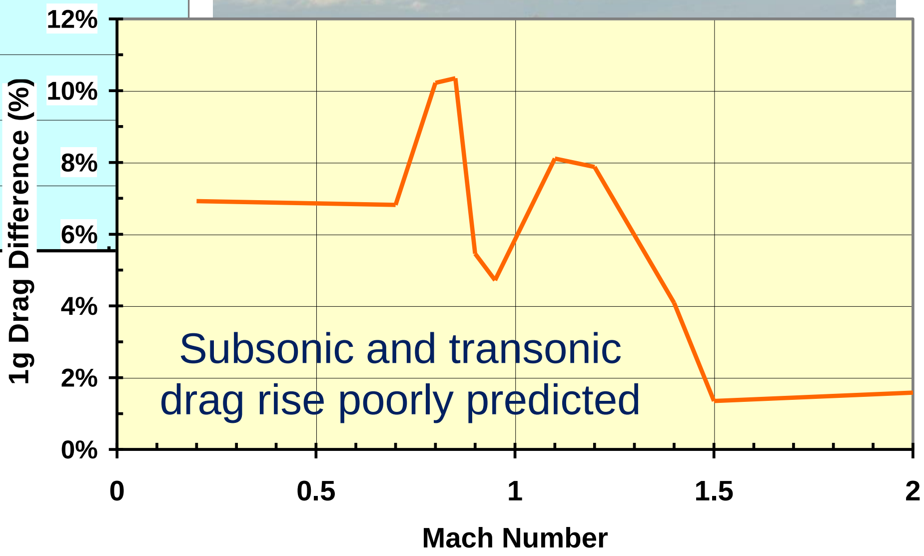
Erroneous Predictions Would Increase Fuel Cost by $153M (FY96 dollars) for Entire Fleet over Service Life!

Impact of Drag Prediction Uncertainty

F-22 Cruise Drag (1990s)



Percent Drag Difference between Preliminary Flight Test Results and Wind Tunnel Predictions at 1G



Subsonic and transonic drag rise poorly predicted

- **Drag predicted using wind-tunnel test matched well with flight test data for Mach 0.9 and 1.5**

Differences between predicted and flight test data may be due to a combination of interpolated pieces

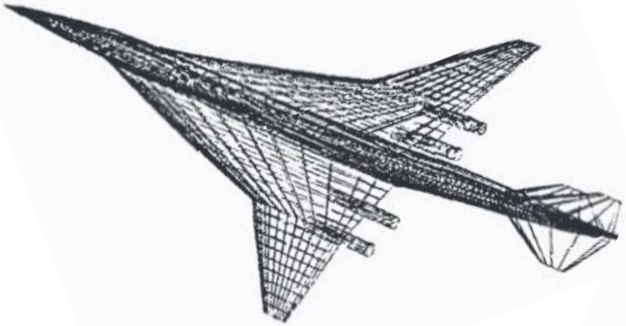
Thrust effects, auxiliary inlet and vents, control surface scheduling, etc.

Impacts accelerations, decelerations, cruise and loiter performance

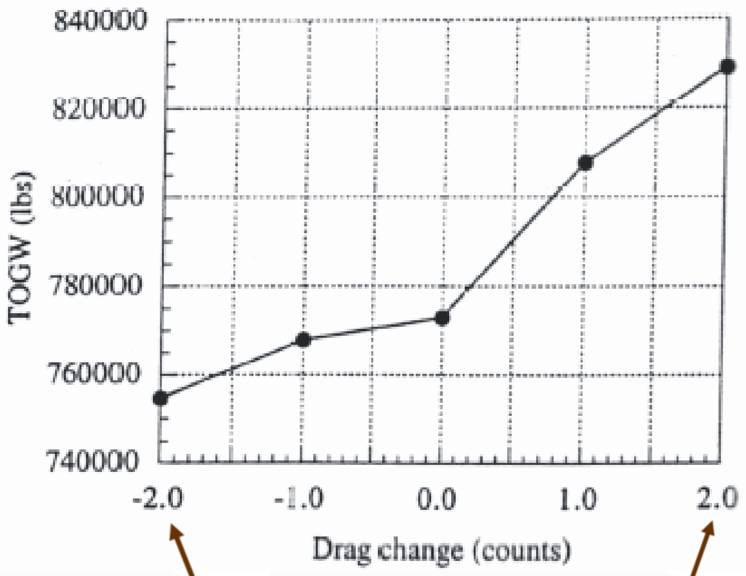
Impact of Drag Prediction Uncertainty

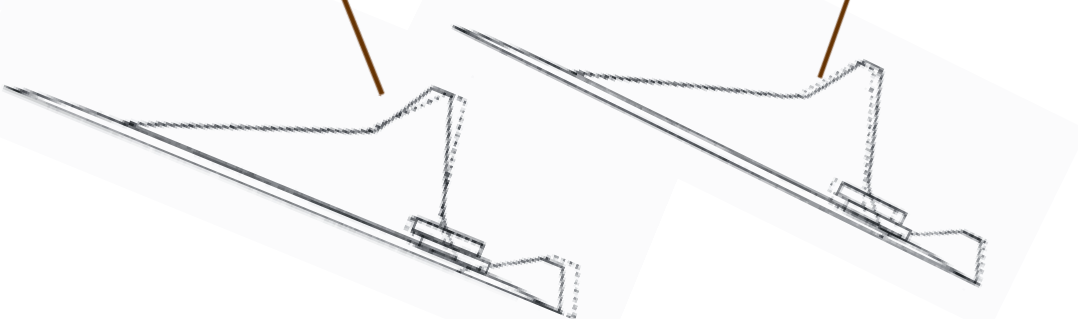
HSCT Conceptual Design MDO Study (mid 1990s)

- **High Speed Civil Transport**
  - *Cruise Mach Number: 2.4*
  - *Range: 5,500 nm*
  - *Payload: 250 passengers*



  - TOGW = 772,907 lbs.
  - Fuel Weight Fraction = 0.52
  - Empty Weight Fraction = 0.39
  - Aspect Ratio = 2
  - L/D$_{max}$ = 9.16





TOGW = 754,560 lbs.

TOGW = 829,100 lbs.

Just Two-count Cruise Drag Overprediction Increases Take-Off Gross Weight by More Than 7%!

C-130J Development: *Risk Example*

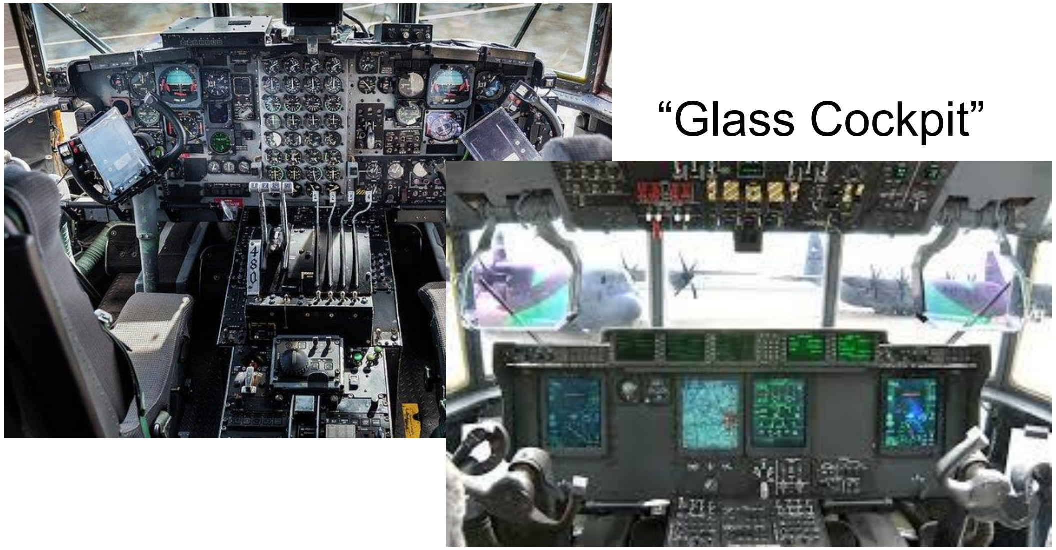
Background

- **April 10, 1951:** Lockheed submits proposal to USAF in response to a tactical airlifter RFP
- **July 2, 1951:** Lockheed declared winner, and contract awarded for two YC-130 prototypes
- **Sep 19, 1952:** Letter contract awarded for seven production aircraft!
- **Aug 23, 1954:** First flight from Burbank to Edwards AFB
- **Apr 7, 1955:** First flight of C-130A
- **1956:** Entry in service with USAF followed by Australia and many other nations
- **1956 – 1990:**
  - Multiple variants of cargo airlifter
  - C-130A (231); C-130B (230); C-130E (491); C-130H (1086)
  - L-100 commercial variant (116)

C-130J Development: *Risk Example*

- **1988:** Lockheed began defining initial baseline C-130J following a meeting with senior staff of USAF Military Airlift Command, MAC *(now Air Mobility Command)*
- **1989:** USAF MAC published Mission Needs Statement for “Enhanced Theater Airlifter”
- **Late 1990:** USAF decided to *<u>not</u>* fund C-130J development and procure C-130Hs instead. No C-130 procurement after FY 93! But, UK RAF very interested
- **Late 1991:** Lockheed decides to pursue development as private venture
- **Two Principal Technology Enablers**

1. Digital Avionics



“Glass Cockpit”

2. Propulsion

AE-2100 D3 engine

Dowty six-bladed R391 propeller

30% more static thrust

C-130J Development: *Risk Management*

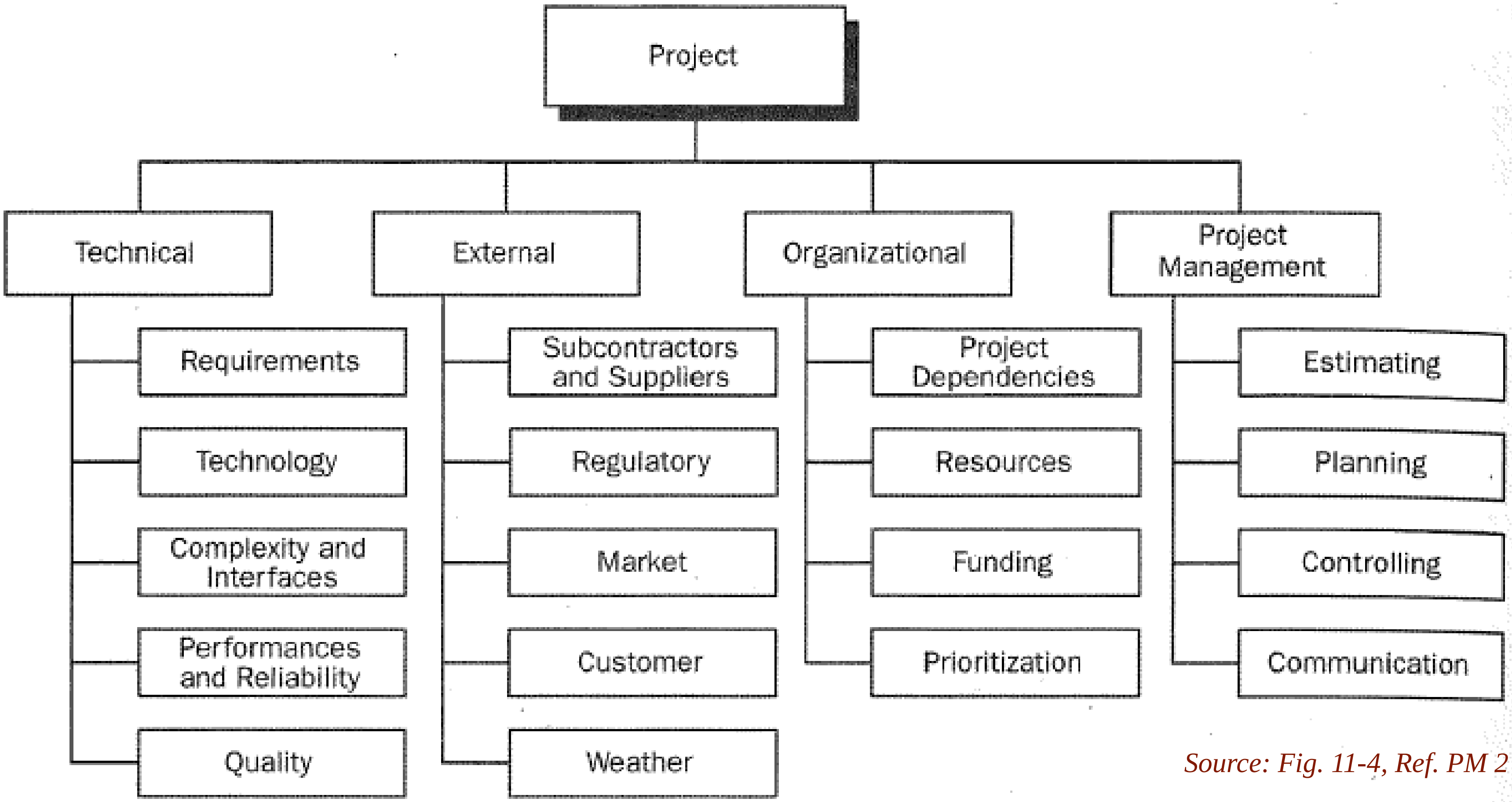
- **Dec 1994:** Program launched with UK RAF contract award
  - *25 aircraft: 10 standard C-130J and 15 longer C-130J-30*
- **April 5, 1996:** First flight
- **Oct 1996:** USAF Five-Year Option Contract (FYOC) I
  - FY96-FY01: 35 aircraft; $2.3B
- **May 1997:** ***"…delay of at least 12 months in the delivery of the first C-130Js."***
  - Software: *"The good news about software is that it's easy to change; the bad news is that it's easy to change."* Airplane functionality made *"better"* with only *"software change"*! New software qualification testing both time consuming and costly.
  - Stall Roll-off: Aerodynamic interaction of new propeller and inner wing caused outer wing to stall first leading to loss of roll control. Aerodynamic fixes (boundary-layer trippers, fences, vortex generators, etc.) did not work. Problem solved by installing stick pusher and optional stick shaker. But…***Significant cost impact [due to delays] when the risk occurred***
- **Aug 24, 1998:** Aircraft delivered to UK RAF

  "*We know we are late and that we have caused problems for our customer.*" – Program Manager
- **Jan 1999:** 1st aircraft delivered to USAF; 400+ delivered since with orders for more!

C-130 Remains Longest Continuously Produced Aircraft for 65 years and counting!

Project Risk Categories:

A Notional Risk Breakdown Structure (RBS)

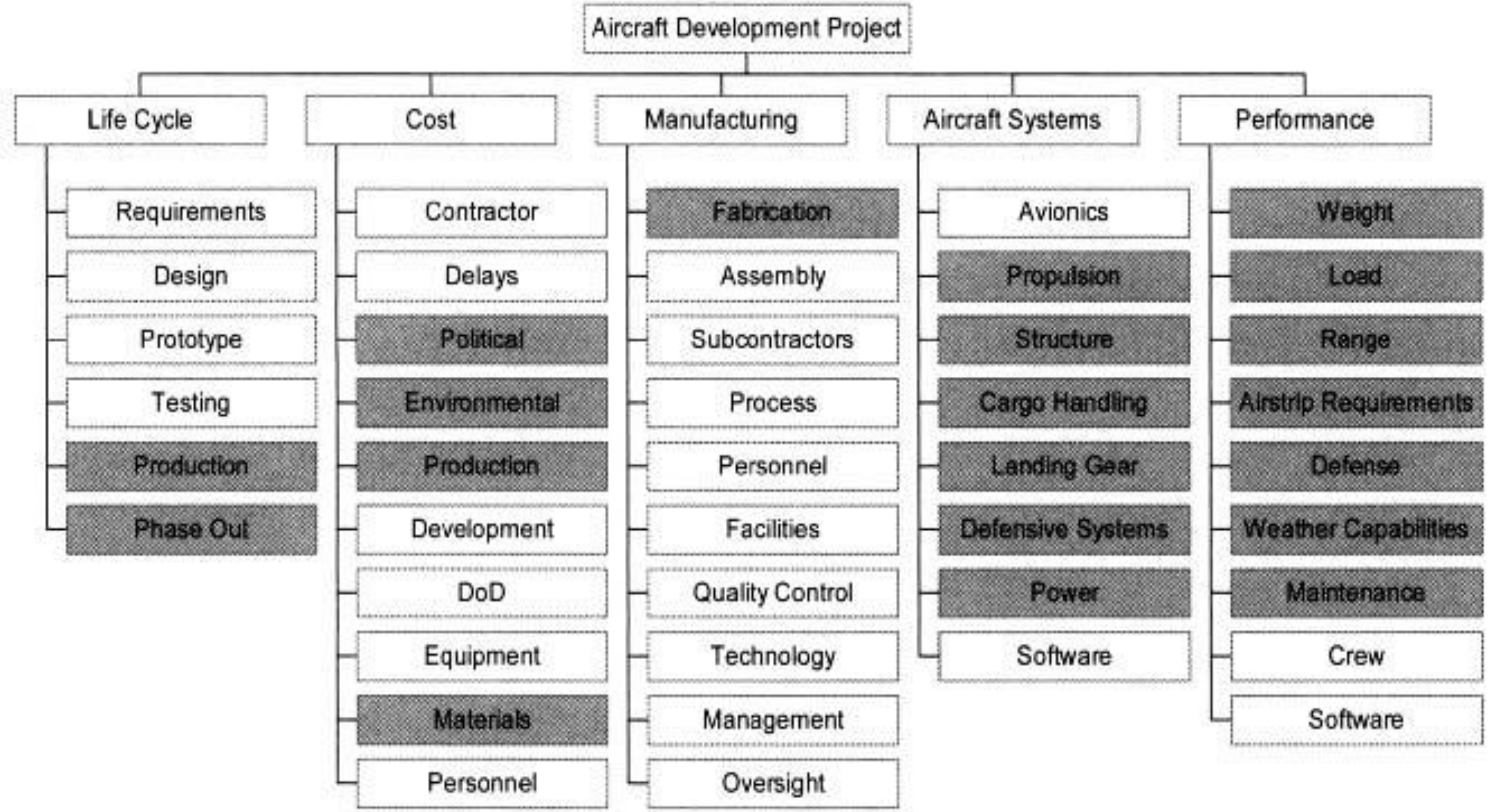


Source: Fig. 11-4, Ref. PM 2

"In today's large sociotechnological systems, there are at least four major categories: (1) Hardware Failure; (2) Software Failure; (3) Human Failure; and (4) Organizational Failure. All are highly interactive and complex."

Source: Ref. PM 3

Aircraft Development Project:
An Example of Risk Breakdown



- Aircraft Development Project
  - Life Cycle
    - Requirements
    - Design
    - Prototype
    - Testing
    - Production
    - Phase Out
  - Cost
    - Contractor
    - Delays
    - Political
    - Environmental
    - Production
    - Development
    - DoD
    - Equipment
    - Materials
    - Personnel
  - Manufacturing
    - Fabrication
    - Assembly
    - Subcontractors
    - Process
    - Personnel
    - Facilities
    - Quality Control
    - Technology
    - Management
    - Oversight
  - Aircraft Systems
    - Avionics
    - Propulsion
    - Structure
    - Cargo Handling
    - Landing Gear
    - Defensive Systems
    - Power
    - Software
  - Performance
    - Weight
    - Load
    - Range
    - Airstrip Requirements
    - Defense
    - Weather Capabilities
    - Maintenance
    - Crew
    - Software

- **Risks identified using Hierarchical Holographic Modeling (HHM)**
- **Critical risks determined by filtering using Risk Filtering, Ranking, and Management (RFRM) methodology**

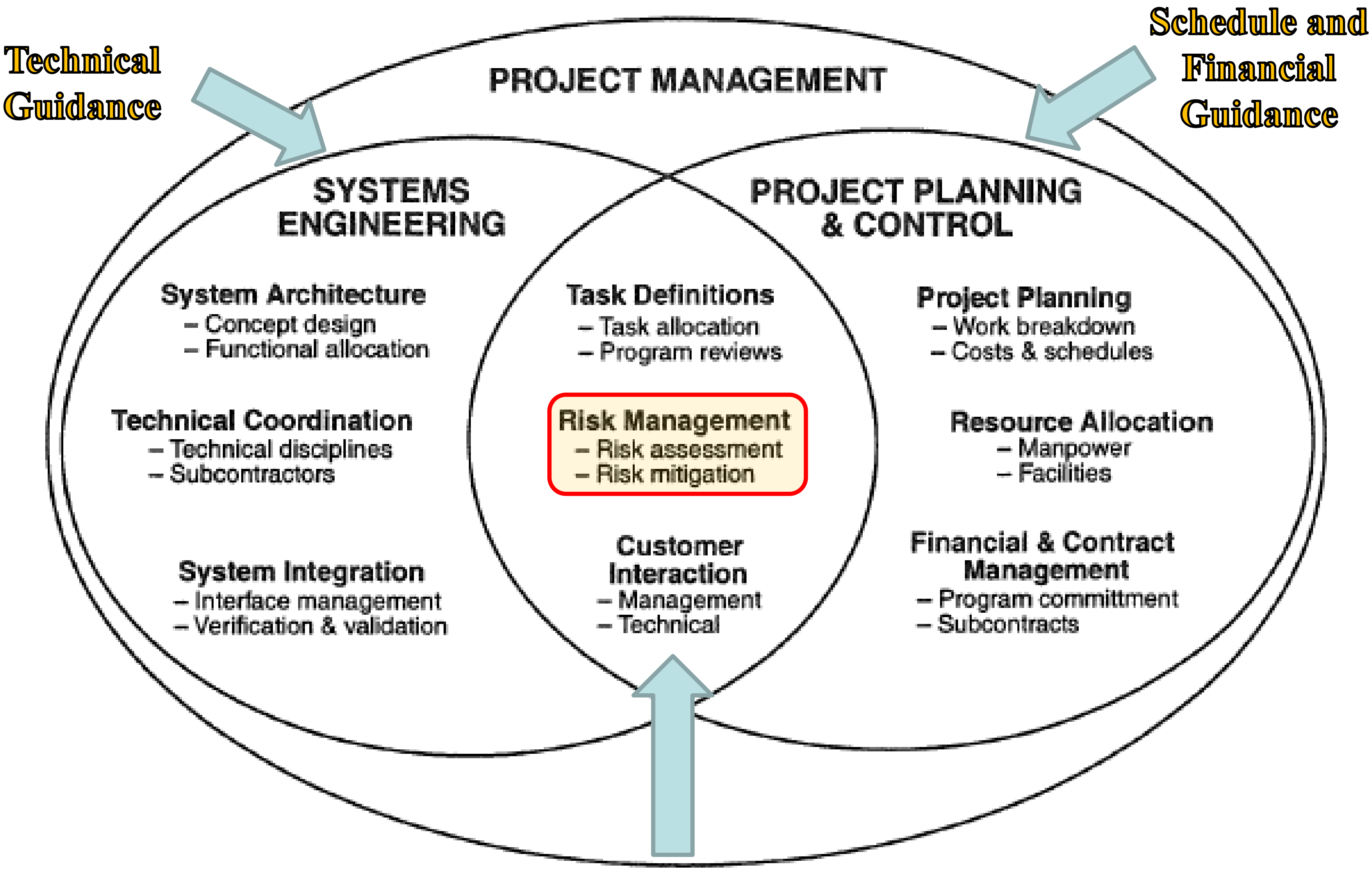
Source: Ref. PM 3

Outline

P5. Project Risk Management

Risk Management

A Critical Element of Project Management (PM)



Technical Guidance

Schedule and Financial Guidance

PROJECT MANAGEMENT

SYSTEMS ENGINEERING

PROJECT PLANNING & CONTROL

System Architecture
- Concept design
- Functional allocation

Technical Coordination
- Technical disciplines
- Subcontractors

System Integration
- Interface management
- Verification & validation

Task Definitions
- Task allocation
- Program reviews

Risk Management
- Risk assessment
- Risk mitigation

Customer Interaction
- Management
- Technical

Project Planning
- Work breakdown
- Costs & schedules

Resource Allocation
- Manpower
- Facilities

Financial & Contract Management
- Program committment
- Subcontracts

Shared Functions

Source: Fig. 4-1, Ref. SE 2 (Kossiakoff and Sweet)

Risk Management: *A Brief History*

- **1987**: The **Project Management Institute (PMI)** included Risk Management in an initial Body of Knowledge (PMBOK). PMP certification and PMBOK in 1996 describe the identification, analysis, response and ongoing control of risks.
- **In the early 1990s**, **Carnegie Mellon University's (CMU) Software Enterprise Institute (SEI)** established Continuous Risk Management, in **1996 a Guidebook.** Later into a capability maturity model (CMMI-DEV).
- **NASA** adopted the SEI Continuous Risk Management approach and evolved it for human spaceflight.
- **1994**: The International Council on **Systems Engineering** (INCOSE) Handbook (1994, 2nd Version in 2002) closely aligned with DOD practices. 3rd Version, 2006 and updated 2011, calls out a **Risk Management Process (RMP**).
- In **2009**, a PMI certification called **Risk Management Professional (PMI-RMP**). Includes a broad range of tools:
  - qualitative and quantitative analysis, decision trees, cumulative probability diagrams, sensitivity analysis, and simulation.
- **Software Development**: Large uncertainty in software projects. Risk reduced through action in prototyping. Yet without early estimates and commitments, decisions made with weak awareness of downstream and propagating effects.

Source: Adapted from AOE-3564 Lectures by Dr. Bryan Moser, MIT

A Risk Management Framework

Anticipate what can go wrong?

Control deviations

Decide what is important

Track actions

Plan to take action

Source: Adapted from AOE-3564 Lectures by Dr. Bryan Moser, MIT

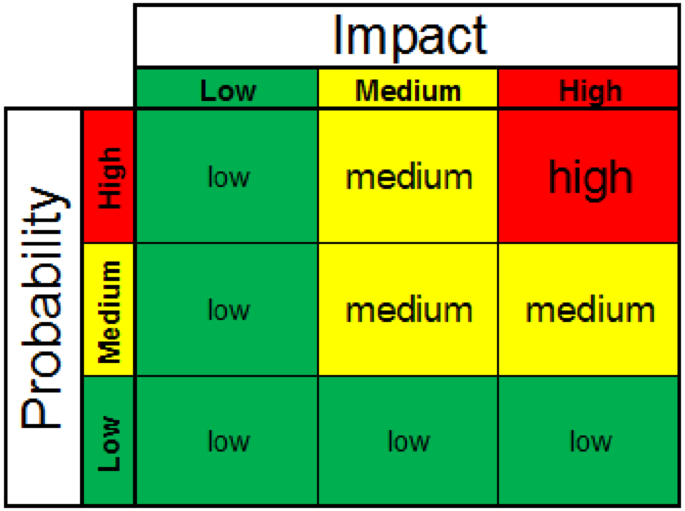
How Do You Identify Risks?

- ***Anticipate what can go wrong: "Just about everything!"***
- **Brainstorm for Potential Problems or Uncertainties, e.g.,**
  - ***Task Duration***
    - Fabrication delays; testing delays; computing delays; …
  - ***Required Resources***
    - Labor hours; model cost; equipment cost; …
  - ***Dependencies***
    - Previous test gets delayed; people not available due to schedule conflicts; tardy vendors; delays in placing procurement orders; …
  - ***Constraints***
    - Funding; finding substitutes for sick, vacationing or otherwise occupied teammates; …
  - ***Dealing with "messy" Problems…***
- **Be Aware of Gaps in Information or Data (aka Unknowns)**
  - ***Insufficient data for project planning***
  - ***Continuously refine plan as more data/ info come in***

Look for Ways You Can Fail to Execute Your Plan!

How Do You Assess Risk?

- **Assessment answers the question: *Which risks are more important?***
- **Analyze Impact *(Consequences – Co)***
  - What will be the consequence of the event on my project?
    - *High (> 0.8) An Unacceptable Outcome*
    - *Medium (0.4 - 0.7) Adverse Impact on Cost, Schedule, Deliverables*
    - *Low (< 0.3) Small Adverse Effects on Project Objectives*
- **Analyze Probability *(Likelihood of occurrence – Lo)***
  - How likely is it that the event will occur?
    - *High (> 0.8)*
    - *Medium (0.4 - 0.7)*
    - *Low (< 0.3)*
- **Prioritize Risks**
  - Organize risks in order of priority
  - *Use your best judgment, not just numerical scores!*



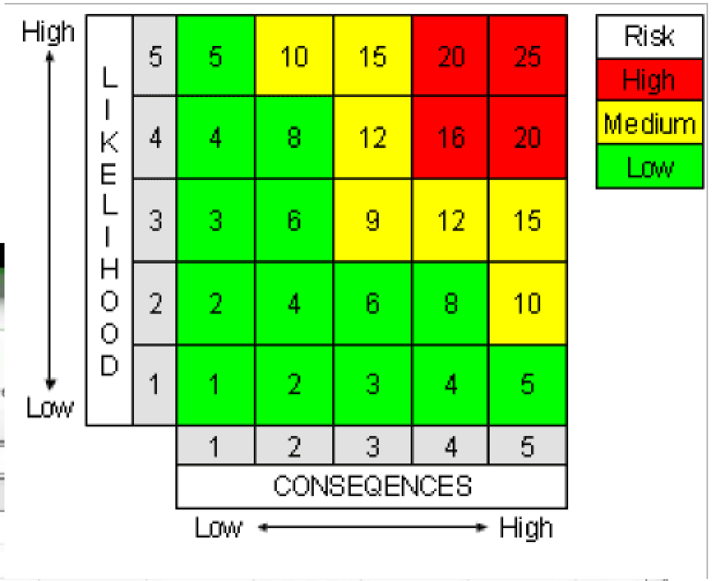
		Impact		
		Low	**Medium**	**High**
Probability	**High**	low	medium	high
	Medium	low	medium	medium
	Low	low	low	low

Overall Risk = Probability x Impact

Luck Favors a Prepared Team!

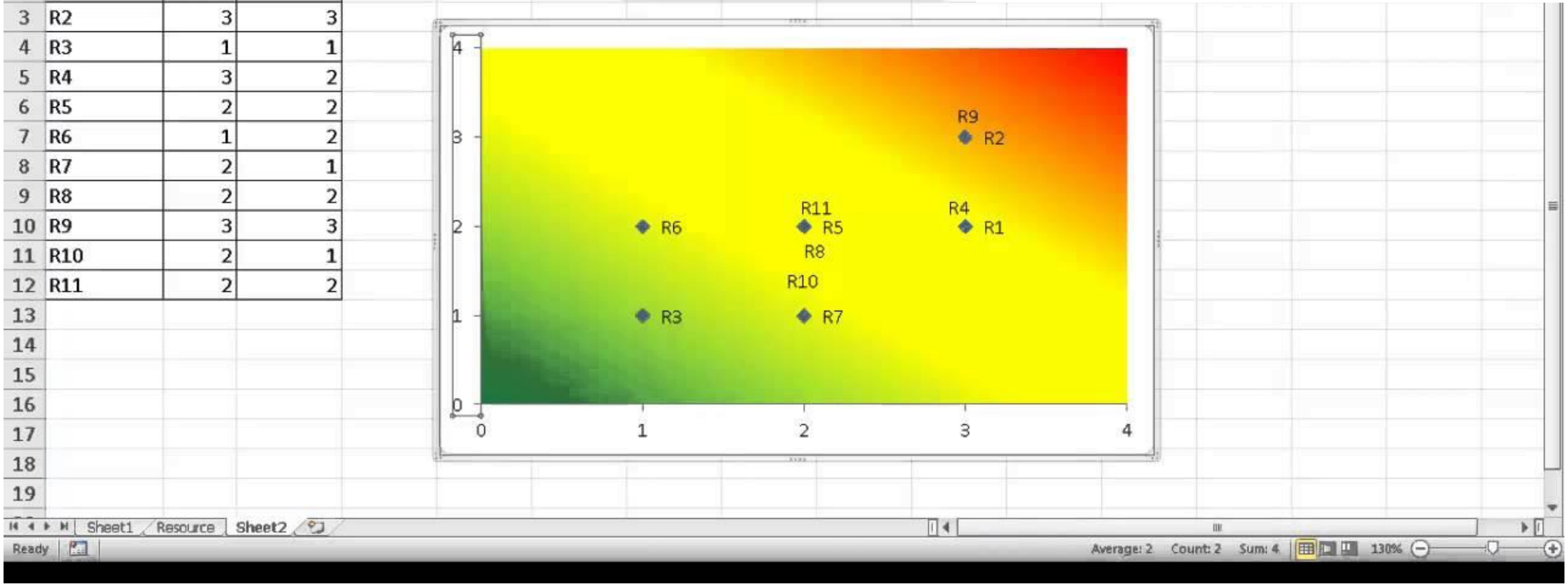
Sample Risk Assessment Matrix

Use Risk Assessment Matrix to Decide what is important before making a plan to take action



LIKELIHOOD					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	CONSEQENCES				

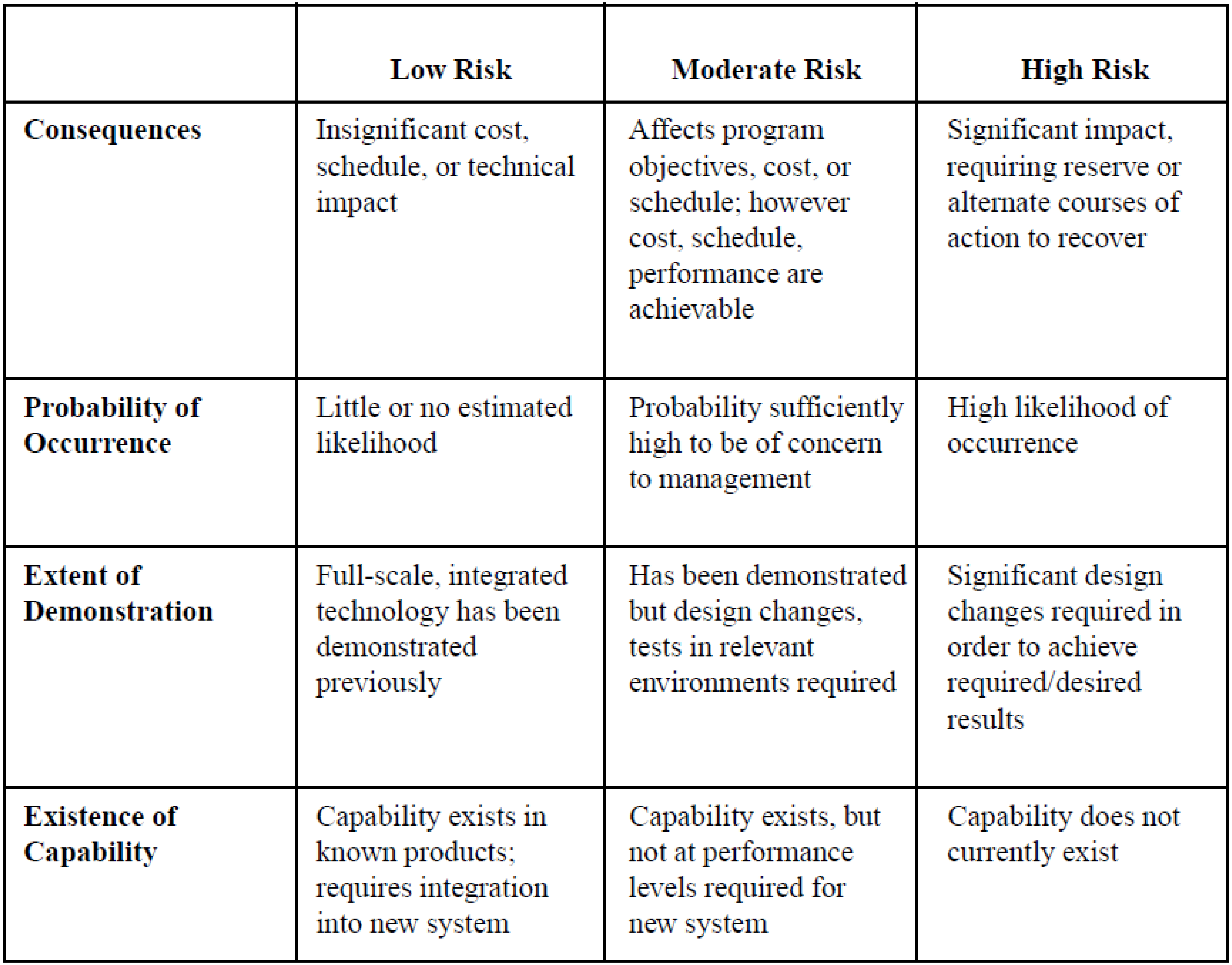
Risk
High
Medium
Low



	A	B	C
1	Risk Factors	Impact	Probabilty
2	R1	3	2
3	R2	3	3
4	R3	1	1
5	R4	3	2
6	R5	2	2
7	R6	1	2
8	R7	2	1
9	R8	2	2
10	R9	3	3
11	R10	2	1
12	R11	2	2

Source: Internet

Model for System Level Risk Assessment



	Low Risk	Moderate Risk	High Risk
Consequences	Insignificant cost, schedule, or technical impact	Affects program objectives, cost, or schedule; however cost, schedule, performance are achievable	Significant impact, requiring reserve or alternate courses of action to recover
Probability of Occurrence	Little or no estimated likelihood	Probability sufficiently high to be of concern to management	High likelihood of occurrence
Extent of Demonstration	Full-scale, integrated technology has been demonstrated previously	Has been demonstrated but design changes, tests in relevant environments required	Significant design changes required in order to achieve required/desired results
Existence of Capability	Capability exists in known products; requires integration into new system	Capability exists, but not at performance levels required for new system	Capability does not currently exist

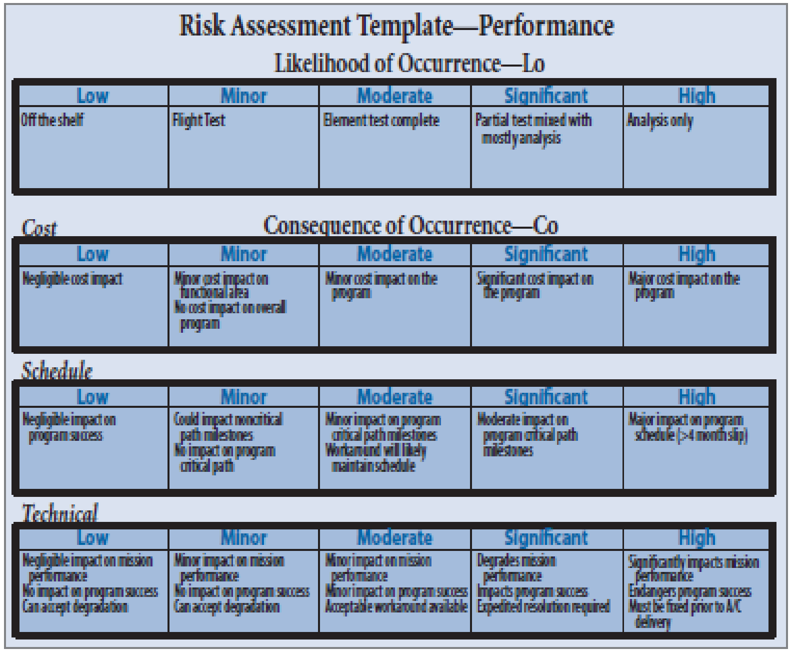
Source: Ref. SE 5 (DoD)

How Do You Address Risk?

- **Accept it**
  - *Not Addressing Risk is the Same as Accepting it!*
    - ○ Some mitigations might “not be worth it.”
    - ○ Sometimes this is the only option—Don’t Get Too Wrapped Up
    - ○ But…Do it knowingly and have a contingency plan
- **Mitigate it**
  - Mitigation seeks to reduce the exposure of identified risks
  - Each mitigation option might affect project performance differently
  - A planned mitigation does not necessarily become actual mitigation
  - Do something “Extra” to reduce the Probability or Impact or both
    - ○ Must weigh cost of mitigation against benefits before embarking on a corrective action
    - ○ Track actions and control deviations
- **Revisit List of Risks Monthly—Update As Needed**

If Things Are Going Better Than You Planned,
You Have Overlooked Something!

Risk Assessment and Mitigation



Risk Assessment Template—Performance

Likelihood of Occurrence—Lo

Low	Minor	Moderate	Significant	High
Off the shelf	Flight Test	Element test complete	Partial test mixed with mostly analysis	Analysis only

Consequence of Occurrence—Co

Cost

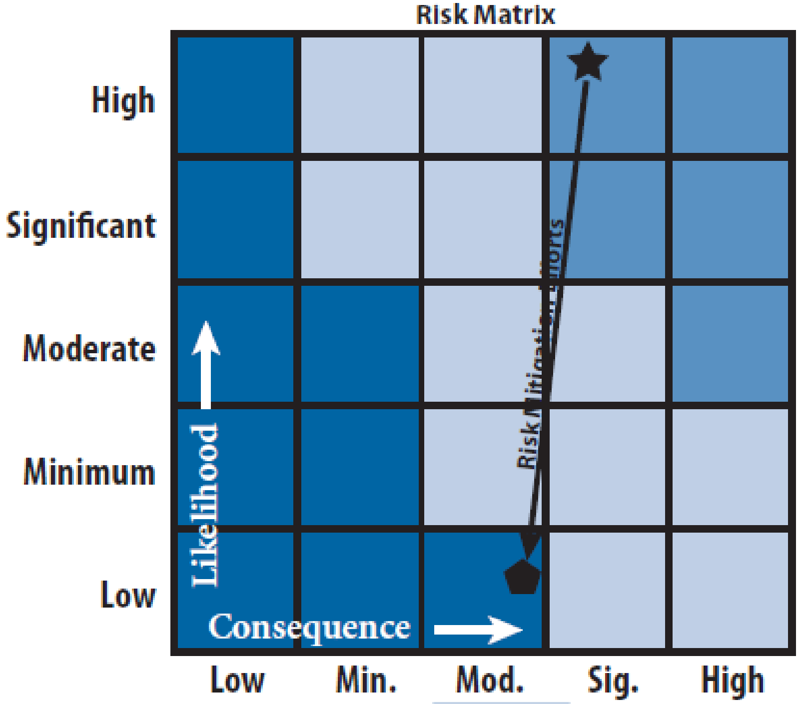
Low	Minor	Moderate	Significant	High
Negligible cost impact	Minor cost impact on functional area No cost impact on overall program	Minor cost impact on the program	Significant cost impact on the program	Major cost impact on the program

Schedule

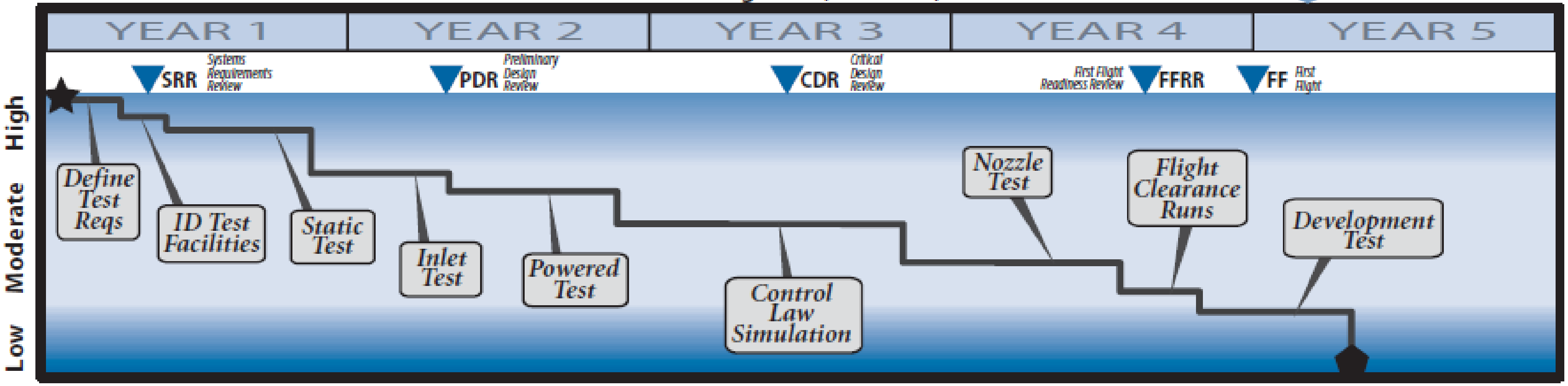
Low	Minor	Moderate	Significant	High
Negligible impact on program success	Could impact noncritical path milestones No impact on program critical path	Minor impact on program critical path milestones Workaround will likely maintain schedule	Moderate impact on program critical path milestones	Major impact on program schedule (>4 month slip)

Technical

Low	Minor	Moderate	Significant	High
Negligible impact on mission performance No impact on program success Can accept degradation	Minor impact on mission performance No impact on program success Can accept degradation	Minor impact on mission performance Minor impact on program success Acceptable workaround available	Degrades mission performance Impacts program success Expedited resolution required	Significantly impacts mission performance Endangers program success Must be fixed prior to A/C delivery



Risk Mitigation (waterfall)

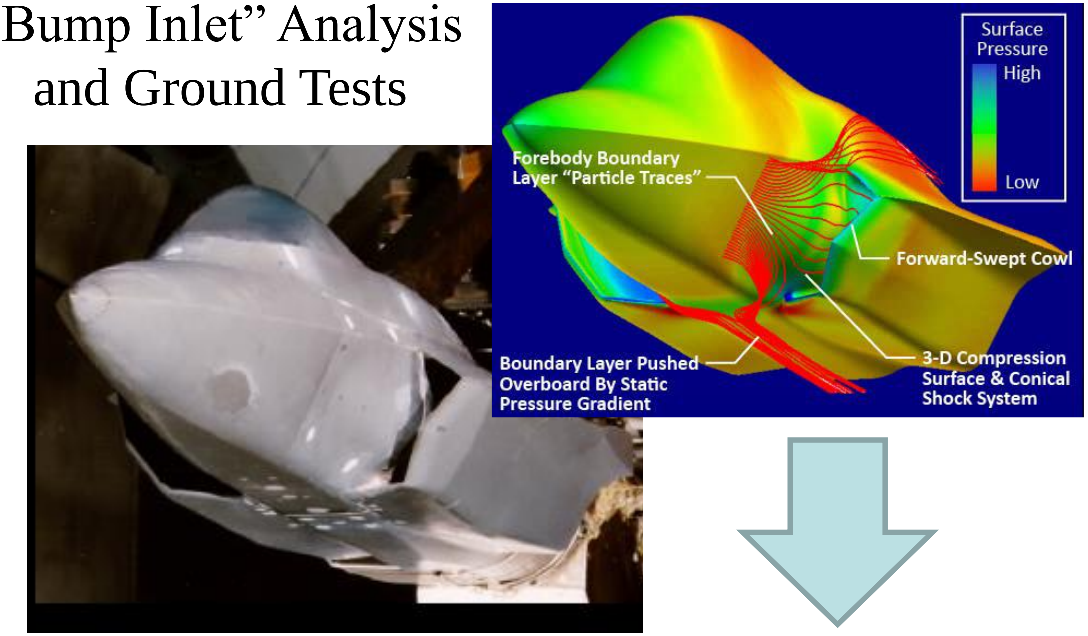


Source: Fig. 25.10, Ref. AVD 1 (Nicolai and Carichner)

Risk Management Example

Novel Technology Integration

“Bump Inlet” Analysis and Ground Tests



Flight Test Demo

Flight Test Demonstrated:
- Mach 2 in Level Flight
- F-16 Maneuver Envelope to Mach 1.6
- Excellent Engine/Inlet Compatibility
- No Engine Stalls or Anomalies

Integrated System

Source: Airplane images from internet

Project Risk Assessment Example
(from a VT student design project)

Event	Impact	Probability	Risk
C3 (Command, Control, and Communications) Loss	0.7	0.7	0.49
Ground Delays- Refueling or Repair	0.6	0.8	0.48
Propulsion Failure	0.9	0.4	0.36
Structural Failure	0.9	0.4	0.36
Inclement Weather at Landing Site	0.5	0.7	0.35
Payload Instrumentation Failure	0.4	0.6	0.24
Climate Impacts (i.e. wing icing)	0.3	0.8	0.24
Payload Power Failure	0.3	0.7	0.21
Security Breach - Hacking or Hijacking	0.9	0.2	0.18
Unfavorable Wind Conditions	0.2	0.8	0.16

Project Risk Mitigation Example
(from a VT student design project)

- **C3 Loss**
  - Have a backup communications system in place, in case the primary one fails
  - In case of complete failure, have a preset flight plan available in the control system to be followed if command, control, or communications are lost with ground stations. This follows existing UAS protocols.
- **Ground Delays**
  - Anticipate delays and budget additional ground time in between flights.
- **Propulsion Failure**
  - Design the aircraft with multiple engines to allow for survivable engine out condition
  - Continental TSIOL-550-C was selected for high reliability

Risk Management
Limitations

- **Despite all that is known about managing risk, major catastrophes continue to surprise the world at an alarming rate. Why?**
- **Key insights have been obtained by adopting the view that uncertainty and risk are part of a socio-economic system**
  - After all, humans make and implement decisions about how to respond!
- **Human Impediments**
  - **Overconfidence and Cognitive Illusions of understanding and validity**: the belief that we know more about a complex system than in reality and the use of invalid assumptions about the system.
  - **Misplaced confidence in expert intuition and opinion**: Many studies show that simple, statistical formulas based on a few key variables trump the intuition of experts in predicting behavior of complex systems.
  - **Confirmation bias**: discarding of facts that do not support a favorite hypothesis. For example, human bias for optimism leads to a planning fallacy--the odds and payoff for success are inflated and realistic evaluation of risk is deflated.
  - **Hubris**: an ego trip intended to prove a point or advance a career. In a “damn-the-torpedoes, we-will-do-this” approach, risk management is replaced by a gigantic planning fallacy.

Source: Adapted from AOE-3564 Lectures by Dr. Bill Grossmann

Risk Management

Approaches to Address Limitations

- **Stimulate awareness** so that known risks are exposed and responses are more easily developed as mitigation options.
- Engineering teams are supported by **categories and checklists assembled from lessons learned**. Each project re-visits and refines, updating to dismiss conditions and effects no longer relevant, updating to reflect new conditions and environment, and to add recently discovered risks.
- These practices **leverage the embedded judgment of teams and make efficient their use**. Known-knowns quickly identified. Known-unknowns inserted to ensure consideration. Previous unknowns recently discovered brought to attention. Risks no longer relevant quickly dismissed.

Source: Adapted from AOE-3564 Lectures by Dr. Bill Grossmann

Outline

P5. Project Risk Management

P5.1 Understanding Risk

P5.2 Sources of Risk

P5.3 Risk Management

Appendix A: Basics of Fault Tree Analysis

Fault Tree Analysis (FTA):

A Tool for Risk Management

- **A FTA is conducted to produce a fault tree diagram (FTD) which is the *logical model* of the relationship of an *undesired event* to more *basic events*.**
  - **Define an *undesired event***
  - **Resolve the event into its *immediate causes***
  - **Continue this resolution of events until *basic causes* are identified**
  - **Construct a logical diagram called a *fault tree diagram (FTD)* showing the logical event relationships**

- **Highly recommended for flight demonstration projects.**

- **For more details, see**
  - Vesely, Bill, *"Fault Tree Analysis: Concepts and Applications*," NASA HQ, *http://www.hq.nasa.gov/office/codeq/risk/docs/ftacourse.pdf*
  - *"Fault Tree Analysis Handbook with Aerospace Applications,"* Ver. 1.1, NASA, August 2002

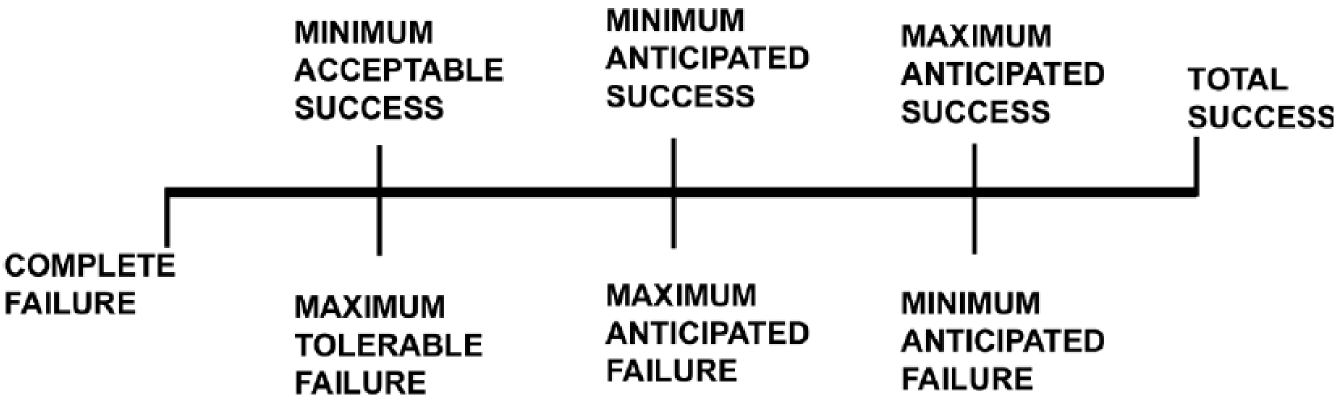
Why do FTA?

- To exhaustively identify the causes of a failure
- To identify weaknesses in a system
- To assess a proposed design for its reliability or safety
- To identify effects of human errors
- To prioritize contributors to failure
- To identify effective upgrades to a system
- To quantify the failure probability and contributors
- To optimize tests and maintenances

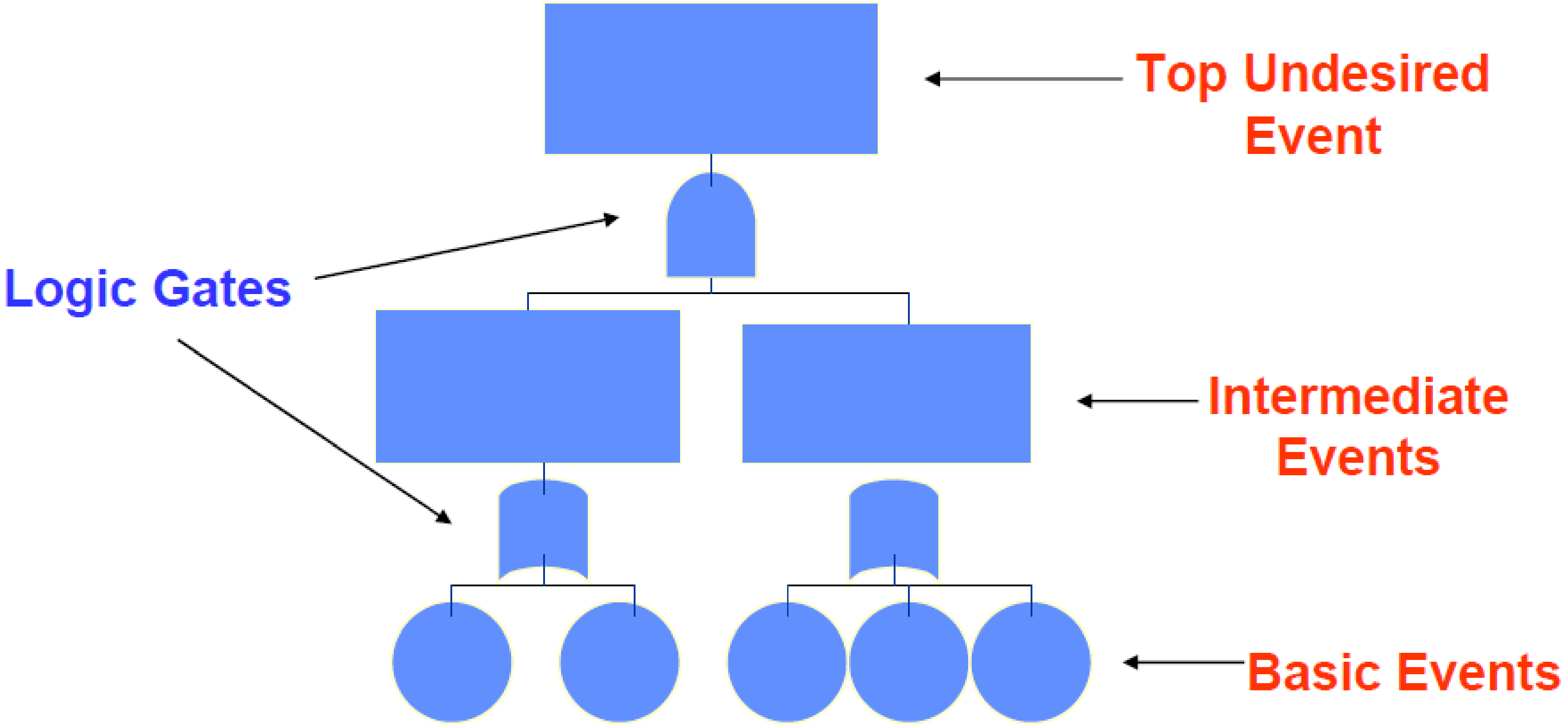
Why do FTA?

- Designers design for success
- Safety analysts analyze for failure
- There can be various degrees of success
- Thresholds for failure are identifiable
- Failure events can be more readily discretized
- Failure quantifications are simpler
- The “failure mindset” probes for weaknesses and gaps

Success space vs. Failure space



Basic Fault Tree Structure



Top Undesired Event

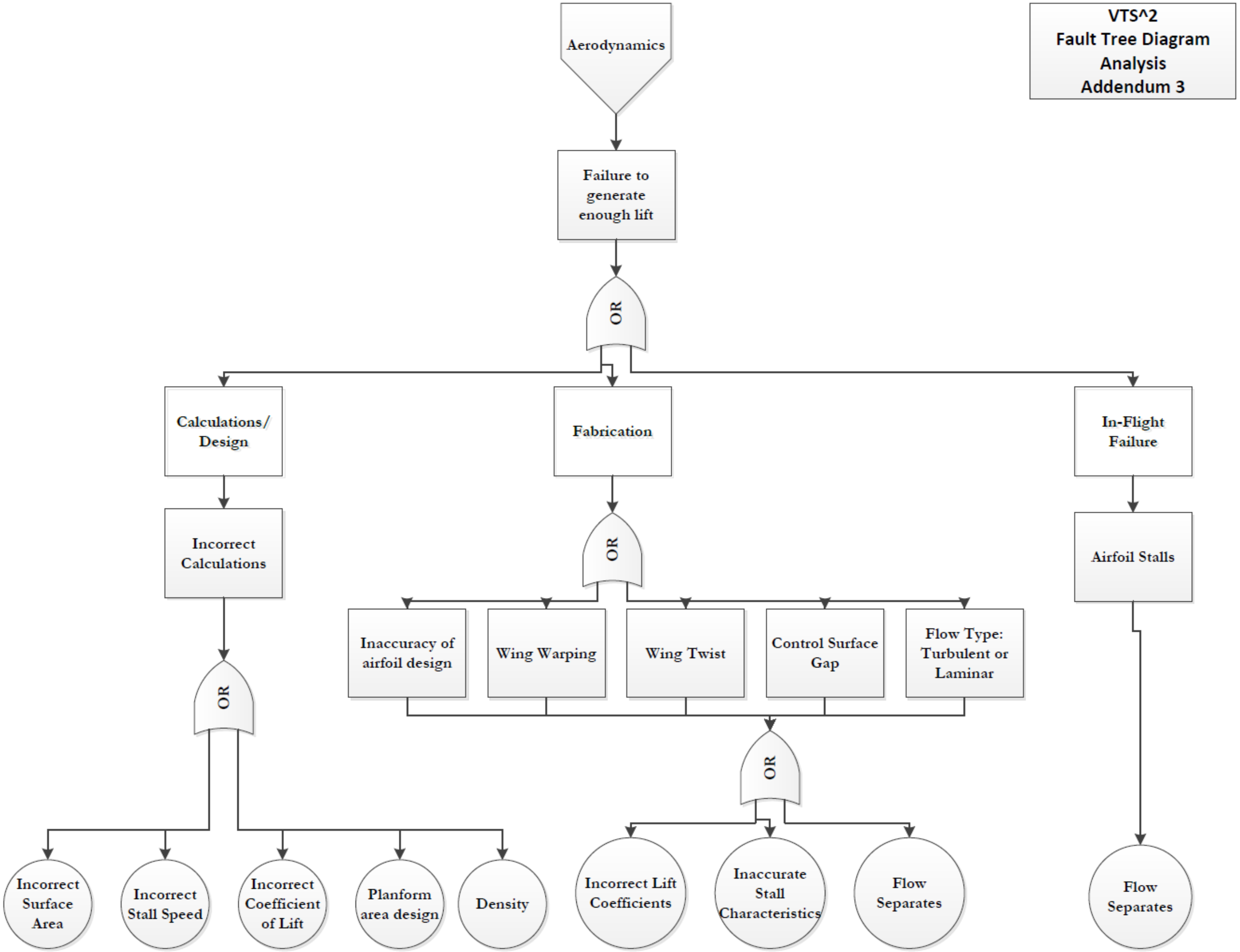
Logic Gates

Intermediate Events

Basic Events

Sample Fault Tree

(from a VT student design project)



Bibliography

Ref. No.	Author(s)	Title
PROJECT MANAGEMENT (PM)		
PM 1	Ruskin, A.M., and Estes, W.E.	***What Every Engineer Should Know About Project Management,*** 2nd Ed., Marcel Dekker, Inc., New York, NY, 1995. **ONE copy in ASDI Library**
PM 2	Anon.	***A Guide to the Project Management Body of Knowledge (PMBOK® Guide),*** 3rd Edition, Project Management Institute, Inc., 2004
PM 3	Haimes, Y.Y.	**Risk Modeling, Assessment, and Management,** 3rd Ed., Johns Wiley & Sons., 2009.

Ref. No.	Author(s)	Title
SYSTEMS THINKING & SYSTEMS ENGINEERING (SE)		
SE 1	Burge, S.E.	***Systems Engineering: Using Systems Thinking to Design Better Aerospace Systems ,*** Wiley Online Library
SE 2	Kossiakoff, A. and Sweet, W.N.	***Systems Engineering Principles and Practice ,*** John Wiley and Sons, Ltd., 2003.
SE 3	Haberfellner, R., de Weck, O., Frickle, E., and Vossner, S.	***Systems Engineering: Fundamentals and Applications ,*** Birkhauser, 2019.
SE 4	NASA	***NASA Systems Engineering Handbook* , NASA SP-2007-6105 Rev 1**, December 2007
SE 5	DoD	***Systems Engineering Fundamentals ,*** Defense Acquisition University Press, Fort Belvoir, VA, 2001