The Overall Process

The [FAA] administrator was interviewed for a documentary film on the [Paris DC−10] accident. He was asked how he could still consider the infamous baggage door safe, given the door failure proven in the Paris accident and the precursor accident at Windsor, Ontario. The Administrator replied−and not facetiously either− 'Of course it is safe, we certified it.'

C.O. Miller

A Comparison of Military and Civilian Approaches to Aviation Safety

Three Approaches to Safety Engineering

- Civil Aviation
- Nuclear Power
- Defense

Civil Aviation

- Fly−fix−fly: analysis of accidents and feedback of experience to design and operation
- Fault Hazard Analysis:
  - Trace accidents (via fault trees) to components
  - Assign criticality levels and reliability requirements to components
- Fail−Safe Design (in Appendix B)

  "No single failure of probable combination of failures during any one flight shall jeopardize the continued safe flight and landing of the aircraft."
- Other airworthiness requirements
- DO−178B (software certification requirements)

Nuclear Power (Defense in Depth)

- Multiple independent barriers to propagation of malfunctions
- High degree of single element integrity and lots of redundancy
- Handling single failures (no single failure of any component will disable any barrier)
- Protection ("safety") systems: automatic system shut−down
- Emphasis on reliability and availability of shutdown system and physical barriers

  Primary approach to achieving this reliability is redundancy
- More emphasis on learning from experience since TMI

Why are these effective?

- Relatively slow pace of basic design changes
  - Use of well−understood and "debugged" designs
- Ability to learn from experience
- Conservatism in design
- Slow introduction of new technology
- Limited interactive complexity and coupling

(But software starting to change these factors)

NOTE EMPHASIS ON COMPONENT RELIABILITY

Defense (and Aerospace) − System Safety

- Emphasizes building in safety rather than adding it on to a completed design.
- Looks at systems as a whole, not just components
  - A top−down systems approach to accident prevention
- Takes a larger view of accident causes than just component failures.
  - Includes interactions among components
- Emphasizes hazard analysis and design to eliminate or control hazards.
- Emphasizes qualitative rather than quantitative approaches.

System Safety

- A planned, disciplined, and systematic approach to preventing or reducing accidents throughout the life cycle of a system.
- ‘‘Organized common sense ’’ (Mueller, 1968)
- Primary concern is the management of hazards:

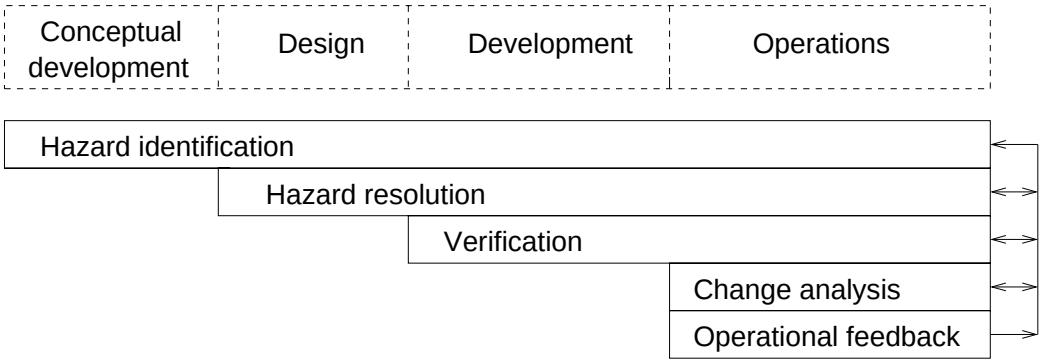
  Hazard
  - identification
  - evaluation
  - elimination
  - control

  through
  - analysis
  - design
  - management

- MIL−STD−882

System Safety (2)

- Analysis: hazard analysis and control is a continuous, iterative process throughout system development and use.



- Design: Hazard resolution precedence:
  1. Eliminate the hazard
  2. Prevent or minimize the occurrence of the hazard
  3. Control the hazard if it occurs.
  4. Minimize damage.
- Management: audit trails, communication channels, etc.

System Safety Process

Safety must be specified and designed into the system and software from the beginning.

- Program/Project Planning
  - Develop policies, procedures, etc.
  - Develop a system safety plan
  - Establish management structure, communication channels, authority, accountability, responsibility
  - Create a hazard tracking system
- Concept Development
  - Identify and prioritize system hazards
  - Generate safety−related system requirements and and design contraints

System Safety Process (2)

- System Design
  - Apply hazard analysis to design alternatives
    - Determine if and how system can get into hazardous states
    - Eliminate hazards from system design if possible
    - Control hazards in system design if cannot eliminate
    - Identify and resolve conflicts between design goals
  - Trace hazard causes and controls to components (hardware, software, and human)
  - Generate component safety requirements and design constraints from system safety requirements and constraints

System Safety Process (3)

- System Implementation
  - Design safety into components
  - Verify safety of constructed system
- Configuration Control and Maintenance
  - Evaluate all proposed changes for safety
- Operations
  - Incident and accident analysis
  - Performance monitoring
  - Periodic audits

Software Safety Tasks

- Establish software safety management structure, authority, responsibility, accountability, communication channels, etc.
- Develop a software hazard tracking system and link to. system hazard tracking system.
- Trace identified system hazards and system safety design constraints to software interface.
- Translate identified software−related hazards and constraints into requirements and constraints on software behavior.
- Evaluate software requirements with respect to system safety design constraints and other safety−related criteria.

Software Safety Tasks (2)

- Design software and HMI to eliminate or control hazards. Design safety into the software.

  Defensive programming
  Assertions and run−time checks
  Separation of critical functions
  Elimination of unnecessary functions
  Exception handling
  etc.

- Analyze the behavior of all reused and COTS software for safety (conformance with safety requirements and constraints)

- Trace safety requirements and constraints to the code. Document safety−related design decisions, design rationale, and other safety−related information.

Software Safety Tasks (3)

- Perform special software safety analyses
  e.g.
  human−computer interaction and interface
  formal or informal walkthroughs or proofs
  interface between critical and non−critical software

- Plan and perform software safety testing. Review test results for safety issues. Trace identified hazards back to system level.

- Analyze all proposed software changes for their effect on safety.

- Establish feedback sources. Analyze operational software and relate to hazard analysis and documented design assumptions.

Hazard List for TCAS

H1: Near midair collision (NMAC): An encounter for which, at the closest point of approach, the vertical separation is less than 100 feet and the horizontal separation is less than 500 feet.

H2: TCAS causes controlled maneuver into ground
e.g. descend command near terrain

H3: TCAS causes pilot to lose control of the aircraft.

H4: TCAS interferes with other safety−related systems
e.g. interferes with ground proximity warning

Level−1 Safety Constraints and Requirements

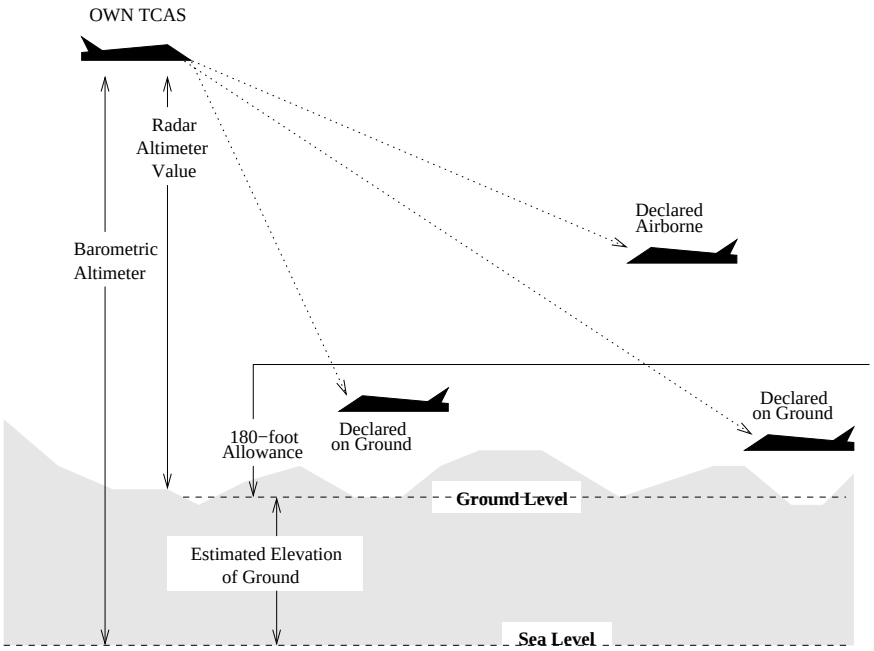
SC−5: The system must not disrupt the pilot and ATC operations during critical phases of flight nor disrupt aircraft operation. [H3] [2.2.3, 2.19, 2.42.2, 2.37]

SC−5.1: The pilot of a TCAS−equipped aircraft must have the option to switch to the Traffic−Advisory mode where traffic advisories are displayed but display of resolution advisories is prohibited [2.37]

Assumption: This feature will be used only during final approach to parallel runways when two aircraft are projected to come close to each other and TCAS would call for an evasive maneuver [6.17]

- TCAS does not display a resolution advisory.
  - TCAS unit is not providing RAs.
    - <Self−monitor shuts down TCAS unit>
    - Sensitivity level set such that no RAs are displayed.
    - ...
  - No RA inputs are provided to the display.
    - No RA is generated by the logic
      - Inputs do not satisfy RA criteria
        - Surveillance puts threat outside corrective RA position.
          - Surveillance does not pass adequate track to the logic
            - <Threat is non−Mode C aircraft> → L.5
            - <Surveillance failure> → 1.23.1
          - to be calculated>
        - Altitude reports put threat outside corrective RA position
          - Altitude errors put threat on ground
            - <Uneven terrain> ↓ 2.19
            - <Intruder altitude error>
            - <Own Mode C altitude error> → 1.23.1
            - <Own radar altimeter error> → 1.23.1
          - Altitude errors put threat in non−threat position.
          - ...
        - <Intruder maneuver causes logic to delay RA beyond CPA> → SC4.2 ↓ 2.35
        - ...
      - <Process/display connectors fail>
  - <Display is preempted by other functions> → SC4.8 ↓ 2.22
  - <Display hardware fails> → 1.23.1

.19 When below 1700 feet AGL, the CAS logic uses the difference between its own aircraft pressure altitude and radar altitude to determine the approximate elevation of the ground above sea level (see Figure 2.5). It then subtracts the latter value from the pressure altitude value received from the target to determine the approximate altitude of the target above the ground (barometric altitude − radar altitude + 180 feet). If this altitude is less than 180 feet, TCAS considers the target to be on the ground [SC−4.9] Traffic and resolution advisories are inhibited for any intruder whose tracked altitude is below this estimate. Hysteresis is provided to reduce vacillations in the display of traffic advisories that might result from hilly terrain [FTA−320]. All RAs are inhibited when own TCAS is within 500 feet of the ground.



TCAS displays a resolution advisory that the pilot does not follow.

- Pilot does not execute RA at all.
  - Crew does not perceive RA alarm.
    - <Inadequate alarm design> → 1.6,1.7,1.8 ↓ 2.74, 2.76
    - <Crew is preoccupied>
  - <Crew does not believe RA is correct.> → OP.1
  - ...
- Pilot executes the RA but inadequately
  - <Pilot stops before RA is removed> → OP.10
  - <Pilot continues beyond point RA is removed> → OP.4
  - <Pilot delays execution beyond time allowed> → OP.10

- Operator Requirements

  OP. 4 After the threat is resolved the pilot shall return promptly and smoothly to his/her previously assigned flight path.
  [FTA−560, 3.3, 6.49.7]

- Human−Machine Interface Requirements

  1.8 A red visual alert shall be provided in the primary field of view for each pilot for resolution advisories.
  [FTA−515, 2.84]

- System Limitations

  L.5 TCAS provides no protection against aircraft with nonoperational or non−Mode C transponders.
  [FTA−370]

SC−7: TCAS must not create near misses (result in a hazardous (result in a hazardous level of vertical separation that would not have occurred had the aircraft not carried TCAS) [H1]

SC−7.1: Crossing maneuvers must be avoided if possible. [2.36, 2.38, 2.48, 2.49.2]

SC−7.2: The reversal of a displayed advisory must be extremely rare [2.51, 2.56.3, 2.65.3, 2.66]

SC−7.3: TCAS must not reverse an advisory if the pilot will have insufficient time to respond to the RA before the closest point of approach (four seconds or less) or if own and intruder aircraft are separated by less then 200 feet vertically when ten seconds or less remain to closest point of approach [2.52]

Example Level−2 System Design for TCAS

SENSE REVERSALS ↓Reversal−Provides−More−Separation

2.51 In most encounter situations, the resolution advisory sense will be maintained for the duration of an encounter with a threat aircraft.
[SC−7.2]
However, under certain circumstances, it may be necessary for that sense to be reversed. For example, a conflict between two TCAS−equipped aircraft will, with very high probability, result in selection of complementary advisory senses because of the coordination protocol between the two aircraft. However, if coordination communications between the two aircraft are disrupted at a critical time of sense selection, both aircraft may choose their advisories independently.
[FTA−1300]
This could possibly result in selection of incompatible senses.
[FTA−395]

2.51.1 [Information about how incompatibilities are handled]

Example from Level 3 Model of Collision Avoidance Logic

INTRUDER.STATUS

- Other–Traffic
- Proximate–Traffic
- Potential–Threat
- Threat
- Unknown

= Other–Traffic

		OR			
	Alt–Reporting **in–state** Lost	T	T	T	.
	Bearing–Valid	F	.	T	.
AND	Range–Valid	.	F	T	.
	Proximate–Traffic–Condition	.	.	F	.
	Potential–Threat–Condition	.	.	F	.
	Other–Aircraft **in–state** On–Ground	.	.	.	T

Description: A threat is reclassified as other traffic if its altitude reporting has been lost (↑2.13) and either the bearing or range inputs are invalid; if its altitude reporting has been lost and both the range and bearing are valid but neither the proximate nor potential threat classification criteria are satisfied; or the aircraft is on the ground (↑2.12) .

Mapping to Level 2: ↑2.23, ↑2.29

Mapping to Level 4: ↓4.7.1, Traffic_advisory_detection

Example MITRE Pseudo–Code from Level 4

```
PROCESS Traffic_advisory_detection;
    CLEAR  PROX_TEST;
    IF  (ITF.TACODE  EQ  $RA)
          THEN  ITF.TATIME = P.MINATIME;
    ELSEIF  (ITF.IOGROUND  EQ  $TRUE)
          THEN ITF.TACODE = $NOTAPA;
               ITF.TATIME = 0;
    OTHERWISE  PERFORM  Traffic_parameters;
          PERFORM  Traffic_range_test;
          IF  (RHITA  EQ  $TRUE)
               THEN  PERFORM  Range_hit_processing;
               ELSEIF  (ITF.TATIME  NE  0)
                    THEN  ITF.TATIME = ITF.TATIME – 1;
                          IF  (ITF.MODC  EQ  $FALSE)
                              THEN  ITF.TACODE = $TANMC;
                              ELSE  ITF.TACODE = $TAMC;
                    ELSE  SET  PROX_TEST;
          IF  (PROX_TEST  EQ  $TRUE)
               THEN  PERFORM  Proximity_test;
                     IF  (PRXHITA  EQ  $TRUE)
                         THEN  ITF.TACODE = $PENDPA;
                         ESLE  ITF.TACODE = $NOTAPA;
     END  Traffic_advisory_detection;
```

Hazard Analysis for oftware−Intensive Systems

Terminology

Accident: An undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss.

Incident: An event that involves no loss (or only minor loss) but with the potential for loss under different circumstances.

Hazard: A state or set of conditions that, together with other conditions in the environment, will lead to an accident (loss event).

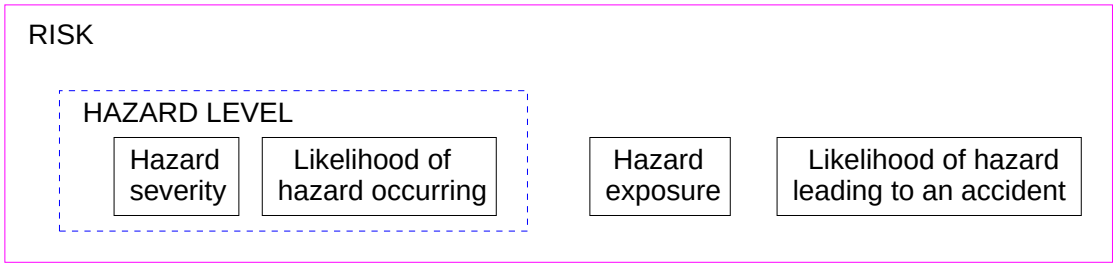
Note that a hazard is NOT equal to a failure.

‘‘Distinguishing hazards from failures is implicit in understanding the difference between safety and reliability engineering.

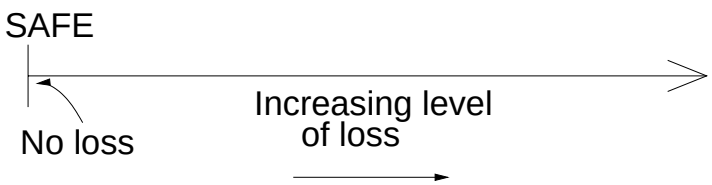
C.O Miller

Hazard Level: A combination of severity (worst potential damage in case of an accident) and likelihood of occurence of the hazard.

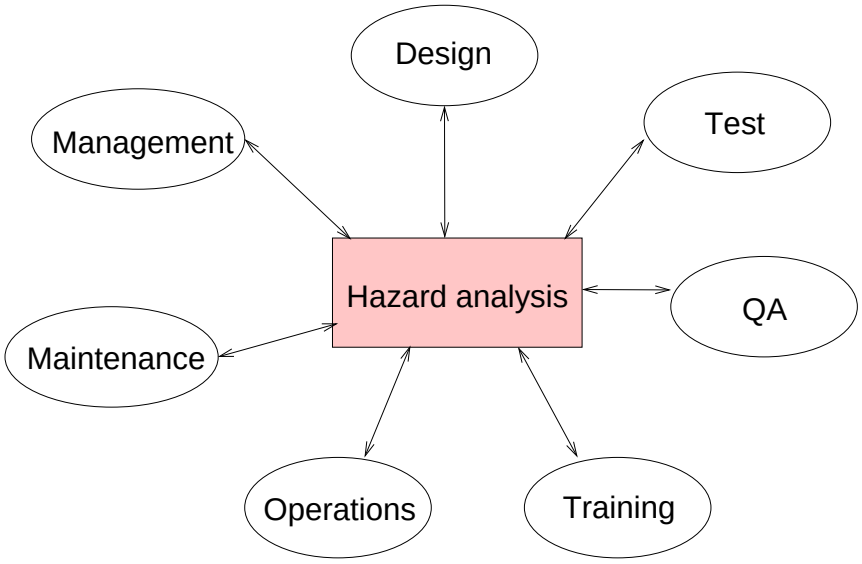
Risk: The hazard level combined with the likelihood of the hazard leading to an accident plus exposure (or duration) of the hazard.



Safety: Freedom from accidents or losses.



Hazard analysis affects, and in turn, is affected by all aspects of the development process.



Hazard Analysis

Hazard analysis is the heart of any system safety program.

Used for:

- Developing requirements and design constraints
- Validating requirements and design for safety
- Preparing operational procedures and instructions
- Test planning
- Management planning

Serves as:

- A framework for ensuing steps
- A checklist to ensure management and technical responsibilities for safety are accomplished.

"Types" (Stages) of Hazard Analysis

- Preliminary Hazard Analysis (PHA)
  - Identify, assess, and prioritize hazards
  - Identify high−level safety design constraints
- System Hazard Analysis (SHA)
  - Examine subsystem interfaces to evaluate safety of system working as a whole
  - Refine design constraints and trace to individual components (including operators)

"Types" (Stages) of Hazard Analysis (2)

- Subsystem Hazard Analysis (SSHA)
  - Determine how subsystem design and behavior can contribute to system hazards.
  - Evaluate subsystem design for compliance with safety constraints.
- Change and Operations Analysis
  - Evaluate all changes for potential to contribute to hazards
  - Analyze operational experience

Preliminary Hazard Analysis

1. Identify system hazards
2. Translate system hazards into high−level system safety design constraints.
3. Assess hazards if required to do so.
4. Establish the hazard log.

System Hazards for Automated Train Doors

- Train starts with door open.
- Door opens while train is in motion.
- Door opens while improperly aligned with station platform.
- Door closes while someone is in doorway
- Door that closes on an obstruction does not reopen or reopened door does not reclose.
- Doors cannot be opened for emergency evacuation.

System Hazards for Air Traffic Control

- Controlled aircraft violate minimum separation standards (NMAC).
- Airborne controlled aircraft enters an unsafe atmospheric region.
- Controlled airborne aircraft enters restricted airspace without authorization.
- Controlled airborne aircraft gets too close to a fixed obstable other than a safe point of touchdown on assigned runway (CFIT)
- Controlled airborne aircraft and an intruder in controlled airspace violate minimum separation.
- Controlled aircraft operates outside its performance envelope.
- Aircraft on ground comes too close to moving objects or collides with stationary objects or leaves the paved area.
- Aircraft enters a runway for which it does not have clearance.
- Controlled aircraft executes an extreme maneuver within its performance envelope.
- Loss of aircraft control.

Exercise: Identify the system hazards for this cruise−control system

The cruise control system operates only when the engine is running. When the driver turns the system on, the speed at which the car is traveling at that instant is maintained. The system monitors the car's speed by sensing the rate at which the wheels are turning, and it maintains desired speed by controlling the throttle position. After the system has been turned on, the driver may tell it to start increasing speed, wait a period of time, and then tell it to stop increasing speed. Throughout the time period, the system will increase the speed at a fixed rate, and then will maintain the final speed reached.

The driver may turn off the system at any time. The system will turn off if it senses that the accelerator has been depressed far enough to override the throttle control. If the system is on and senses that the brake has been depressed, it will cease maintaining speed but will not turn off. The driver may tell the system to resume speed, whereupon it will return to the speed it was maintaining before braking and resume maintenance of that speed.

Hazard Identification

- Use historical safety experience, lessons learned, trouble reports, hazard analyses, and accident and incident files.
- Look at published lists, checklists, standards, and codes of practice.
- Examine basic energy sources, flows, high−energy items, hazardous materials (fuels, propellants, lasers, explosives, toxic substances, and pressure systems).
- Look at potential interface problems such as material incompatibilties, possibilities for inadvertent activation, contamination, and adverse environmental scenarios.
- Review mission and basic performance requirements including environments in which operations will take place. Look at all possible system uses, all modes of operation, all possible environments, and all times during operation.

Hazard Identification (2)

- Examine human−machine interface.
- Look at transition phases, nonroutine operating modes, system changes, changes in technical and social environment, and changes between modes of operation.
- Use scientific investigation of physical, chemical, and other properties of system.
- Think through entire process, step by step, anticipating what might go wrong, how to prepare for it, and what to do if the worst happens.

Specifying Safety Constraints

- Most software requirements only specify nominal behavior

  Need to specify off−nominal behavior

  Need to specify what software must NOT do

- What must not do is not inverse of what must do

- Derive from system hazard analysis

HAZARD	DESIGN CONSTRAINT
Train starts with door open.	Train must not be capable of moving with any door open.
Door opens while train is in motion.	Doors must remain closed while train is in motion.
Door opens while improperly aligned with station platform.	Door must be capable of opening only after train is stopped and properly aligned with platform unless emergency exists (see below).
Door closes while someone is in doorway.	Door areas must be clear before door closing begins.
Door that closes on an obstruction does not reopen or reopened door does not reclose.	An obstructed door must reopen to permit removal of obstruction and then automatically reclose.
Doors cannot be opened for emergency evacuation.	Means must be provided to open doors anywhere when the train is stopped for emergency evacuation.

Example ATC Approach Control

HAZARDS	REQUIREMENTS/CONSTRAINTS
1. A pair of controlled aircraft violate minimum separation standards.	1a. ATC shall provide advisories that maintain safe separation between aircraft. 1b. ATC shall provide conflict alerts.
2. A controlled aircraft enters an unsafe atmospheric region. (icing conditions, windshear areas, thunderstorm cells)	2a. ATC must not issue advisories that direct aircraft into areas with unsafe atmospheric conditions. 2b. ATC shall provide weather advisories and alerts to flight crews. 2c. ATC shall warn aircraft that enter an unsafe atmospheric region.
3. A controlled aircraft enters restricted airspace without authorization.	3a. ATC must not issue advisories that direct an aircraft into restricted airspace unless avoiding a greater hazard. 3b. ATC shall provide timely warnings to aircraft to prevent their incursion into restricted airspace.
4. A controlled aircraft gets too close to a fixed obstacle or terrain other than a safe point of touchdown on assigned runway.	4. ATC shall provide advisories that maintain safe separation between aircraft and terrain or physical obstacles.
5. A controlled aircraft and an intruder in controlled airspace violate minimum separation standards.	5. ATC shall provide alerts and advisories to avoid intruders if at all possible.
6. Loss of controlled flight or loss of airframe integrity.	6a. ATC must not issue advisories outside the safe performance envelope of the aircraft. 6b. ATC advisories must not distract or disrupt the crew from maintaining safety of flight. 6c. ATC must not issue advisories that the pilot or aircraft cannot fly or that degrade the continued safe flight of the aircraft. 6d. ATC must not provide advisories that cause an aircraft to fall below the standard glidepath or intersect it at the wrong place.

Classic Hazard Level Matrix

SEVERITY

LIKELIHOOD	I Catastrophic	II Critical	III Marginal	IV Negligible
A Frequent	I–A	II–A	III–A	IV–A
B Moderate	I–B	II–B	III–B	IV–B
C Occasional	I–C	II–C	III–C	IV–C
D Remote	I–D	II–D	III–D	IV–D
E Unlikely	I–E	II–E	III–E	IV–E
F Impossible	I–F	II–F	III–F	IV–F

Another Example Hazard Level Matrix

	A Frequent	B Probable	C Occasional	D Remote	E Improbable	F Impossible
Catastrophic I	Design action required to eliminate or control hazard 1	Design action required to eliminate or control hazard 2	Design action required to eliminate or control hazard 3	Hazard must be controlled or hazard probability reduced 4	9	12
Critical II	Design action required to eliminate or control hazard 3	Design action required to eliminate or control hazard 4	Hazard must be controlled or hazard probability reduced 6	Hazard control desirable if cost effective 7	Assume will not occur 12	Impossible occurrence 12
Marginal III	Design action required to eliminate or control hazard 5	Hazard must be controlled or hazard probability reduced 6	Hazard control desirable if cost effective 8	Normally not cost effective 10	12	12
Negligible IV	10	11	Negligible hazard 12	12	12	12

NASA Closure Classification Risk Matrix

LIKELIHOOD	SEVERITY: Catastrophic	Critical	Marginal
Probable	Unacceptable Risk	Accepted Risks	Accepted Risks
Infrequent	Accepted Risks	Accepted Risks	Accepted Risks
Remote	Accepted Risks	Accepted Risks	Controlled
Improbable	Controlled	Controlled	Controlled

Eliminated hazard − A hazard that has been eliminated by completely removing the hazard causal factors.

Controlled hazard − A hazard for which the frequency of occurrence and/or severity level has been reduced by implementing the appropriate hazard reduction precedence sequence to comply with program requirements.

Accepted risk − A hazard for which the controls for one or more hazard causes fail to meet the hazard reduction precedence sequence and therefore, have limitations or uncertainties such that the hazard could occur during the life of the program. The following are examples of conditions that could be considered accepted risk hazards:

1. Critical single failure point.
2. Limited controls, or controls that are subject to human error or interpretation.
3. System designs or operations that do not meet industry or Government standards
4. Complex fluid system leaks
5. Safety detection and suppression devices which are not adequate
6. Uncontrollable random events which could even with even with established precautions and controls in place, such as weather

Risk Assessment

Hazard Level Assessment:

- Not feasible for complex human/computer−controlled systems
  - No way to determine likelihood, even qualitatively
  - Almost always involves new designs and new technology
- Severity is usually adequate (and that can be determined) to determine effort to spend on eliminating or mitigating hazard.

System Risk Assessment:

- Again, not feasible.
- May be possible to establish qualitative criteria to evaluate potential risk to make deployment or technology decisions, but will depend on system.

Example Qualitative Hazard Level Assessment

AATT Safety Criterion:

The introduction of AATT tools will not degrade safety from the current level.

Risk assessment for each tool based on:

- Severity of worst possible loss associated with tool
- Likelihood that introduction of tool will reduce current safety level of ATC system.

Example Severity Level

(from a proposed JAA standard)

- Class I: Catastrophic
  - Unsurvivable accident with hull loss.
- Class II: Critical
  - Survivable accident with less than full hull loss; fatalities possible
- Class III: Marginal
  - Equipment loss with possible injuries and no fatalities
- Class IV: Negligible
  - Some loss of efficiency
  - Procedures able to compensate, but controller workload likely to be high until overall system demand reduced.
  - Reportable incident events such as operational errors, pilot deviations, surface vehicle deviation.

Example Likelihood Level

- User tasks and responsibilities

  Low: Insignificant or no change
  Medium: Minor change
  High: Significant change

- Potential for inappropriate human decision making

  Low: Insignificant or no change
  Medium: Minor change
  High: Significant change

- Potential for user distraction or disengagement from primary task

  Low: Insignificant or no change
  Medium: Minor change
  High: Significant change

xample Likelihood Level (2)

- Safety margins
  - Low: Insignificant or no change
  - Medium: Minor change
  - High: Significant change
- Potential for reducing situation awareness
  - Low: Insignificant or no change
  - Medium: Minor change
  - High: Significant change
- Skills currently used and those necessary to backup and monitor new decision support tools
  - Low: Insignificant or no change
  - Medium: Minor change
  - High: Significant change
- Introduction of new failure modes and hazard causes
  - Low: New tools have same function and failure modes as system components they are replacing
  - Medium: Introduced but well understood and effective mitigation measures can be designed
  - High: Introduced and cannot be classified under medium
- Effect of software on current system hazard mitigation measures
  - Low: Cannot render ineffective
  - High: Can render ineffective
- Need for new system hazard mitigation measures
  - Low: Potential software errors will not require
  - High: Potential software errors could require