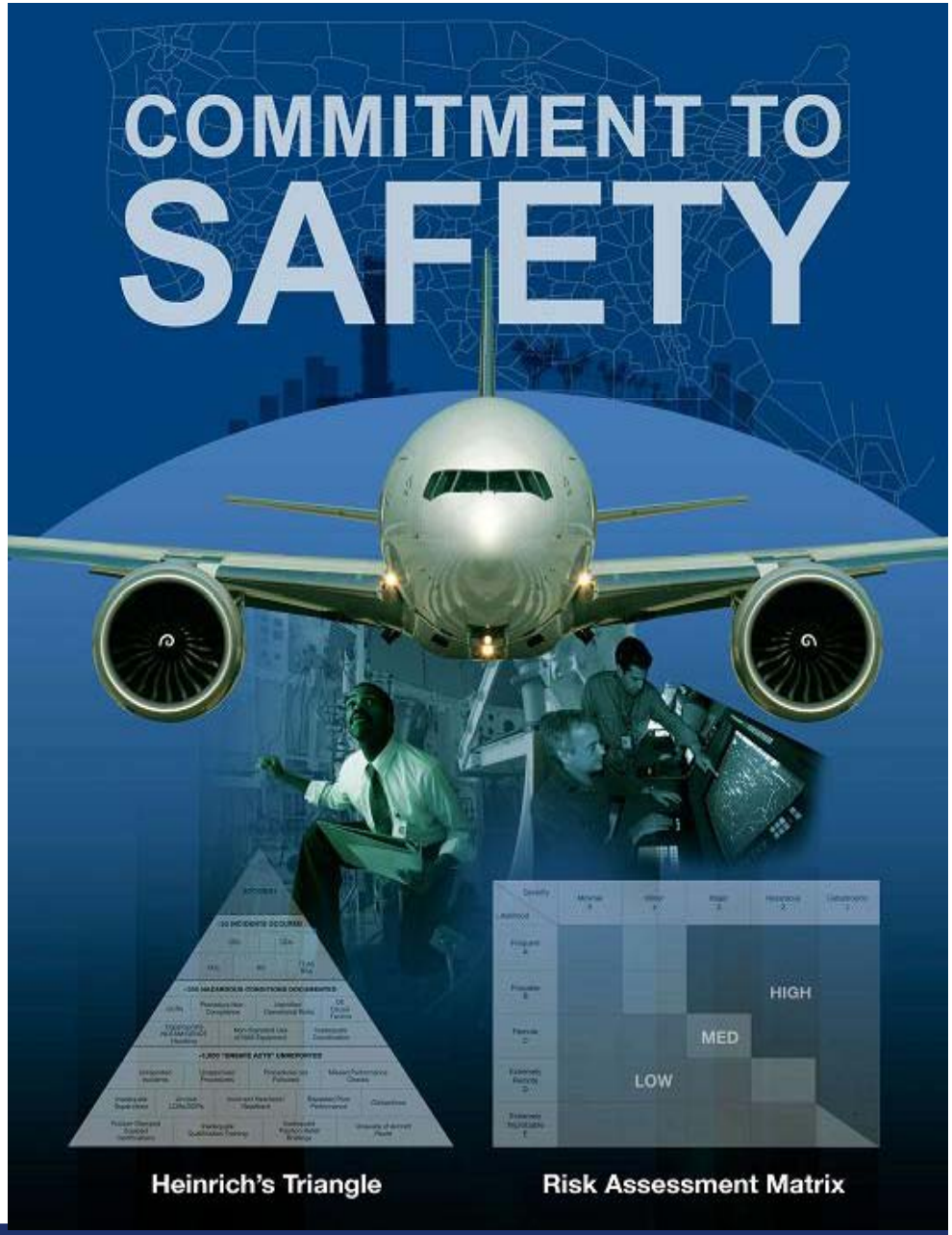
ATO

Safety Risk Management



Presented By:
Michael Falteisek
Federal Aviation Administration
Air Traffic Organization-Office of Safety
Manager, Safety Risk Management

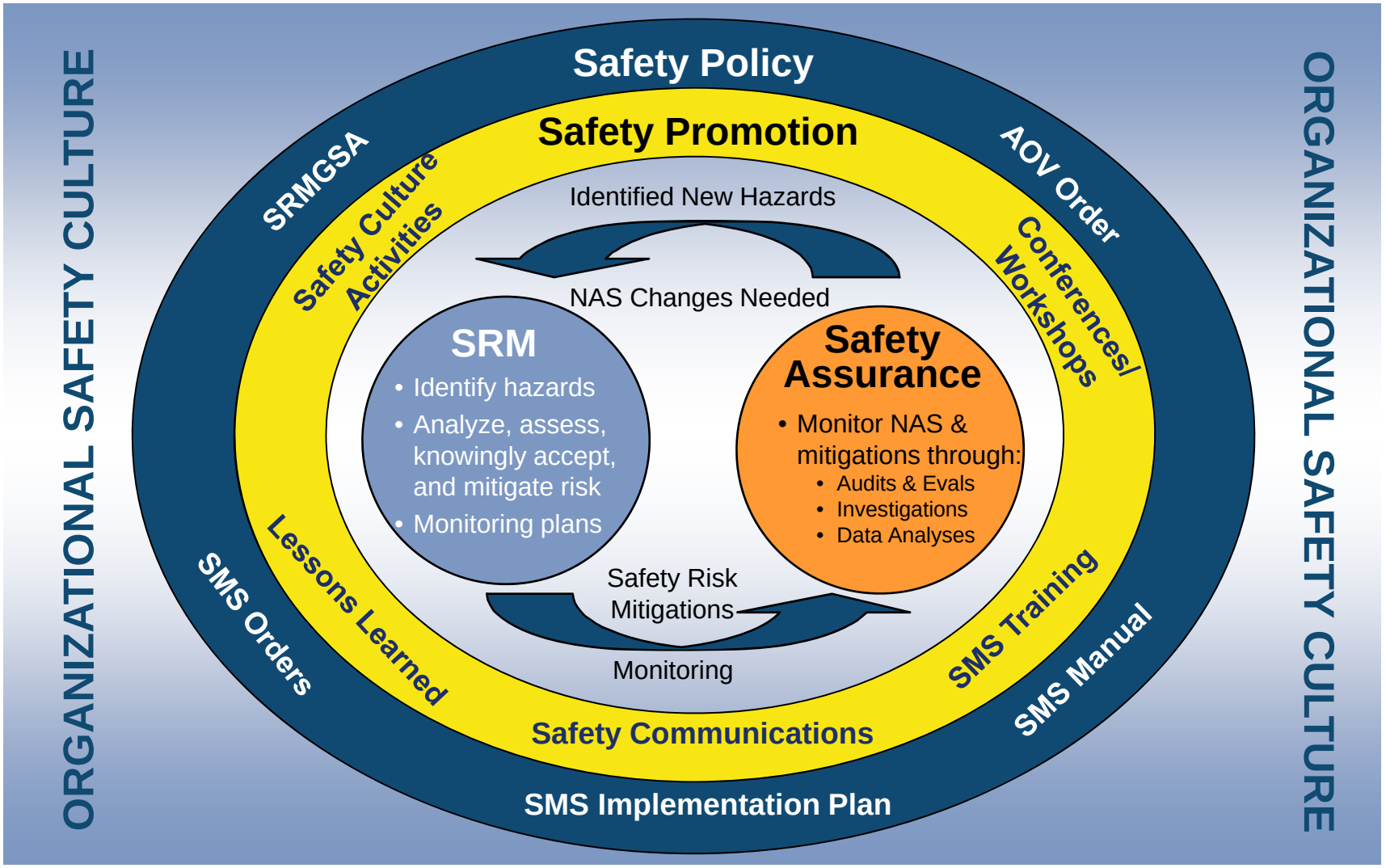
What Is the FAA's Safety Management System?

SMS Definition*

- An integrated collection of processes, procedures, policies, and programs that are used to assess, define, and manage the safety risk in the provision of ATC and navigational services

*** AOV Safety Oversight Circular 08-06, *ATO Safety Management System (SMS) Definitions***

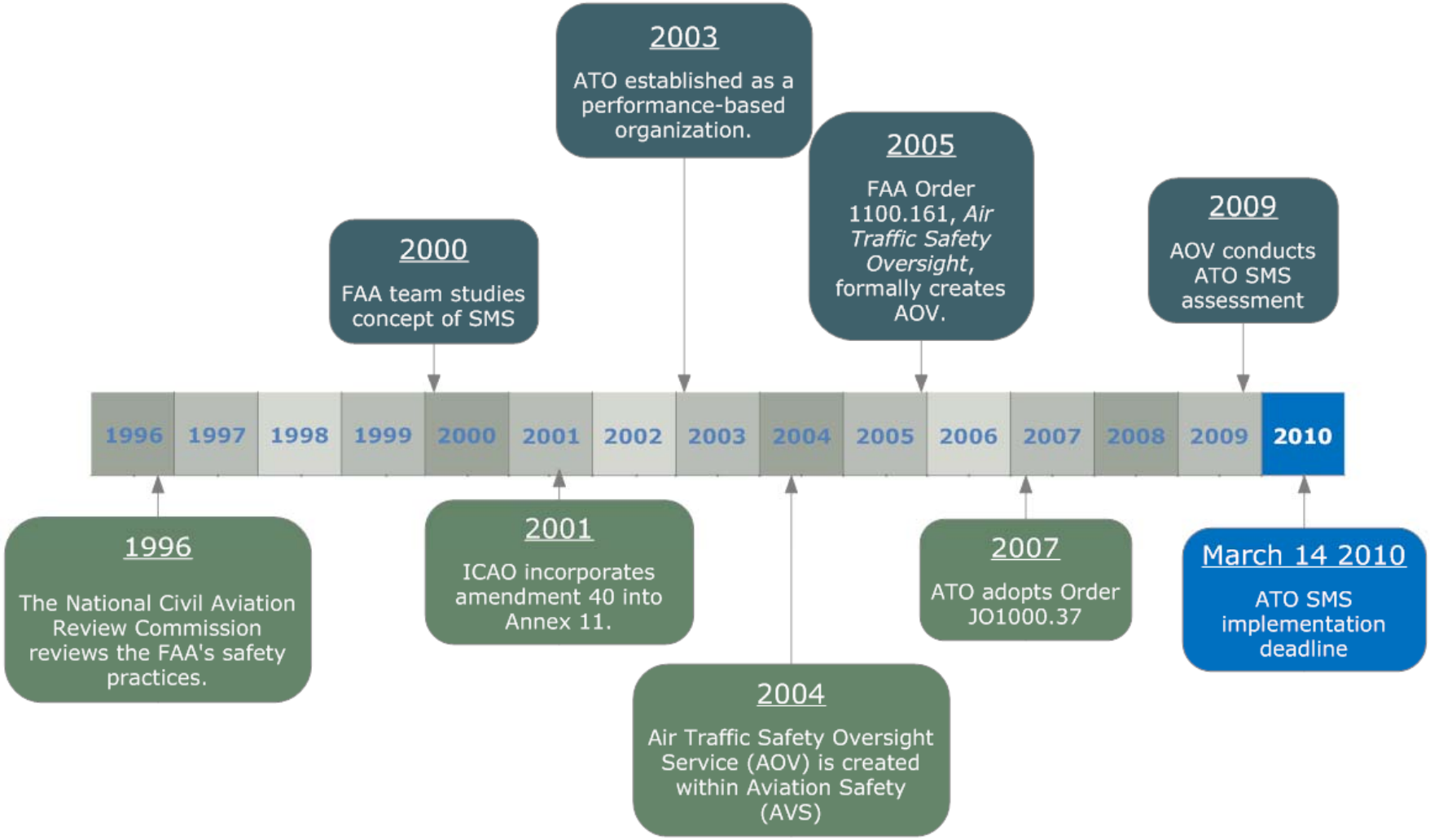
SMS Components



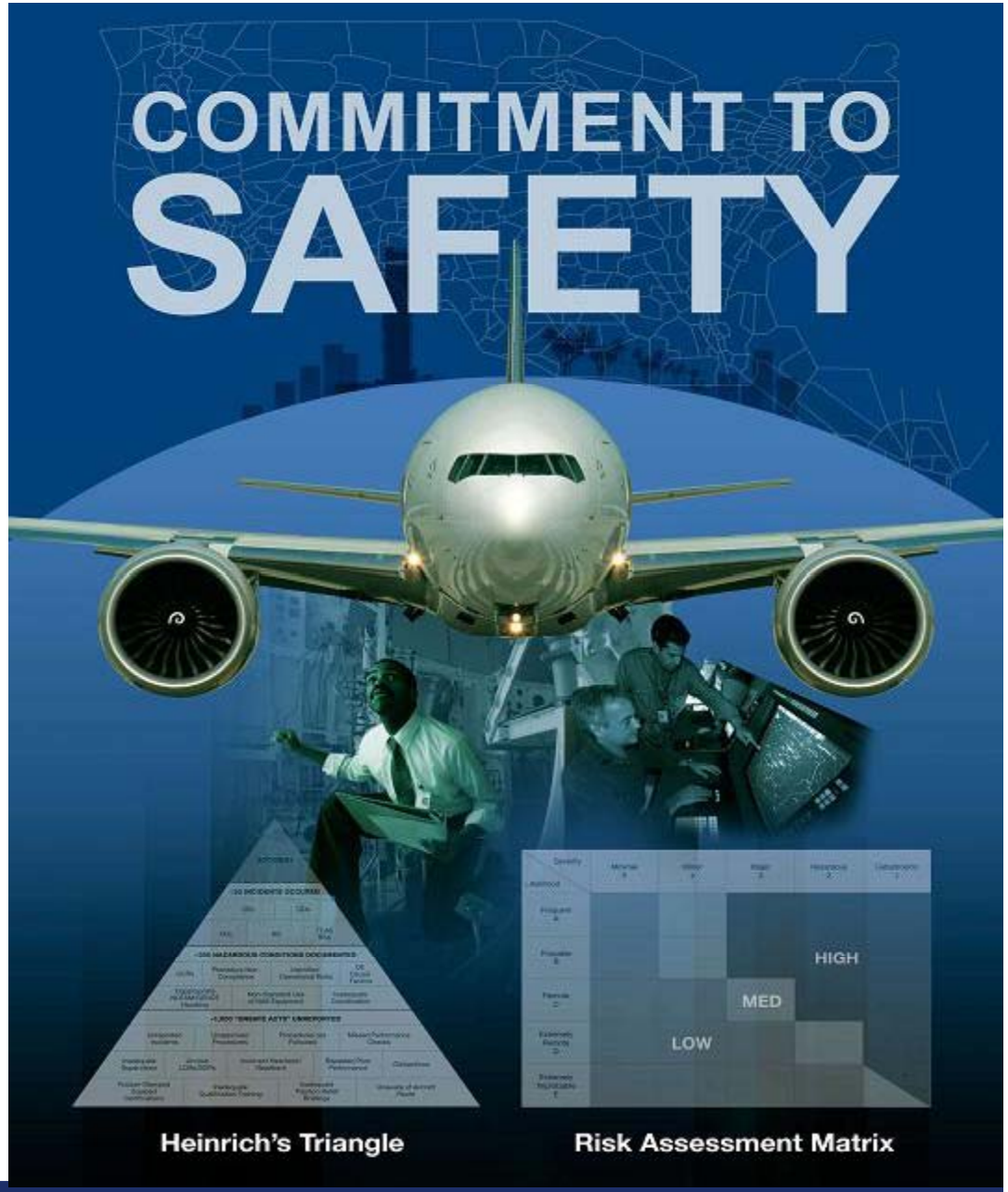
SMS in the FAA ATO

- Formal system approach to managing the safety risk of Air Traffic Control (ATC) and navigation services
- Provides consistent processes and documentation in managing safety risk
- Provides a standardized methodology to identify and address safety hazards that occur within the National Airspace System (NAS) or in which some element of the NAS is a contributing factor
- FAA Flight Plan Goal

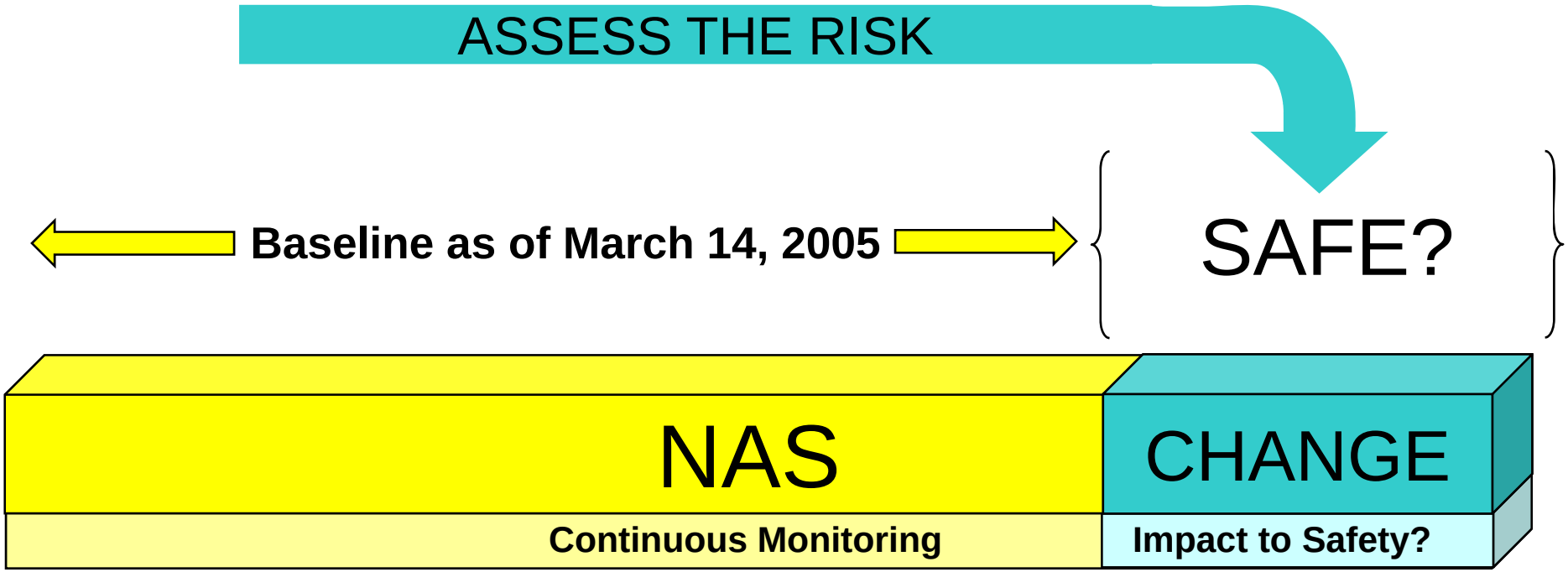
SMS Historical Highlights



Safety Risk Management



Risk Assessment of ALL Changes

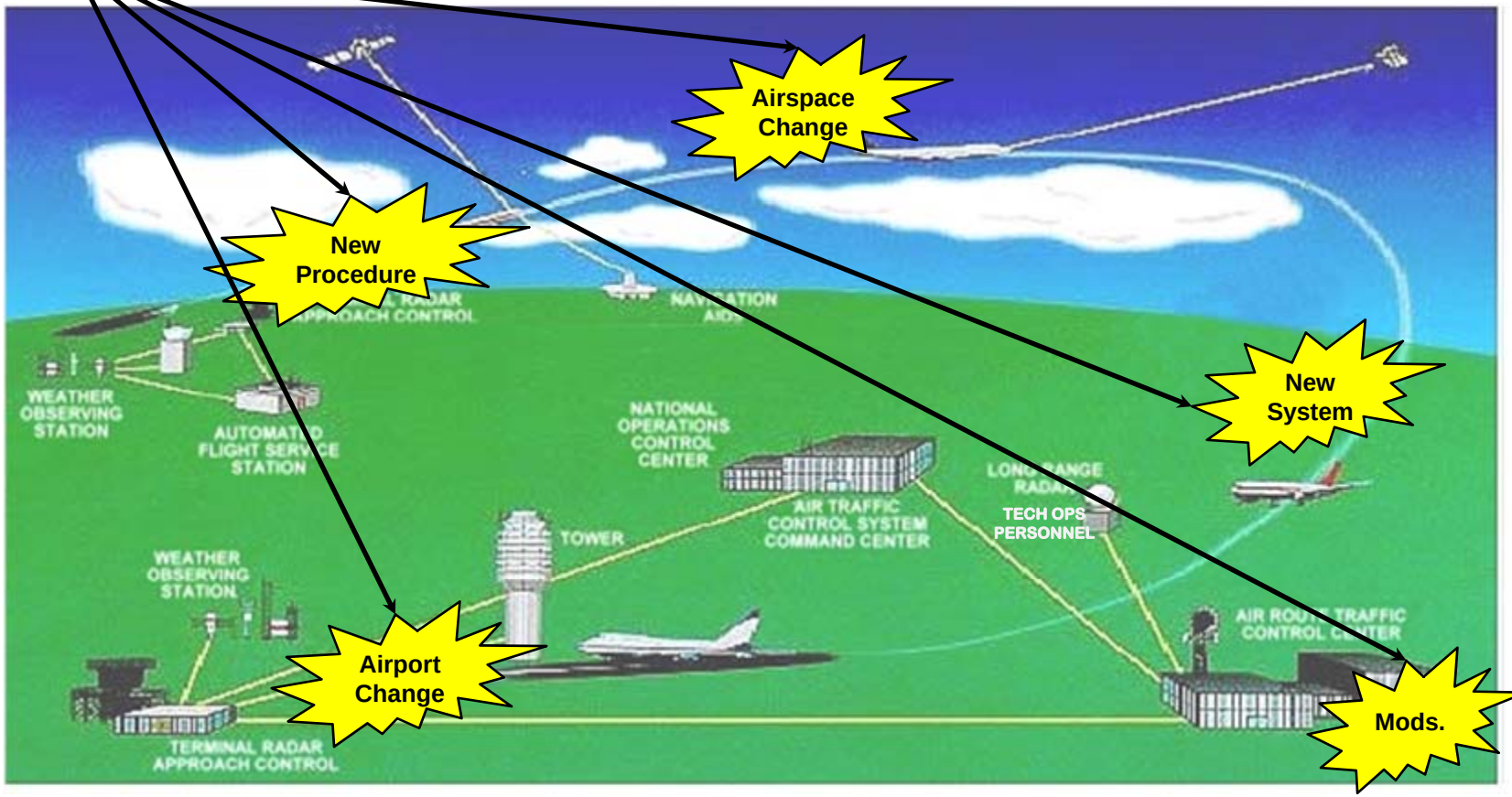


Maintain and Improve the Safety of the NAS

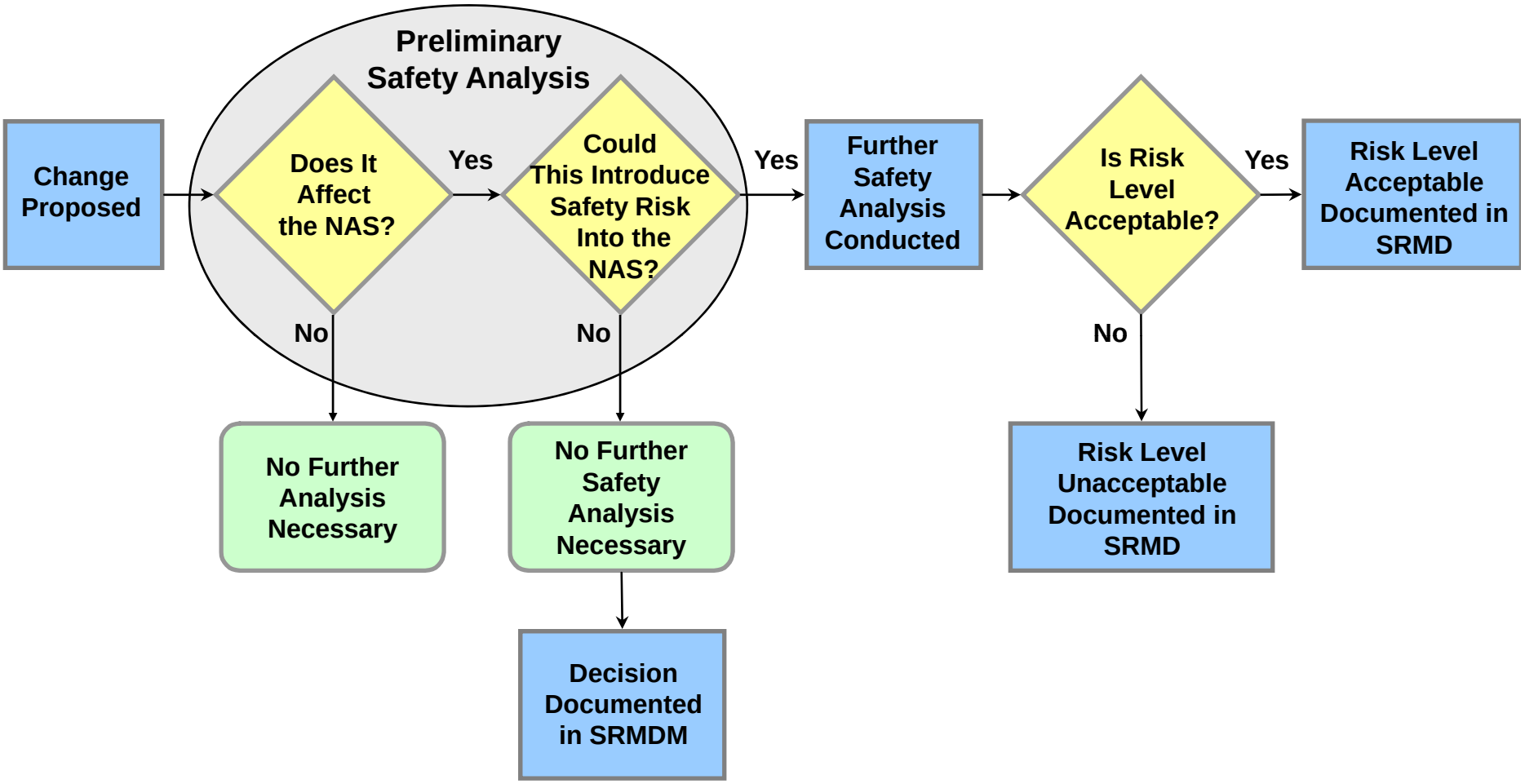
National Airspace System: Is comprised of airspace; airports; aircrafts; pilots; air navigation facilities; air traffic control (ATC) facilities; communication, surveillance, navigation, and supporting technologies and systems; operating rules, regulations, policies, and procedures; and the people who implement, sustain, or operate the system components

Safety Risk Management and the ATO

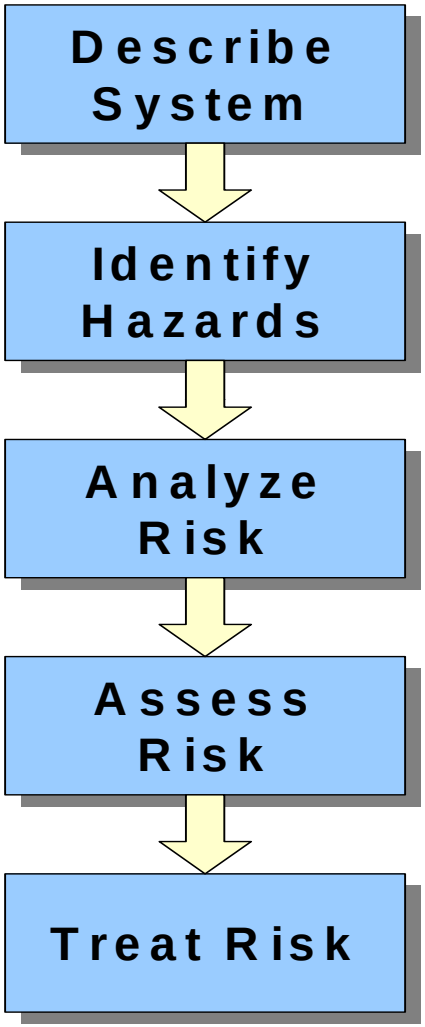
Safety Risk Management → Describe System → Identify Hazards → Analyze Risk → Assess Risk → Treat Risk



SRM Decision Process



SRM Process



- Define scope and objectives
- Define stakeholders
- Identify criteria and plan for risk management effort (including any modeling/ simulation potentially required)
- Describe system/change (use, environment, and intended function, including planned future configuration)

Identify hazards (what can go wrong?) that exist in the context of the NAS change

- Use structured approach
- Be comprehensive (and do not dismiss hazards prematurely)
- Employ lessons learned and experience supplemented by checklists

For each hazard:

- Identify existing mitigations/controls
- Determine risk (severity and likelihood) of outcome
  - Qualitative or quantitative (preferred)

- Rank hazards according to the severity and likelihood of their risk
- Select hazards for detailed risk treatment (based on risk)

- Identify feasible mitigation options
- Develop risk treatment plans
- Implement and verify
- Monitor

Severity Definitions

Effect On: ↓	Hazard Severity Classification				
	Minimal 5	**Minor 4**	**Major 3**	**Hazardous 2**	**Catastrophic 1**
ATC Services	Conditions resulting in a minimal reduction in ATC services, or a loss of separation resulting in a Category D Runway Incursion (RI)[1], or proximity event	Conditions resulting in a slight reduction in ATC services, or a loss of separation resulting in a Category C RI[1], or Operational Error (OE)[2]	Conditions resulting in a partial loss of ATC services, or a loss of separation resulting in a Category B RI[1], or OE[2]	Conditions resulting in a total loss of ATC services, (ATC Zero) or a loss of separation resulting in a Category A RI[1] or OE[2]	Conditions resulting in a collision between aircraft, obstacles or terrain
Flight Crew	– Flightcrew receives TCAS Traffic Advisory (TA) informing of nearby traffic, or, – Pilot Deviation (PD) where loss of airborne separation falls within the same parameters of a Category D OE [2] or proximity Event – Minimal effect on operation of aircraft	– Potential for Pilot Deviation (PD) due to TCAS Preventive Resolution Advisory (PRA) advising crew not to deviate from present vertical profile, or, – PD where loss of airborne separation falls within the same parameters of Category C (OE) [2] , or – Reduction of functional capability of aircraft but does not impact overall safety e.g. normal procedures as per AFM	– PD due to response to TCAS Corrective Resolution Advisory (CRA) issued advising crew to take vertical action to avoid developing conflict with traffic, or, – PD where loss of airborne separation falls within the same parameters of a Category B OE [2], or, – Reduction in safety margin or functional capability of the aircraft, requiring crew to follow abnormal procedures as per AFM	– Near mid-air collision (NMAC) results due to proximity of less than 500 feet from another aircraft or a report is filed by pilot or flight crew member that a collision hazard existed between two or more aircraft – Reduction in safety margin and functional capability of the aircraft requiring crew to follow emergency procedures as per AFM	– Conditions resulting in a mid-air collision (MAC) or impact with obstacle or terrain resulting in hull loss, multiple fatalities, or fatal injury

Severity Definitions (cont'd)

Effect On: ↓	Hazard Severity Classification				
	Minimal 5	**Minor 4**	**Major 3**	**Hazardous 2**	**Catastrophic 1**
Flying Public	– Minimal injury or discomfort to passenger(s)	– Physical discomfort to passenger(s) (e.g. extreme braking action; clear air turbulence causing unexpected movement of aircraft causing injuries to one or two passengers out of their seats) – Minor[3] injury to greater than zero to less or equal to 10% of passengers	– Physical distress on passengers (e.g. abrupt evasive action; severe turbulence causing unexpected aircraft movements) – Minor[3] injury to greater than 10% of passengers	– Serious[4] injury to passenger(s)	– Fatalities, or fatal[5] injury to passenger(s)

1 – As defined in 2005 Runway Safety Report

2 – As defined in FAA Order 7210.56 – Air Traffic Quality Assurance and *N JO 7210.663*-Operational Error Reporting, Investigation, and Severity Policies

3 – Minor Injury - Any injury that is neither fatal nor serious.

4 – Serious Injury - Any injury which: (1) requires hospitalization for more than 48 hours, commencing within 7 days from the date the injury was received; (2) results in a fracture of any bone (except simple fractures of fingers, toes, or nose); (3) causes severe hemorrhages, nerve, muscle, or tendon damage; (4) involves any internal organ; or (5) involves second- or third-degree burns, or any burns affecting more than 5 percent of the body surface.

5 – Fatal Injury - Any injury that results in death within 30 days of the accident.

Likelihood Definitions

	NAS Systems & ATC Operational	NAS Systems		ATC Operational		Flight Procedures
	Quantitative	Qualitative				
		Individual Item/System	ATC Service/ NAS Level System	Per Facility	NAS-wide	
Frequent A	Probability of occurrence per operation/ operational hour is equal to or greater than $1x10^{-3}$	Expected to occur about once every 3 months for an item	Continuously experienced in the system	Expected to occur more than once per week	Expected to occur more than every 1-2 days	Probability of occurrence per operation/ operational hour is equal to or greater than $1x10^{-5}$
Probable B	Probability of occurrence per operation/ operational hour is less than $1x10^{-3}$, but equal to or greater than $1x10^{-5}$	Expected to occur about once per year for an item	Expected to occur frequently in the system	Expected to occur about once every month	Expected to occur about several times per month	
Remote C	Probability of occurrence per operation/ operational hour is less than or equal to $1x10^{-5}$ but equal to or greater than $1x10^{-7}$	Expected to occur several times in life cycle of an item	Expected to occur numerous times in system life cycle	Expected to occur about once every year	Expected to occur about once every few months	Probability of occurrence per operation/ operational hour is less than or equal to $1x10^{-5}$ but equal to or greater than $1x10^{-7}$
Extremely Remote D	Probability of occurrence per operation/ operational hour is less than or equal to $1x10^{-7}$ but equal to or greater than $1x10^{-9}$	Unlikely to occur, but possible in an item's life cycle	Expected to occur several times in the system life cycle	Expected to occur about once every 10-100 years	Expected to occur about once every 3 years	Probability of occurrence per operation/ operational hour is less than or equal to $1x10^{-7}$ but equal to or greater than $1x10^{-9}$
Extremely Improbable E	Probability of occurrence per operation/ operational hour is less than $1x10^{-9}$	So unlikely that it can be assumed that it will not occur in an item's life cycle	Unlikely to occur, but possible in system life cycle	Expected to occur less than once every 100 years	Expected to occur less than once every 30 years	Probability of occurrence per operation/ operational hour is less than $1x10^{-9}$

FAA-ATO Safety Risk Matrix

Severity / Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A					
Probable B					
Remote C					
Extremely Remote D					
Extremely Improbable E					*

High Risk
Medium Risk
Low Risk

* Unacceptable with Single Point and/or Common Cause Failures

Risk Classification

- High Risk: Unacceptable Risk
  - Change cannot be implemented unless hazard's associated risk mitigated so that risk reduced to medium or low level
  - Tracking, monitoring, and management are required
  - Hazards with catastrophic effects caused by:
    - Single point events or failures,
    - Common cause events or failures, or
    - Undetectable latent events in combination with single point or common cause events

  are considered high risk, even if possibility of occurrence is extremely improbable

Medium Risk: Acceptable Risk

- Minimum acceptable safety objective
- Change may be implemented but tracking, monitoring, and management are required

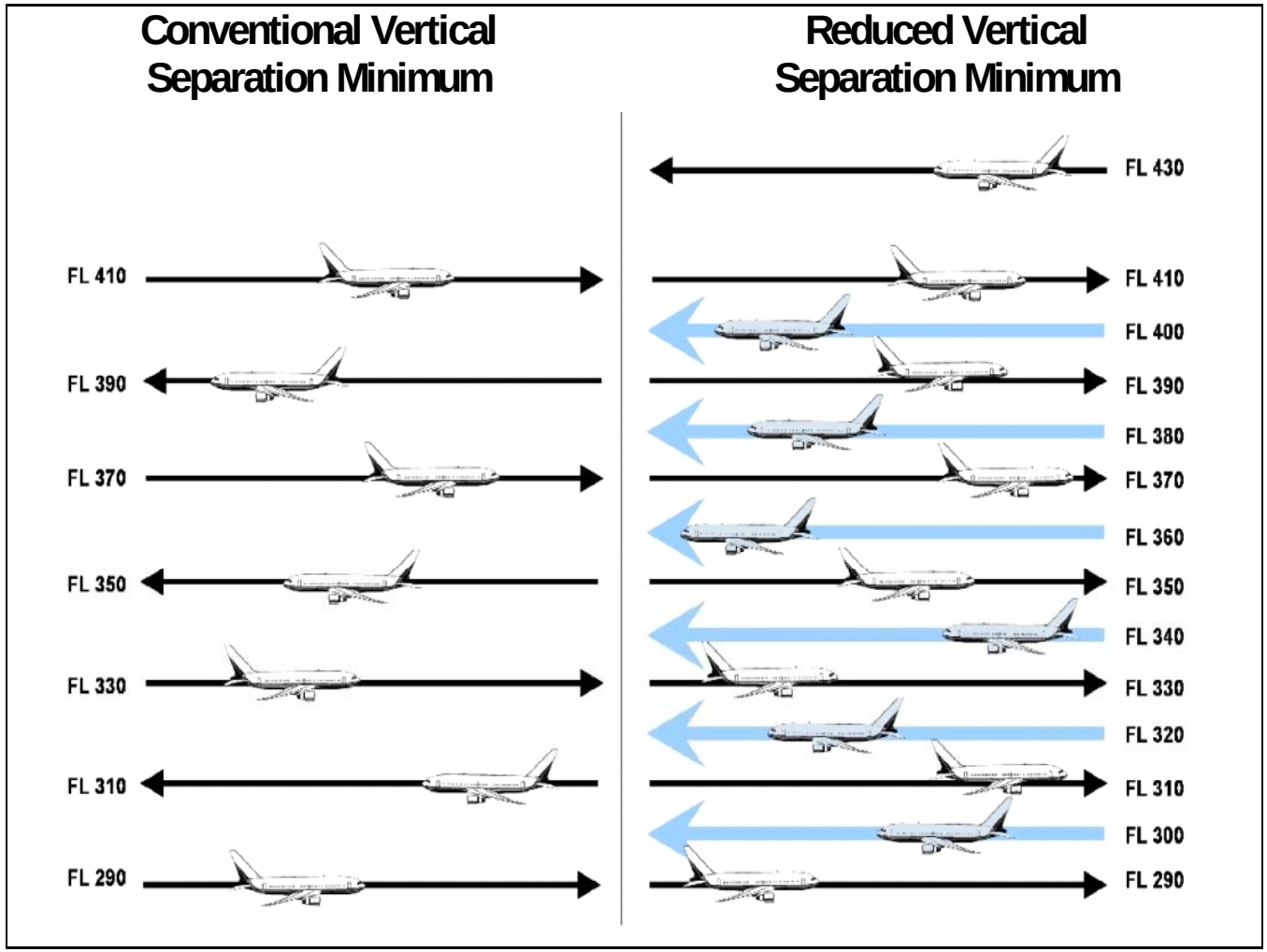
- Low Risk: Acceptable Risk
  - Acceptable without restriction or limitation
  - Hazards not required to be actively managed, but must be documented

Reduced Vertical Separation Minimum

Example-RVSM

- RVSM reduces the vertical separation for FL290 through FL410 from the traditional 2,000-foot minimum to 1,000-foot separation
- RVSM creates exclusionary airspace and only approved aircraft may operate within the stratum.
- This airspace change adds six additional flight levels, which create benefits for Air Traffic Service (ATS) providers and aircraft operators.
- The additional flight levels enable aircraft to safely fly more optimal profiles, gain fuel savings, and increase airspace capacity.

RVSM


Conventional Vertical Separation Minimum
Reduced Vertical Separation Minimum
FL 410
FL 390
FL 370
FL 350
FL 330
FL 310
FL 290
FL 430
FL 410
FL 400
FL 390
FL 380
FL 370
FL 360
FL 350
FL 340
FL 330
FL 320
FL 310
FL 300
FL 290

Risk Analysis

- The feasibility of reducing Vertical Separation Minimum (VSM) above Flight Level (FL) 290, while maintaining an equivalent level of safety, is dependent on operational judgment and a thorough assessment of associated risks.

- The total risk associated with RVSM is a derivative of two factors: the technical risk due to aircraft height-keeping performance and the operational risk due to any vertical deviation of aircraft from their cleared flight levels due to error by the flight crew or Air Traffic Control (ATC).

- The overall collision risk within RVSM airspace is assessed against a Target Level of Safety (TLS) of 5x10-9 fatal accidents per flying hour.

Hazard Analysis

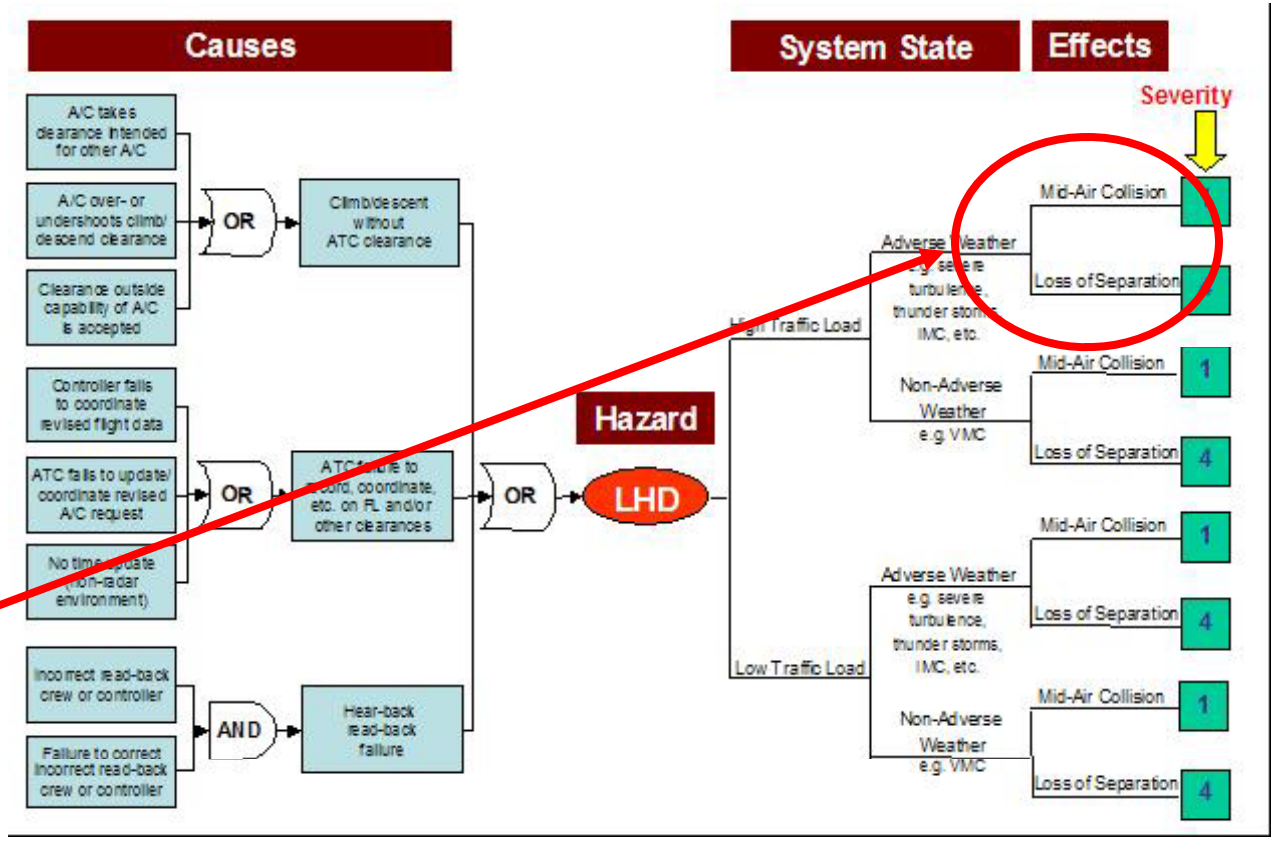
Large Height Deviation Hazard Bow-Tie

- One of the hazards identified for (the implementation of) RVSM is a Large Height Deviation (LHD).

- Any deviation from the assigned or anticipated altitude (that altitude that the controller believes the aircraft to be at, or the pilot believes he/she is to be at, or that the aircraft is climbing or descending to) of 300 feet or greater constitutes a large height deviation.

RVSM Bow Tie

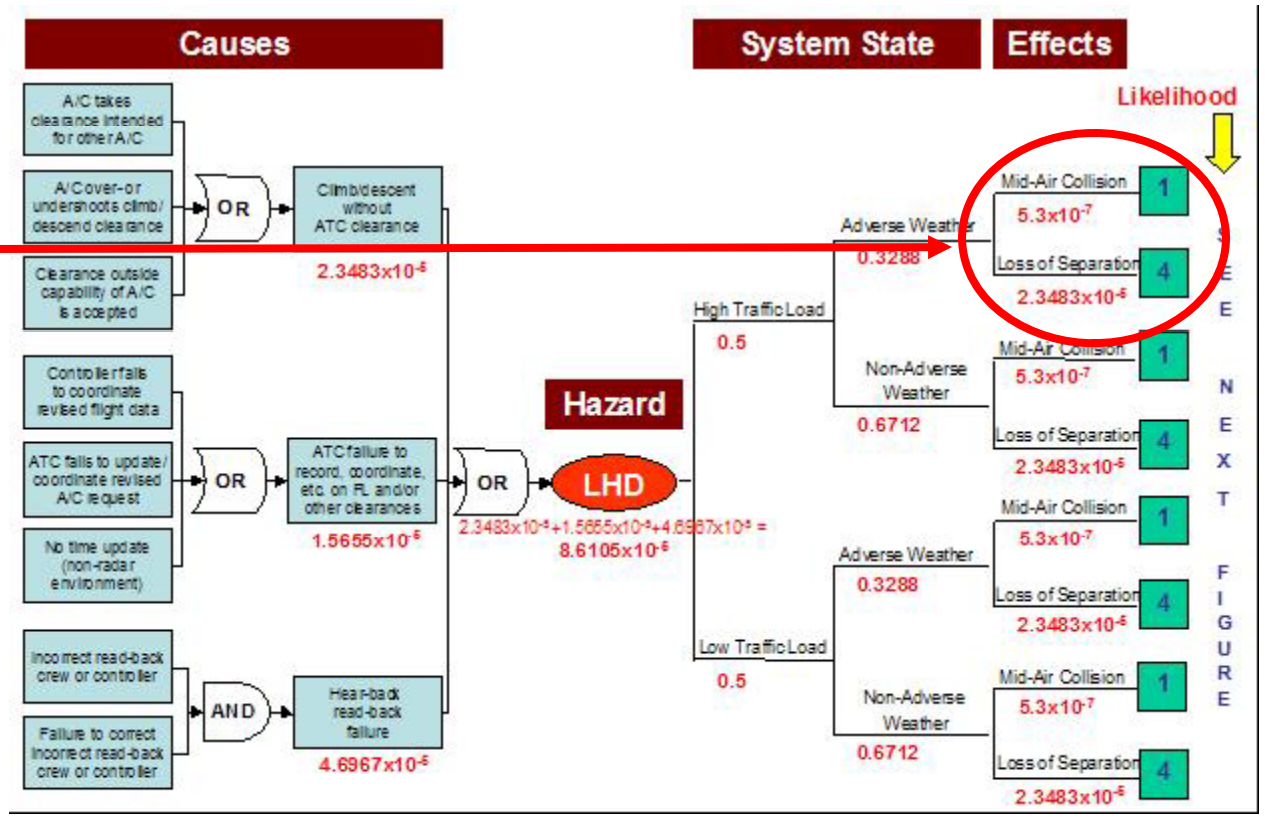
- A simplified overview of the LHD hazard, with some of the high-level causes identified on the left side in rectangles. These causes can then be broken down further into sub-causes. To the right of the hazard, the system states associated with the hazard are identified.
- In essence, Figure I.3 summarizes the two main identified potential outcomes, namely 'Mid-Air Collision' and 'Loss of Separation.' The effects have then been rated for severity in accordance with Table 3.3, indicating four catastrophic potential outcomes and four minor potential outcomes



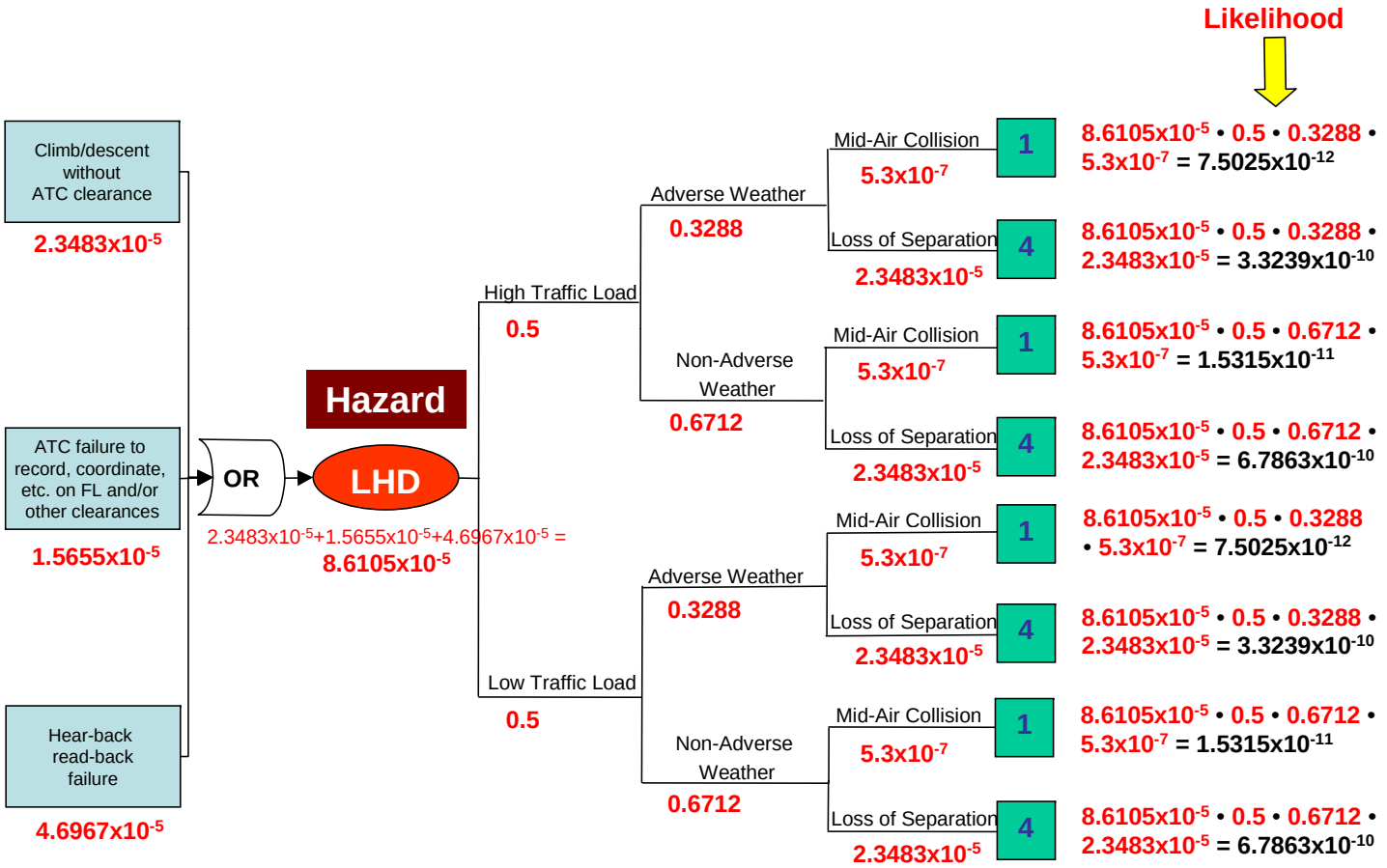
RVSM

- The probability of a Mid-Air Collision in the WATRS Region was extracted from the Safety Risk Management: Worst Credible Outcome Likelihood Values for Mid-air Collisions (MACs) and Controlled Flights into Terrain (CFITs), August 24, 2005, by using the MAC Probability Value in an En Route environment.

- Note: The validity and completeness of (available) data or representative SMEs play a major role in the validity of the calculated likelihoods for the different scenarios.



RVSM

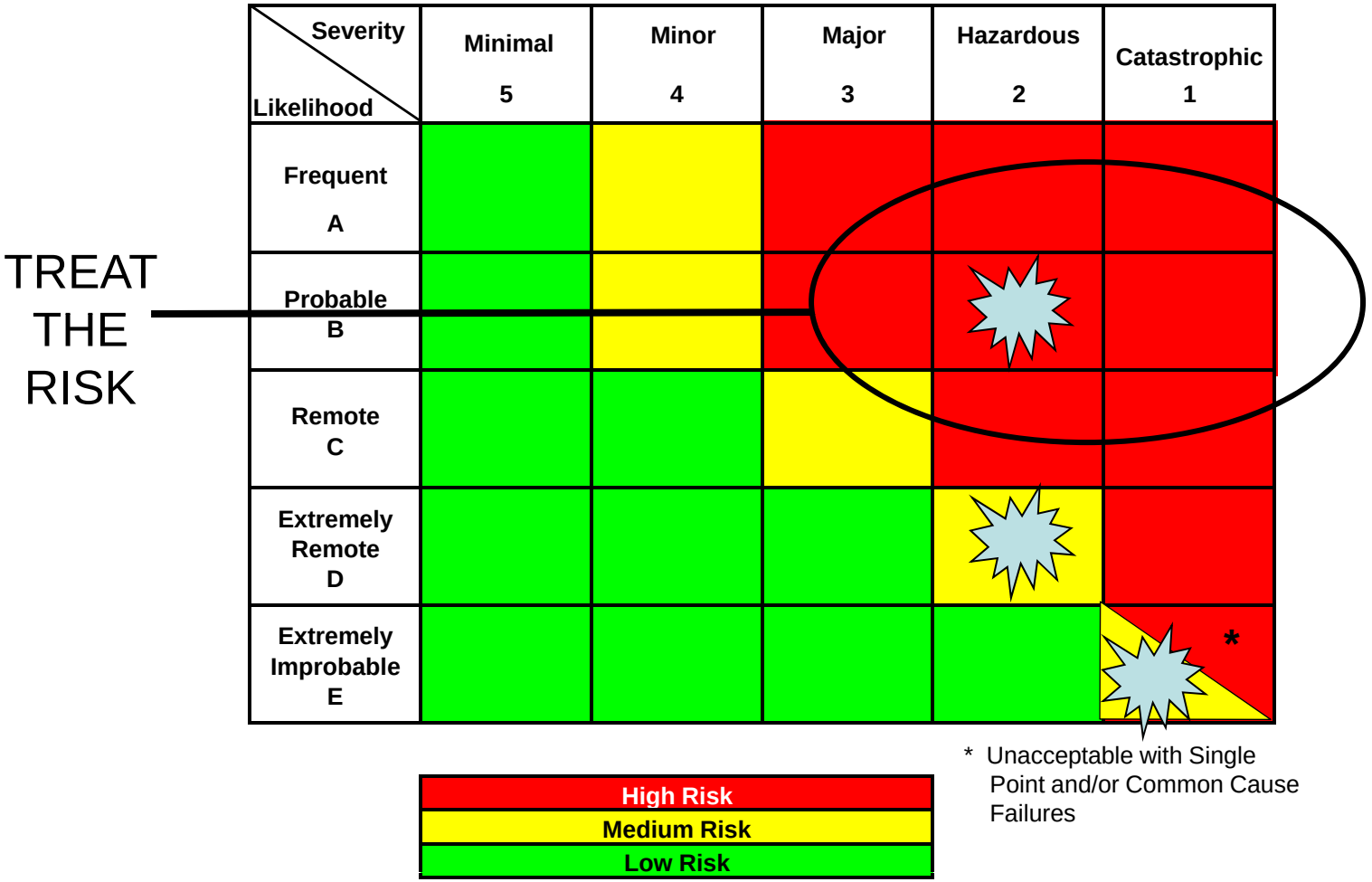

Likelihood
Climb/descent without ATC clearance
2.3483x10-5
ATC failure to record, coordinate, etc. on FL and/or other clearances
1.5655x10-5
Hear-back read-back failure
4.6967x10-5
OR
Hazard
LHD
2.3483x10-5+1.5655x10-5+4.6967x10-5 =
8.6105x10-5
High Traffic Load
0.5
Low Traffic Load
0.5
Adverse Weather
0.3288
Non-Adverse Weather
0.6712
Adverse Weather
0.3288
Non-Adverse Weather
0.6712
Mid-Air Collision
5.3x10-7
Loss of Separation
2.3483x10-5
Mid-Air Collision
5.3x10-7
Loss of Separation
2.3483x10-5
Mid-Air Collision
5.3x10-7
Loss of Separation
2.3483x10-5
Mid-Air Collision
5.3x10-7
Loss of Separation
2.3483x10-5
1
4
1
4
1
4
1
4
8.6105x10-5 • 0.5 • 0.3288 • 5.3x10-7 = 7.5025x10-12
8.6105x10-5 • 0.5 • 0.3288 • 2.3483x10-5 = 3.3239x10-10
8.6105x10-5 • 0.5 • 0.6712 • 5.3x10-7 = 1.5315x10-11
8.6105x10-5 • 0.5 • 0.6712 • 2.3483x10-5 = 6.7863x10-10
8.6105x10-5 • 0.5 • 0.3288 • 5.3x10-7 = 7.5025x10-12
8.6105x10-5 • 0.5 • 0.3288 • 2.3483x10-5 = 3.3239x10-10
8.6105x10-5 • 0.5 • 0.6712 • 5.3x10-7 = 1.5315x10-11
8.6105x10-5 • 0.5 • 0.6712 • 2.3483x10-5 = 6.7863x10-10

Example 0f Documenting Hazard

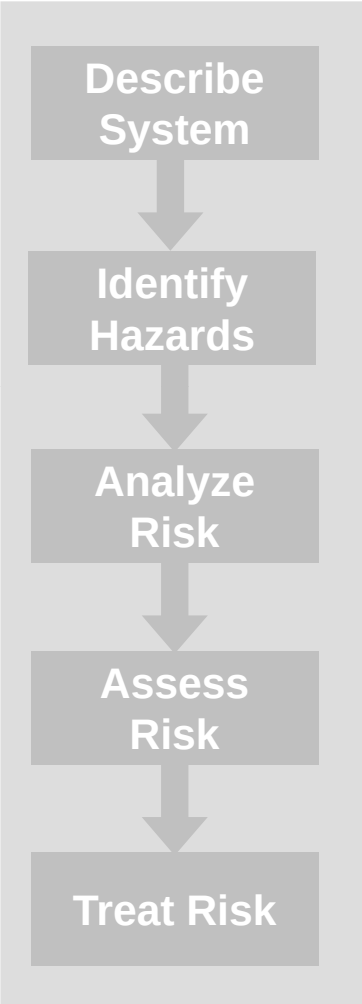
No. & Seg.	Hazard Description	Causes	System State	Existing Controls & Requirements	Possible Effects	Severity/ Rationale	Likelihood / Rationale	Current Risk	Recommended Safety Requirements
H001 S1,S2	Message is misleading to one or more aircraft a. corrupted b. late c. spontaneously generated d. misdirected e. out of sequence S2: f. 4D-Trajectory inconsistent between A/G g. Executed Flight Path is not compliant with the cleared constraints (e.g., incorrectly executed)	The communication system corrupts the message a. Ground user interface failure [F1:HW,SW] b. Ground System Processing failure [F2:HW,SW] --Error checking failure [F2,F6] --Incorrect correlation processing [F2,F6] -- Source data: Incorrect Correlation Data [F2,F6] --Failure to provide update (obsolete info) [F2,F6]	En Route and Terminal airspace DCL issued at surface, potential hazard occurs after takeoff phase High density traffic Instrument Meteorological Conditions (IMC) under Instrument Flight Rules (IFR) conditions Aircraft on a converging or collision course after an initiating failure No credit for ENV upfront	**E1: INITIATING FAILURE CONTROLS** R-P1: System shall comply with RTCA SC-214 CPDLC Operational Safety and Performance Requirements. [F1-F7] R-H1 System shall conform with the FAA Human Factors Design Standard (HFDS) [F1,F2] R-F1: System shall notify the controllers of failures that have an operational impact. [F1,F2] EC-28: Controller procedures exist for determining the position of an aircraft before issuing taxi instructions or takeoff clearance (FAA Order 7110.65 3-1-7. POSITION DETERMINATION). (e))	If the corruption is in a clearance, this could result in the acceptance and execution of an erroneous clearance. Flight crew receives misdirected message A clearance is transmitted and reaches an unintended aircraft. The aircrew does not realize that the clearance is not for them and accepts the clearance. Flight crew does not receive intended message Detected by controller and resolved with tactical (voice) communications, resulting in slight increase in workload. Detected with short time to converging routes, could result in moderate or high operational error.	1 CATASTROPHIC Based on the worst case scenario, if there is Misleading ACL resulting in an erroneous digital ACL msg. and it is undetected by flight crew and ATC during critical phase of flight in IMC conditions, and aircraft trajectory is/remains on conflict path, and conflict is undetected by ATC, and flight crew see & avoid fails, then the outcome could be an aircraft accident resulting in loss of life/serious injury.	E EXTREMELY IMPROBABLE End-to-End error checking algorithm exist, time stamp (PM-CPDLC, FANS1/A+) It is extremely improbable that multiple human and/or system cause and detection errors and traffic geometries will combine to result in an aircraft accident. En route analysis, (ACL)=8,896 transactions per ATSU OP-HR <u>Allocation Representation example</u>: E1= End-to-End initiating failure rate < Remote per msg RTCA OPA CPDLC Failure of integrity = ~1E-6/transaction E7: Either Flight crew or vehicle operator detects and avoids conflict	1E MEDIUM	S2 TBO operations with RTCA ENV-B aircraft counts: PHA-SR-3 The ground automation system shall provide automated conflict detection and resolution in HPA.

EXAMPLE

FAA-ATO Safety Risk Matrix



Treat Risk



- Effectively treating risk involves:
  - Identifying feasible mitigation options
  - Selecting best balanced response
  - Developing risk treatment plans
  - Implementing and verifying
  - Monitoring the hazards to ensure risk levels are achieved

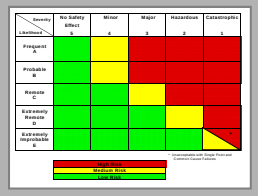
Safety Order of Precedence

Description	Priority	Definition	Example
Design for minimum risk	1	**Design the system (e.g., operation, procedure, or equipment) to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level through selection of alternatives.**	• **If a collision hazard exists because of a transition to a higher Minimum En route Altitude at a crossing point, moving the crossing point to another location would eliminate the risk**
Incorporate safety devices	**2**	**If identified risks cannot be eliminated through alternative selection, reduce the risk via the use of fixed, automatic, or other safety features or devices, and make provisions for periodic functional checks of safety devices.**	• **An automatic "low altitude" detector in a surveillance system** • **Ground circuit in refueling nozzle** • **Automatic engine restart logic**
Provide warning	**3**	**When neither alternatives nor safety devices can effectively eliminate or adequately reduce risk, warning devices or procedures are used to detect the condition and to produce an adequate warning.**	• **A warning in an operator's manual** • **"Engine Failure" light in a helicopter** • **Flashing warning on a radar screen**
Develop procedures and training	**4**	**Where it is impractical to eliminate risks through alternative selection, safety features, and warning devices: procedures and training are used, with management approval for catastrophic or hazardous severity.**	• **A missed approach procedure** • **Training in stall/spin recovery** • **Procedures for loss of communications**

SRM Document (SRMD)

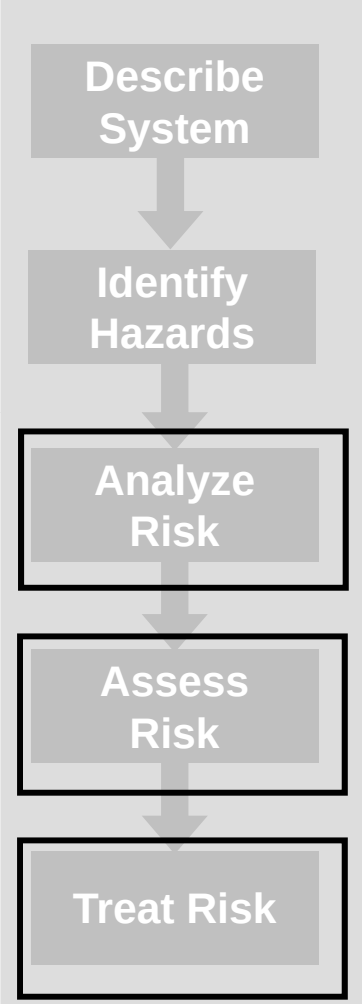
- SRMD defines the proposed change and the SRM process used
- Must be completed for all changes that affect the NAS as defined in the ATO SMS Manual and any change that can affect the safety of the NAS
- Length and depth varies based on type and complexity of change
- Approved SRMD must be retained by change proponent and provided to ATO Office of Safety Services (upon request) and AOV (upon request)
- Updated or changed as project progresses
- Existing risk management documentation may satisfy some SRMD requirements

Risk Acceptance

 Safety Risk	Initial High Risk*	Medium or Low Initial Risk
	Risk Accepted by:	**Risk Accepted Within:**
Stay Within a Service Unit	Service Unit VP	Service Unit
Span Service Units	Each Affected Service Unit VP	Each Affected Service Unit
Affect LOBs Outside the ATO (e.g., ARP and/or AVS)	Each Affected Service Unit VP and Each Associate Administrator	Each Affected Service Unit and LOB

* Please note that initial high risk must be mitigated to medium or low before acceptance

Hazard Tracking and Risk Resolution



- Ensuring requirements and mitigations for initial medium and high risk hazards are implemented
  - Defining additional safety requirements
  - Verifying implementation
  - Reassessing risk to ensure hazard meets risk level requirement and assessment

- ATO requires organizations to formally identify all hazards, and track and monitor all initial medium and high risk hazards for the lifecycle of the system or change, or until they mitigate the risk to low

SRMTS

- **The Safety Risk Management Tracking System (SRMTS) is a web-based comprehensive tool housed on the ATO Portal for the tracking of SRM efforts, hazards, risk mitigations and monitoring the predicted residual risk.**

SRMTS allows users to:

- Improve tracking of SRM efforts, hazards and the predicted residual risk
- Provide a centralized document repository for SRM documentation
- Automate hazard analyses
- Improve efficiency of the application of SRM
- Improve reporting capabilities and trends analysis

PHA

STATURE

Bobby Miller | Default Study Group: Default Study Group (bmiller) | Tuesday, May 4, 2010 | Hide Tabs | Logout

Home | Studies | SRMTS | Admin. Console | Application Design Studio | Help

Groups & Folders | Templates | Baselines | Back to 'OPS_e and Oceanic Services_Policy/Procedure_Policytest3_1696_1.0'

85% | Export

PHA:

Project Title: OPS_e and Oceanic Services_Policy/Procedure_Policytest3_1696

Additional Project Information

Detailed Description Of Project:

Related URL:

Order/Policy:

Attachments:

Operational Objective / Intention Capability:

Provide Preflight Functions:

Hazard Name	Cause	System States	Existing Controls		Effects	Initial Risk						Safety Requirements			Predicted Residual Risk				Monitoring Activities	Frequency	Duration	Performance Measures
			Existing Controls	Justification/Supporting Data		Severity	Severity Rationale	Likelihood	Likelihood Rationale	Initial Risk	Single Point Failure	Safety Requirement	Safety Order Of Precedence	Organization responsible for implementing safety requirements	Severity	Likelihood	Predicted Residual Risk	Single Point Failure				
Policy hazard 1	some	1. ok	this control	this justification	1. some effect	1-Catastrophic	sev rat	B-Probable	like rat	1B		safety requirement	Provide Warning	William Laberis	5-Minimal	B-Probable	5B	No	Do some monitoring	Daily	1 Day	Perform measure the monitorir

Done | Internet

SMS Implementation Lifecycle - Future