

SAFETY PLANNING FOR THE MULTI-STANDARD ENVIRONMENT

Jim Gibbons

james.m.gibbons@boeing.com

(610) 591-8813

Objectives

- Understanding not all standards are standard
 - Varying focus / varying methods
- Working in multiple standards
 - Defining the primary
 - Setting a path forward
- Conclusions

What is standard?

- All standards are not created equal
- Prescriptive versus Performance
 - Objectives vice requirements
- Consensus versus Regulatory
 - Commercial versus state operated aircraft
 - Acceptably safe vice compliantly safe

Standards

REGULATORY STANDARDS

Enacted into law by governing agencies
CFR -14 – FAA regulations (NFPA 70- NEC)



Consensus Standards

Standards agreed to by a consensus group of stakeholders developed within guidelines for standards and include public comment period
SAE / NAS / RTCA standards



Company or Industry Standards

Standards or processes used in a given company or industry with no outside input
BAC Specs



Why Standards?

- Standards become a means of defining acceptable risk
- Consensus standards can become regulatory if enacted by law (e.g. NFPA 70; NEC, NFPA 100; Life Safety Code)
- Not following consensus or company standards demonstrates you did not follow “reasonable industry practice”, therefore, you’ve accepted the liability

Risk Acceptance Approach

MIL-STD-882

- Identify Hazards
- Assess Residual Risk
- Accept risk at appropriate level
- Safety Center as independent opinion

Civil Approach

- Define acceptable risk
- Prove System compliance to acceptable risk
- DER as independent expert

UK Approach

- Identify Hazards
- Assess Risk
- “Argue” residual risk is as low as reasonably practicable (ALARP)
- Hired 3rd party as independent Auditor

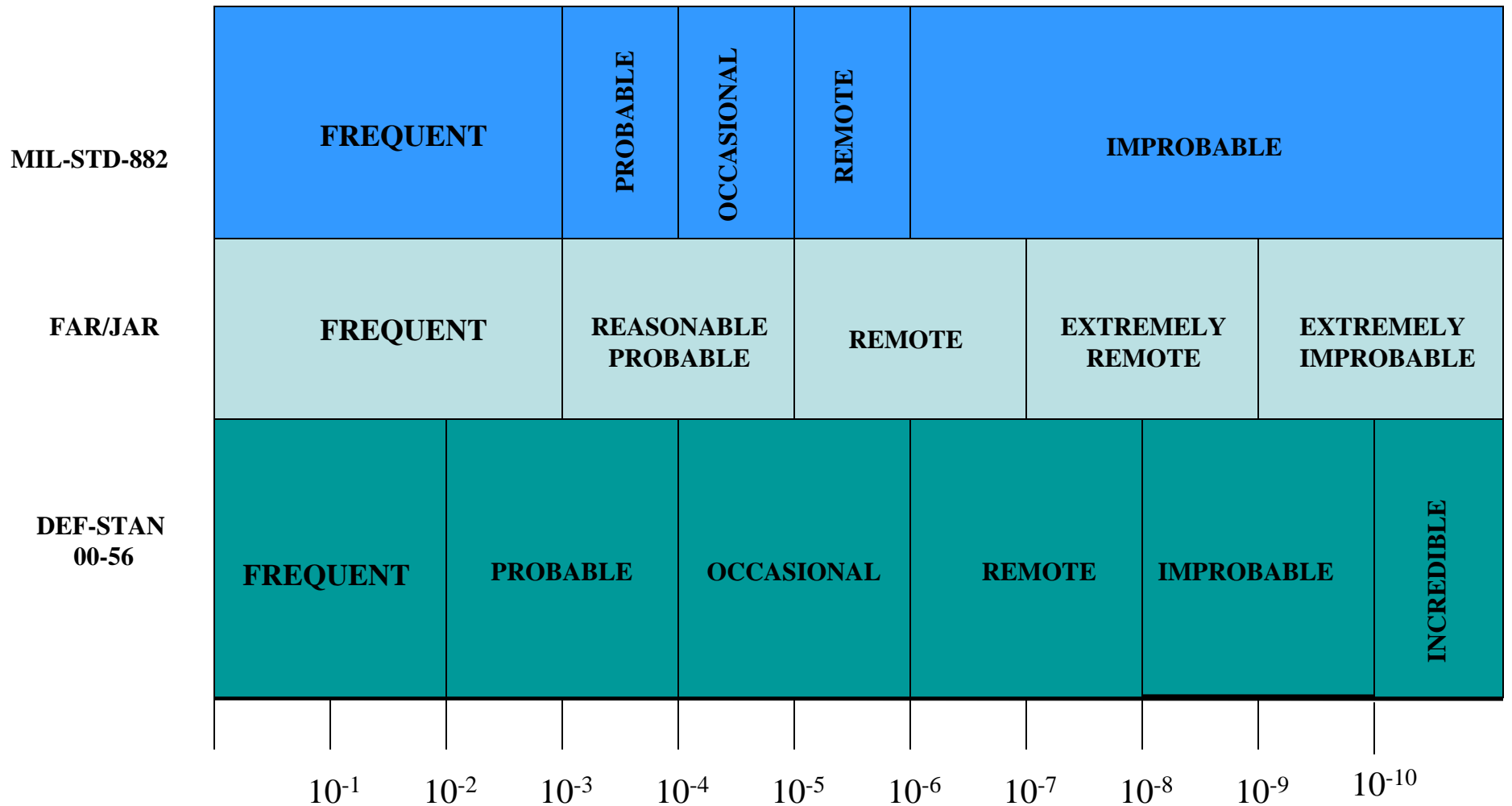
Guiding Documents for this Presentation

- US Military
 - MIL-STD-882 System Safety Practice
 - Various Software Standards (i.e 2167, 498)
- Commercial
 - ARP 4761 / DO-178B
- UK Standards
 - DEF STAN 00-55 & 00-56

Many commonalities – many differences
Approach & emphasis

Severities				
MIL-STD-882D	Negligible	Marginal	Critical	Catastrophic
Equip / Environ	\$2k>10k	\$10K>200K	\$200k>1M	>\$1M
Injury	<1 lost workday	1+ lost workdays	Perm Partial Disability or 3 pers hospitalized	Perm total disability or death
FAA	Minor	Major	Severe Major	Catastrophic
JAA	Minor	Major	Hazardous	Catastrophic
	Slight reduction in safety margin - Increased workload - inconvenience to some occupants	significant reduction in safety margins or functional capabilities - significant increase in crew workload - some discomfort to occupants	Large reduction in safety margins or capabilities - higher workload or distress effecting crew reliability to perform task - adverse effect on occupants	All failure conditions which prevent continued safe flight and landing
DEF STAN 00-56 (Issue 2)	at most a minor injury or occupational illness	A single severe injury and/or multiple minor injuries or occupational illnesses	Single Death and/or multiple severe injuries or occupational illness	Multiple Deaths

QUANTATIVE PROBABILITY LEVELS

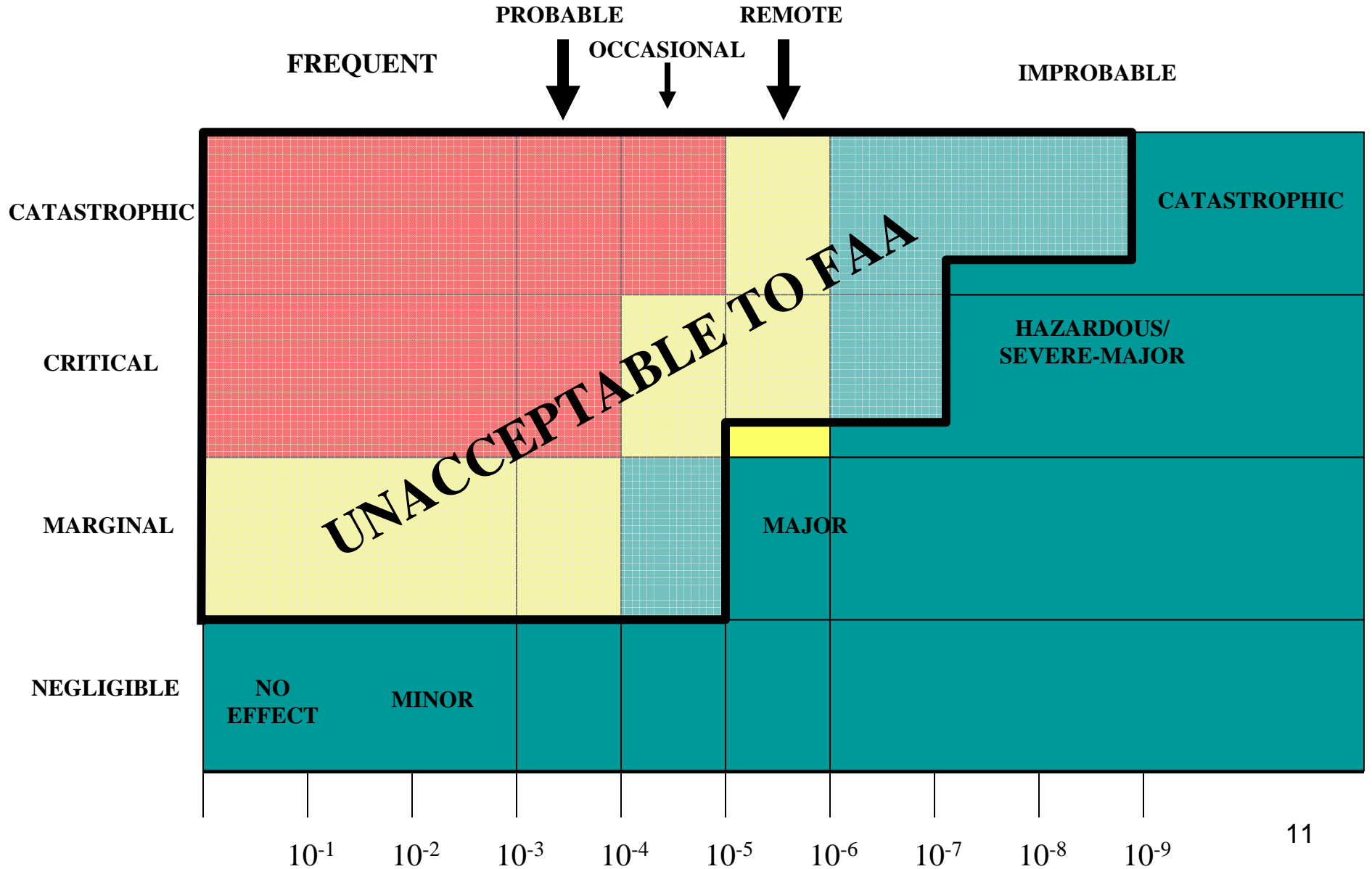


Qualitative Probabilities

	MIL-STD -882		DEF-STAN 00-56 (issue 2)
	Item	Fleet	
Frequent	Likely to occur frequently	Continuously experienced	Likely to be continuously experienced
Probable	Will occur several times during the lifecycle	Will occur frequently	Likely to occur often
Occasional	Likely to occur sometime during the lifecycle	Will occur several times	Likely to occur several times
Remote	Unlikely, but possible to occur during the lifecycle	Unlikely, but reasonably expected to occur	Likely to occur some time
Improbable	So unlikely, assume hazard not experienced	Unlikely to occur, but possible	Unlikely, but may be exceptionally occur
Incredible			Extremely unlikely that the event will occur at all given the assumptions recorded about the domain of the 10 system

Military versus Commercial Acceptance Matrix

NAVAIR 5100.11



MIL-STD* versus DEFSTAN Acceptance Matrix

Probabilities	1.00E-01	1.00E-02	1.00E-03	1.00E-04	1.00E-05	1.00E-06	1.00E-07	1.00E-08	1.00E-09
MIL-STD-882D	Frequent	Probable	Occasional	Remote	Negligible				
Fleet Item	Continuously experienced	Frequently	Several times	Unlikely, but reasonably expected	Unlikely, but possible				
	Often likely	Several times	Likely sometime	Unlikely but possible	So unlikely it may not be experienced				
ARP-4761									
JAA	Frequent	Reasonably Probable	Remote	Extremely Remote	Extremely Improbable				
FAA	Probable	Improbable	Extremely Improbable						
DEF STAN 00-56									
Probability/operating hr	Frequent	Probable	Occasional	Remote	Improbable				

MIL-STD-882D		Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13	
Probable	2	5	9	16	
Occasional	4	6	11	18	
Remote	8	10	14	19	
Improbable	12	15	17	20	
		1 through 5	High	Component Acquisition executive	
		6 through 9	Serious	Program Executive Officer	
		10 through 17	Medium	Program Manager	
		18 through 20	Low	As directed	

DEF STAN 00-56		Catastrophic	Critical	Marginal	Negligible
Frequent	A	A	A	B	
Probable	A	A	B	C	
Occasional	A	B	C	C	
Remote	B	C	C	D	
Improbable	C	C	D	D	
Incredible	C	D	D	D	
Class A	Intolerable				
Class B	Undesirable, and shall only be accepted when risk reduction is impractical				
Class C	tolerable with endorsement of the Project Safety Review Committee				
Class D	tolerable with the endorsement of the normal Review Projects				

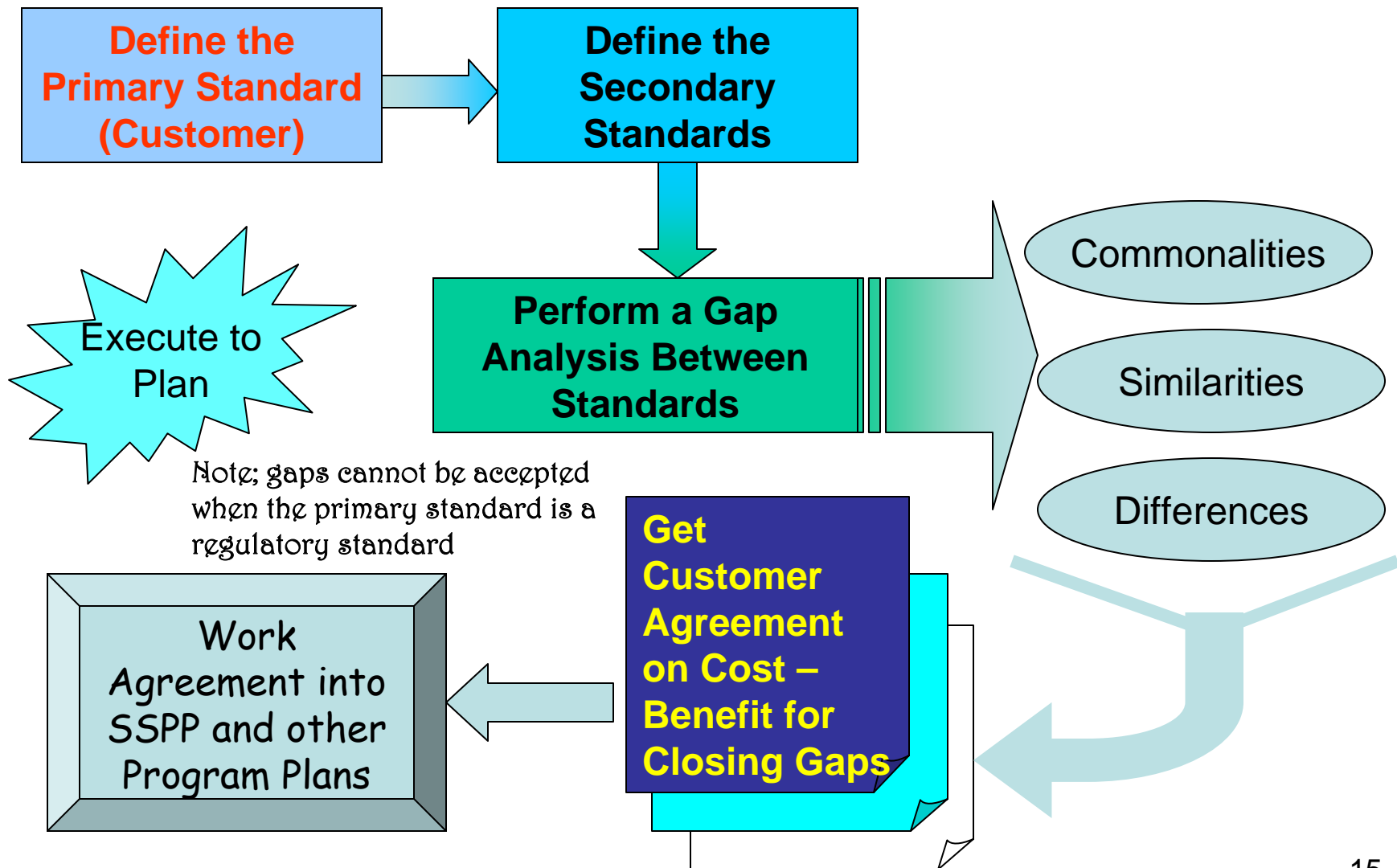
Software Safety Requirements - Military vs. Commercial

	Military	Commercial
System Safety / Risk Mngmt	MIL-STD-882	FAA / TSO/ FAR Compliance Certification
		ARP 4761 Guidelines for Safety Assessment...
Software Development	MIL-STD-498 MIL-STD-2167 (tailored to item)	DO-178 (to level indicated by functional safety analysis)
Oversight	SSWG / DCMA	Independent Auditors

What's This All Mean?

- Risk are measured differently by the various standards even though their terminology may be the same.
- Customer and practitioner experts in each standard will question risk assessments (& credibility) when presented in another scale
- Consider multi-risk measure tracking in your hazard database
 - Keep your primary system active as the risk to be fully processed IAW the standard
 - Add a “reference only” RAC to track the assessed risk per the secondary standard(s)
 - This additional effort will have a near term pay-off in reduced explanation and justification times in the program lifecycle
 - Reports can be customized to match evaluator preference

The Standards Mixing Bowl



Conclusions

- All standards require defining residual risk
- Civil Standards are Pass/Fail compliance
- Military standards recognize the increased risk associated with their operations and evaluate risk versus benefit
- All require documentation

Final Thoughts

- The objectives have many common elements
- Think about how your programs typically design systems – a different standard may only require additional signatures and reviews to satisfy other programs
- **COMMUNICATE** – you may be separated by a common language