Understanding and Applying Total Risk Summing

Mr. Bill Edmonds, Mr. Tom Pfitzer,
Mr. Bob Baker, Mr. Pat Clemens, Ms. Melissa Emery

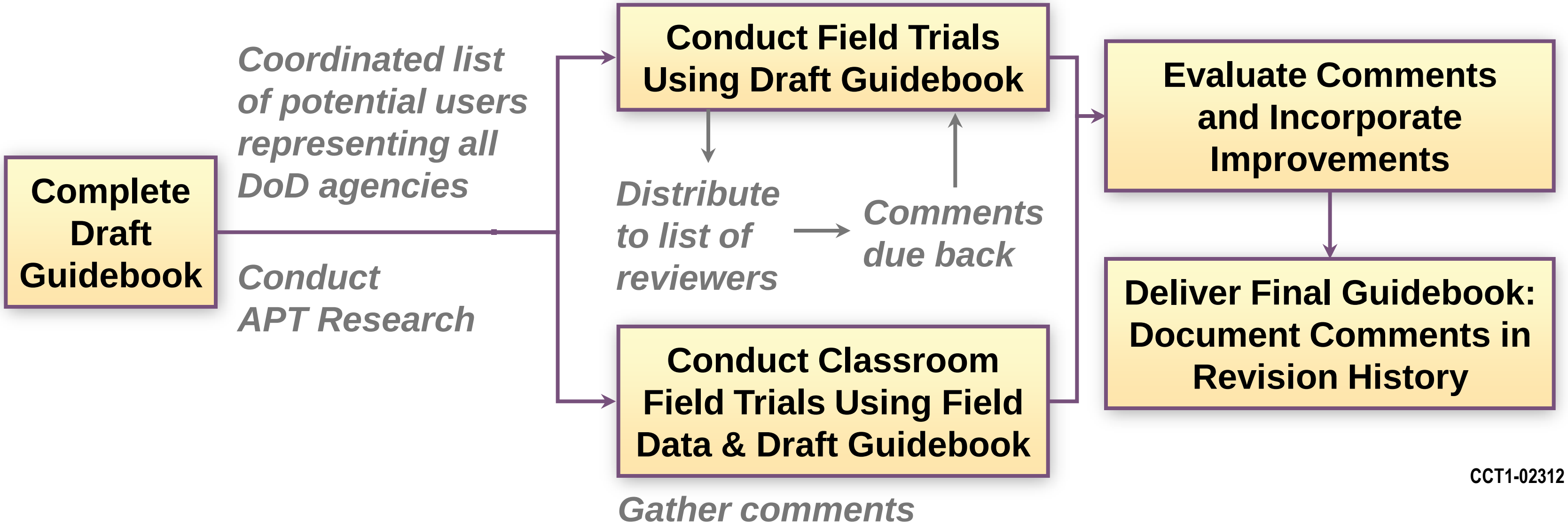
August 2012

Background and Intro

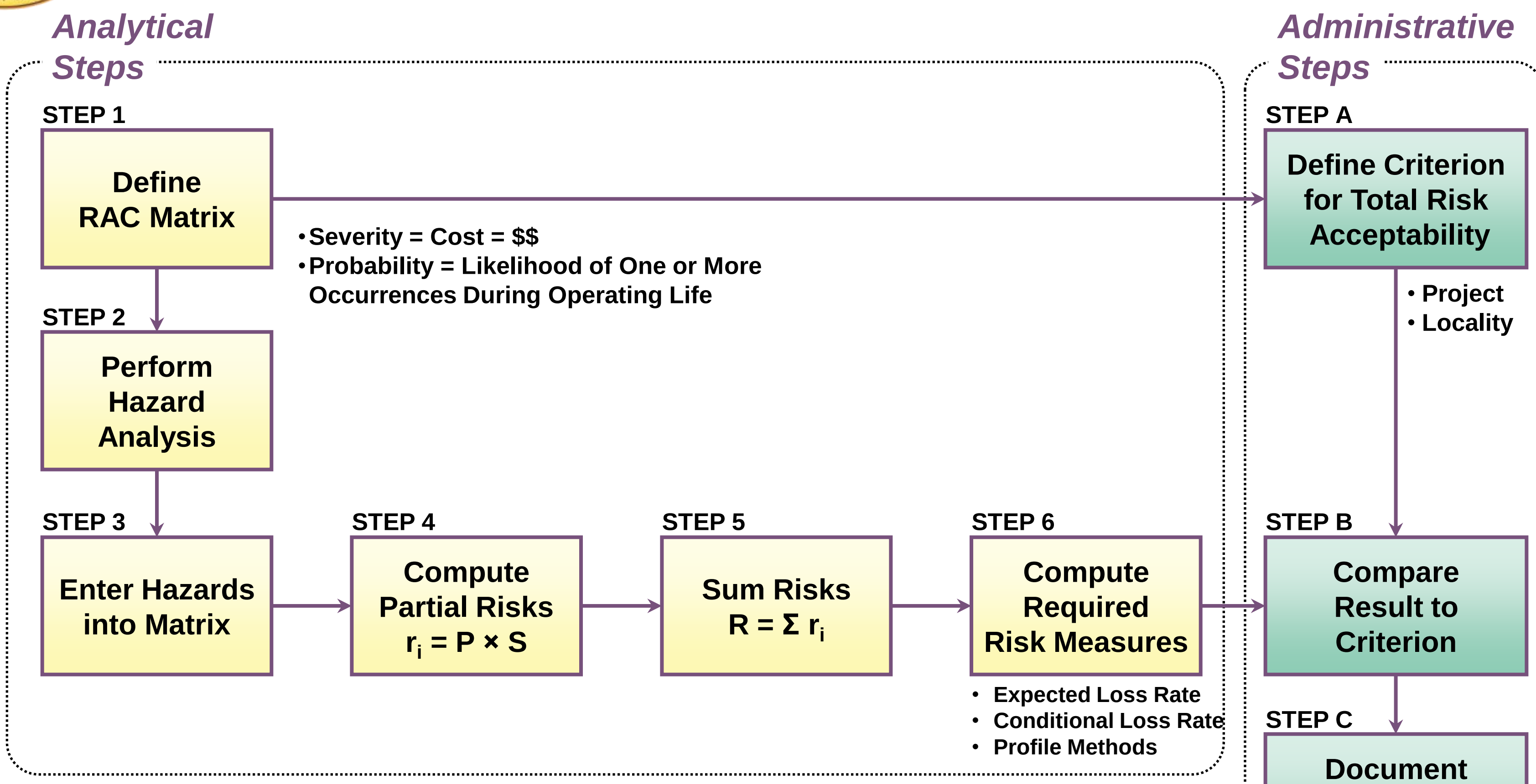
ATP TF Initiative: Develop a Risk Summing Guidebook on summing subjectively analyzed partial risk to produce a whole-system risk representation on which informed risk acceptance judgments can be made by DoD programs.

- » Enhance overall risk management process
- » Provide guidance in evaluating overall system risk by summing partial risks
- » Produced Guidebook in 2010
  - > The DSOC website where you can find the risk summing guidebook is located at (CAC enabled only): https://prext.osd.mil/RFM/readiness/dsoc/TF/ATP/Guidance/Forms/AllItems.aspx
  - > APT Website www.apt-research.com

Risk Summing Guidebook Development



Major Steps in Risk Summing Methodology



Haz ID	Short Title	Sev. Cat	Prob. Cat	Sev. Value	Prob. Value	Partial Risk, $$	Notes
A1.1	Exposure to heat/cold	2	D	$ 300,000	2.14E-04	$ 64	1
A1.2	Exposure to Toxics	1	E	$ 10,000,000	1.37E-06	$ 14	
A2.1	Loss of Breathable Air	1	D	$ 2,000,000	[illegible]	[illegible]	
B3.7	Crushing by dropped mass	2	[illegible]	[illegible]	[illegible]	[illegible]	
[illegible]8.4							

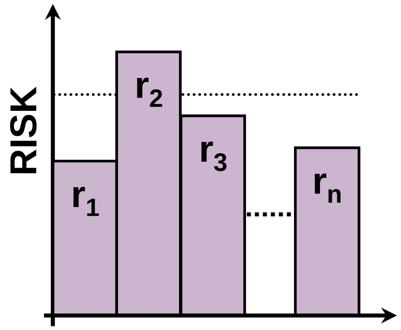
A Major Subjective Analysis Shortfall…

All "Line-Item Inventory" hazard analysis/risk assessment methods * suffer this shortfall:

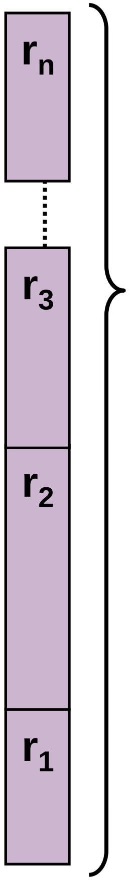
THE ANALYTICAL CONSTRUCT

Hazards	Severity	Probability	Risk
h_1	s_1	p_1	r_1
h_2	s_2	p_2	r_2
h_3	s_3	p_3	r_3
⋮	⋮	⋮	⋮
h_n	s_n	p_n	r_n

THE ANALYST'S VIEW OF SYSTEM RISK



REAL WORLD SYSTEM RISK



$$R_T = \sum (s_1 \times p_1) + (s_2 \times p_2) + (s_3 \times p_3) + \ldots (s_n \times p_n) +$$

RISK SUMMATION METHODS ARE NEEDED!

Examples:

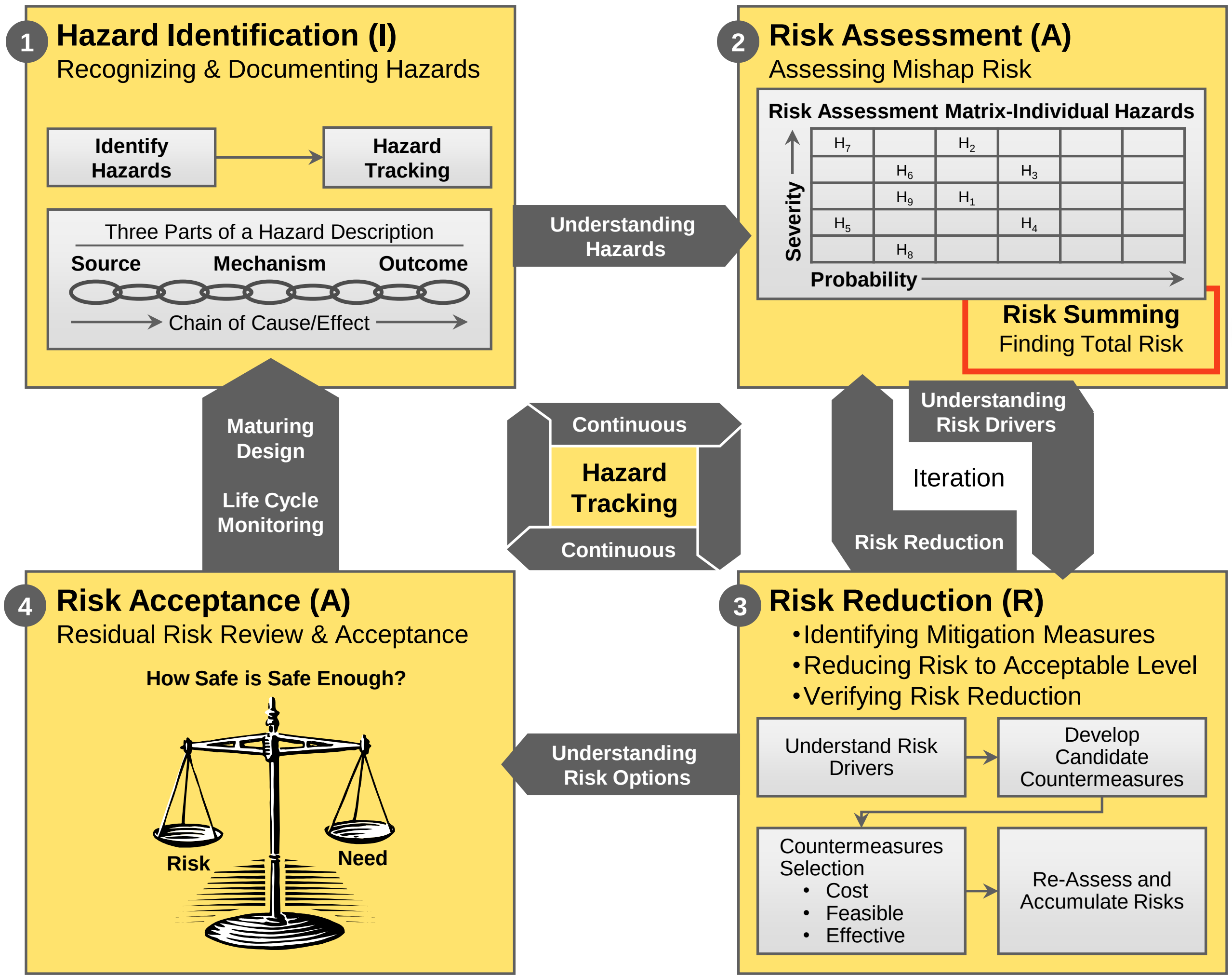
Preliminary Hazard Analysis
Failure Modes and Effects Analysis
Functional Hazard Analysis

Concept and Justification

» Items to be Covered:
- > When to Sum
- > The Need
- > Addressing the Need
- > The Risk Summing Equation
- > Assumptions for Use

When Should We Sum?

A Rational Summing Point…



System Risk should be summed at initial Risk Assessment and should be adjusted at final Risk Reduction.

The Need

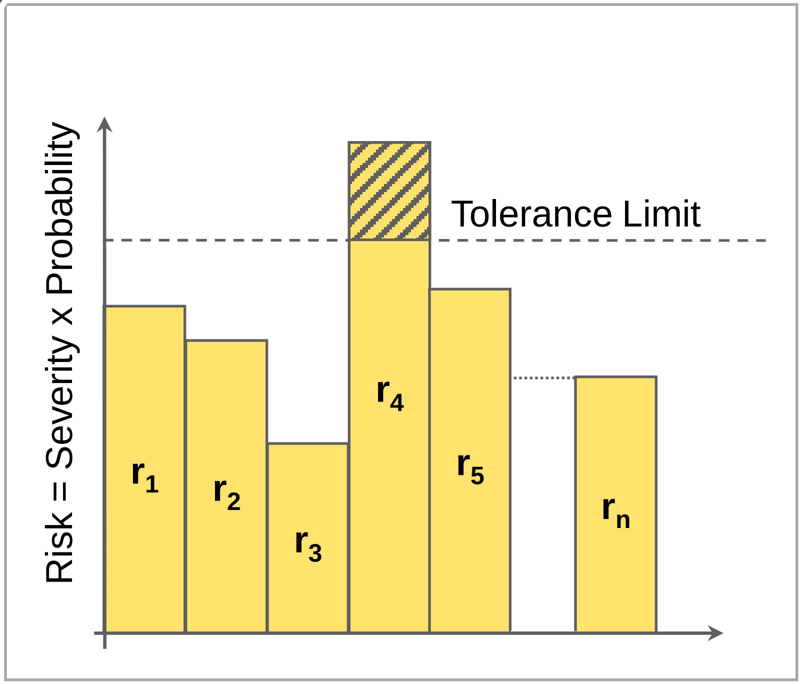
2 Problems Exist

Individual hazards are inventoried. Their risks are assessed.

Hazard No.	Description	Severity s_i	Probability p_i	Risk r_i
1		IV	C	III / C
2		III	C	IV / C
3		IV	D	IV / D
4		I	B	I / B
5		II	E	II / D
n	?	?	?	?

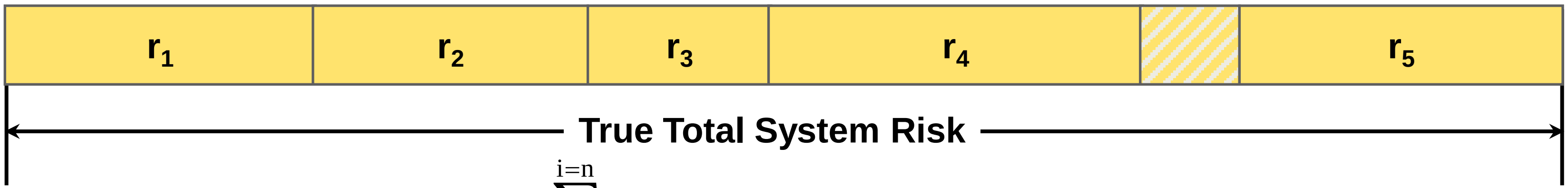
How much Total Risk does this System pose?

Leading to a hypothetical result Modeled by this paradigm.

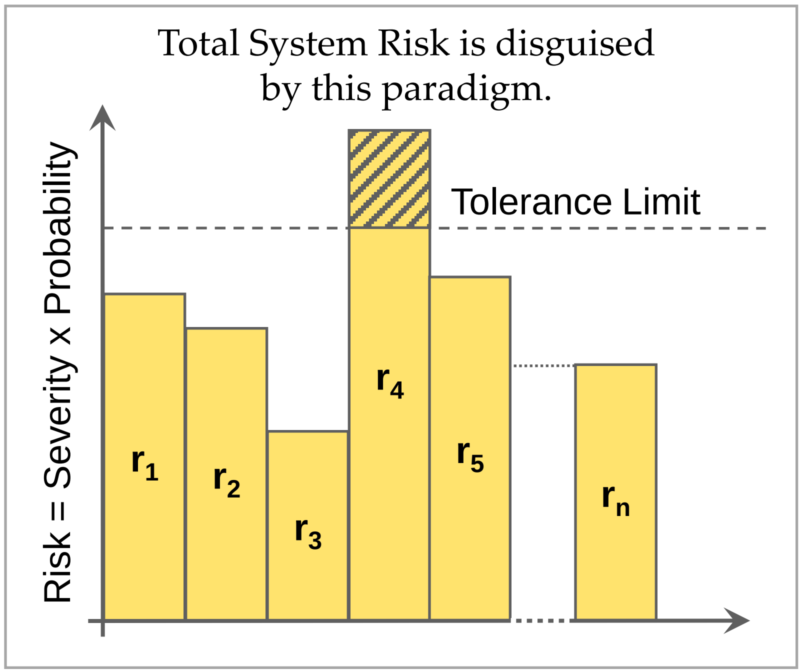


1. Crafty practitioners can break r_4 into subsets where the piece parts are all tolerable. Risk summing removes this temptation.
2. Risk for Hazard No. 4 exceeds the Tolerance Limit, requiring mitigation costing, e.g. ≈ $437K, just less than the Program funding limit.

The Need (cont.)



$$R_T \approx \sum_{i=1}^{i=n} r_i = r_1 + r_2 + r_3 + r_4 + r_5 \ldots + r_n \; *$$



Risk for Hazard No. 4 exceeds the Tolerance Limit, requiring mitigation costing e.g. ≈ $437K, just less than the Program funding limit.

True Total Risk

Because the identified hazards are statistically independent,** their risks simply sum. The resulting paradigm appears as an end-to-end display.

Conundrum

A cost analysis shows that risk for hazard r_1 can be eliminated for ≈ $22K. Note that r_1 greatly exceeds the excess risk of r_4. Conventional practice requires that the excess risk for hazard r_4 must be abated.

---

* Expressed as a rare event approximation.

** No single hazard causes nor is caused by another.

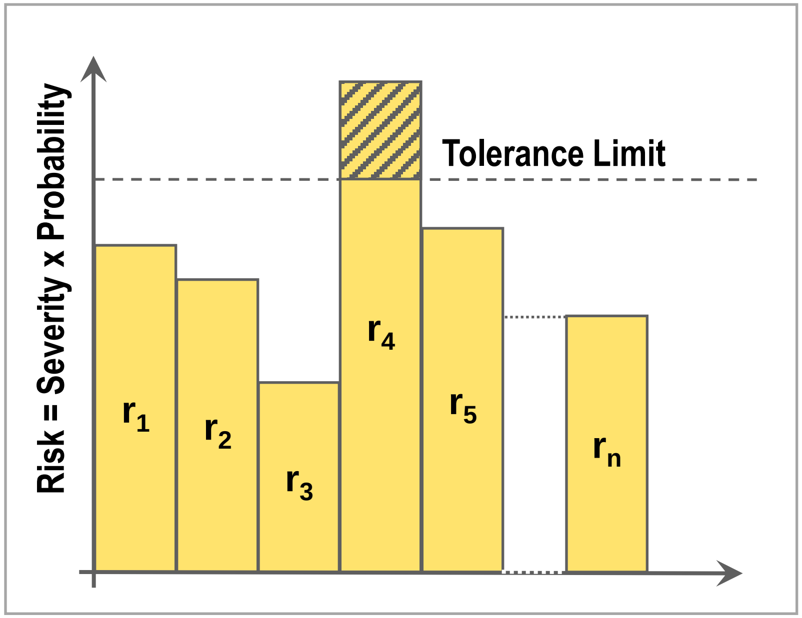
Addressing the Need…

Consult with the Risk Acceptance Authority

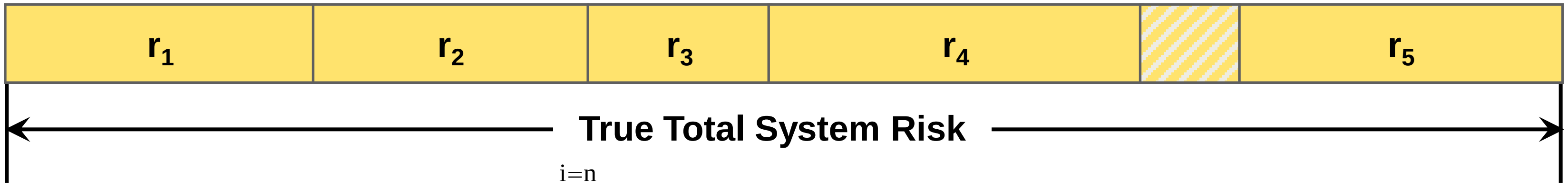
> The problem is *NOT* one to be resolved by the system safety analyst alone!

Some Aspects to Consider

- Do we think differently if r_4 is "severity rich" than if it is "probability rich?"
- Can the enterprise *survive* a one-time "hit" by the hazard r_4?
- What trade-offs are available? …e.g., cost vs Δ risk for r_2, r_3, and r_5. "Go" for greatest risk decrement per dollar outlay?



Risk for Hazard No. 4 requires mitigation costing, e.g. ≈ $437K, just less than the Program funding limit; r_1 can be eliminated for $22K.



$$R_T \approx \sum_{i=1}^{i=n} r_i = r_1 + r_2 + r_3 + r_4 + r_5 \ldots + r_n \; *$$

* Expressed as a rare event approximation.

The Complete Expression……

$$R_T \approx \sum_{k=1}^{k=n} \sum_{j=1}^{j=m} \sum_{i=1}^{i=l} (r_{ijk} = s_{ijk} \times p_{ijk})$$

where:

R_T = the total risk posed by all identified hazards to all threatened assets during the system's complete life cycle.

s_{ijk} = severity of the injury/damage that the i^{th} identified hazard may produce in the j^{th} asset under threat during the k^{th} mission phase under consideration.

p_{ijk} = the probability that the consequence described by s_{ijk} is produced in the specified asset by the specified hazard during the specified mission phase.

r_{ijk} = the partial risk posed by the i^{th} identified hazard to the j^{th} asset under threat during the k^{th} mission phase under consideration.

* The expression shown here is used throughout in the interest of simplicity. Its use produces a numerical result that is very slightly larger in value – i.e., pessimistic – when compared to an exact solution. Such substitutions, often used in system safety practice, are known as "rare event approximations."

Assumptions for Totaling System Risk

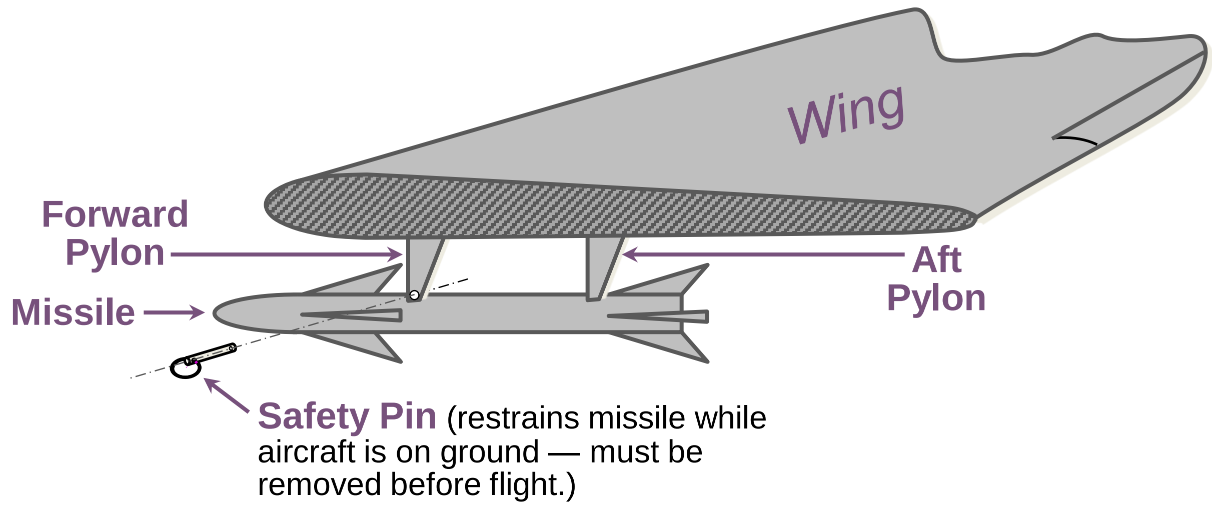
» For Subjective Totaling

- System hazards are statistically independent.
- Subjective judgments of Severity and Probability take on numerical values at mid-spans of designated cells.
- Mid-span matrix cell values are logarithmic averages of extreme values (not arithmetic averages).
- All probability declarations are for the same, declared exposure interval.
- If hazards evaluated are not statistically independent, summing of risks may produce a pessimistic result.

Demonstrating the Method

The Fast Asp™ Missile Adapted to the Sea-Chèvre Aircraft

Fast Asp™ Missile on Pylons at Wing Station



STEP 1 — Define RAC Matrix

STEP 2 — Perform Hazard Analysis

STEP 3 — Enter Hazards into Matrix

STEP 4 — Compute Partial Risks $r_i = P \times S$

STEP 5 — Sum Risks $R = \Sigma r_i$

STEP 6 — Compute Required Risk Measures

Step 1: The RAC Matrix*… (typical)

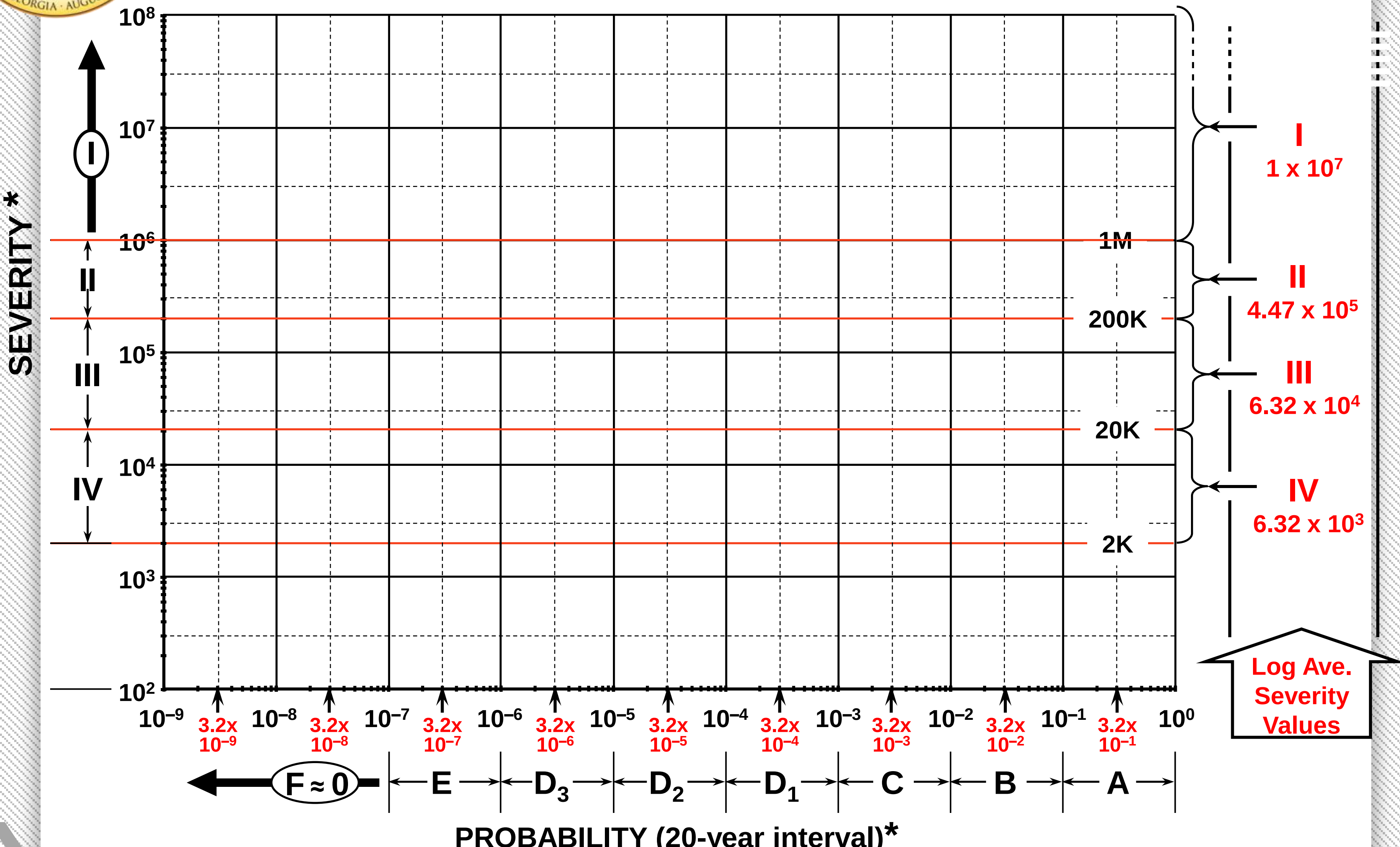
Severity of Consequences				Probability of Mishap**					
Category / Descriptive Word	Personnel Injury / Illness	Equipment Loss $	Down Time	F Impossible	E Improbable	D Remote	C Occasional	B Probable	A Frequent
I Catastrophic	Death	>1M	>4 Mo						
II Critical	Severe Injury or Severe Illness	200K to 1M	4Wks to 4Mo						
III Marginal	Minor Injury or Minor Illness	20K to 200K	1 Day to 4Wks						
IV Negligible	No Injury or Illness	<20K	<1 Day						
V None	None	None	None						

*Adapted from MIL-STD-882D

**Life Cycle: Personnel: 20 yrs / Others: 120 missions/sorties

Risk Code/ Action			
1	Imperative to suppress risk to lower levels		
2	Operation requires written, time-limited waiver, endorsed by managing authority		
3	Operation permissible		

The Matrix, as Scaled for Fast Asp Application



*Matrix and scales adapted from MIL-STD-882D

Step 2: Perform Hazard Analysis

Background

The Royal Frambesian Navy is updating the Mk-2 Sea Chèvre aircraft weapons inventory to include the Fast Asp™ missile, to be launched from Sea Chèvre wing pylons. Certification requires system safety analyses for aircraft-missile interfaces.

Operation

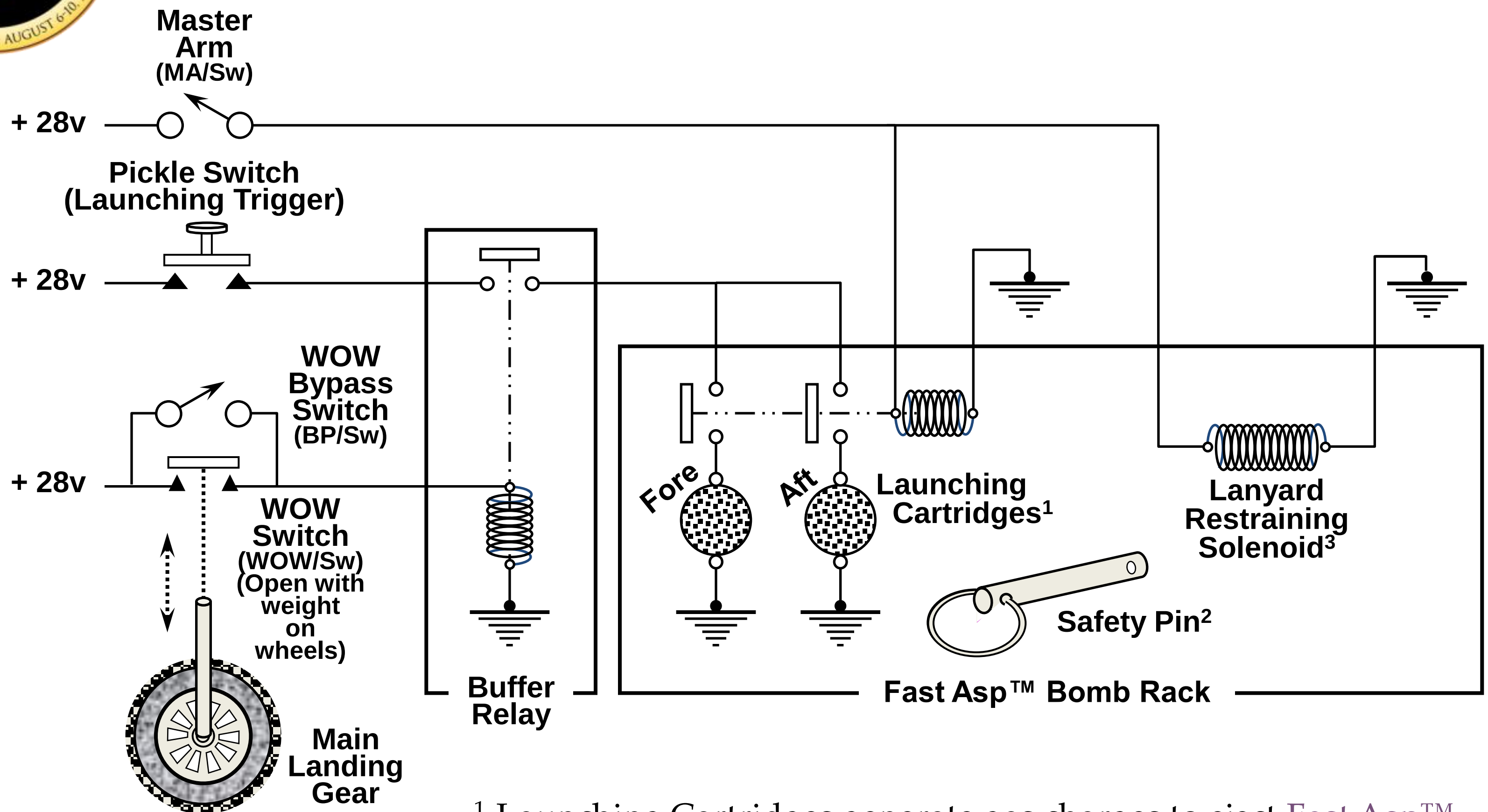
To fire a missile:

1. The Master Arm Switch must be selected "ON." This…
   - enables the pilot's Pickle Switch (i.e., the "trigger").
   - enables missile-launching gas generator cartridges on fore and aft Missile Mounting Pylons.
   - energizes a missile-arming Lanyard Restraining Solenoid, increasing lanyard anchor tension.
2. The pilot must execute the "FIRE" command by actuating the Pickle Switch (i.e., the "trigger").

Potential Loss Events of Concern

- Missile release on the ground is considered a "Catastrophic" outcome.
- Failure to arm the missile when fired is considered a mission failure — i.e., a "Critical" hazard, based on $750K missile replacement cost.
- Other than a normal firing signal, Electromagnetic Environmental Effects (E^3) from external sources may initiate a missile "FIRE" command.

System Schematic…



[1] Launching Cartridges generate gas charges to eject Fast Asp™ missile from Sea-Chèvre wing mounting pylons.

[2] Manually installed Safety Pin restrains missile while aircraft is on ground — must be removed manually before flight.

[3] Solenoid, activated by Master Arm Switch, restrains missile arming lanyard, pulling it free from missile at launch to arm missile.

Preliminary Hazard List…

Potential Hazards

1. Uncommanded Missile Release on Ground
2. Hung Missile ("Hangfire,"/unknown missile state)
3. Failure to Release Missile on "FIRE" Command
4. Failure to Jettison Missile on Command
5. Jettisoned Missile is Armed
6. Live Launch Fails to Arm
7. WOW Bypass Left in Place

A Preliminary Hazard Analysis has been performed for these hazards.

Preliminary Hazard Analysis…

HAZARD DESCRIPTION	TARGET	S	P*	RAC	ADDITIONAL COUNTERMEASURES	S	P*	RAC
Uncommanded release of missile from wing pylon on ground, resulting in mass fire/explosion.	Personnel Equipment Downtime	I I II	C D D	1 2 3	1. Add level of formal, independent, sign-off, Safety Pin and WOW Bypass Switch inspections with "REMOVE BEFORE FLIGHT" banners (P/W). NOTE: Verify adequacy of countermeasures by Fault Tree Analysis.	I I II	E E E	3 3 3
Hung missile in unknown state: mission aborted for that missile; uncommanded release now more probable; downloading now more hazardous.	Personnel Equipment Downtime	I I III	C D D	1 2 3	1. Test/inspect launch system on ground w/dummy missile each 3 sorties (P). 2. Provide safe recovery area for hung-stores aircraft (S/P). 3. Verify valid Launching Cartridge dates (P).	I I III	E E E	3 3 3
Failure to release missile on FIRE command; potential loss of missile and aircraft (Pilot may eject).	Personnel Equipment Downtime	I I II	C D D	1 2 3	1. Countermeasure 1 for Hazard 2 (P). 2. Test/verify electrical ARM and FIRE functions with dummy loads during missile installation (P). 3. Add level of formal, independent, sign-off, Safety Pin inspections (P). 4. Train pilot in hi-G "pull-up," maneuver (P).	I I II	E E E	3 3 3
Failure to release missile on JETTISON command; potential for recovery with damaged aircraft and ordnance on board.	Personnel Equipment Downtime	I I III	D E E	2 3 3	1. Countermeasure 1 for Hazard 1 to ensure Safety Pin withdrawn (P). 2. Countermeasure 1 for Hazard 2 (P).	I I III	E E E	3 3 3
Arming of jettisoned missile with potential for impact on inhabited area, causing collateral damage.	Personnel Equipment Downtime	I I III	E E E	3 3 3	1.Test/verify Lanyard Restraining Solenoid tension during ARM and FIRE function test (P)[1]. 2. Redesign Master Arm circuit to "open" (disable) on jettison command (E)[1]. [1]Optional; risk acceptable as-is.	I I III	E E E	3 3 3
Failure of live launch to arm, resulting in missile failure and loss of missile.	Personnel Equipment Downtime	I I II	C D D	1 2 3	1. Countermeasure 1 for Hazard 2 (P). 2. Countermeasure 1 for Hazard 5 (P).	I I II	E E E	3 3 3

Failure Modes and Effects Analysis…

ITEM ID	FAILURE MODE	FAILURE CASE	FAILURE EFFECT	TARGET	S	P*	RAC	ACTION REQUIRED	S	P*	RAC
WOW Switch Contacts (WOW/Sw)	Open w/close command	1. Debris lodged in contacts 2. Arcing residue 3. Mechanical failure of contact spring	1. Lost launch-on-command capability 2. Potentially compromised jettison capability	Personnel Equipment Downtime	I I II	D E E	2 3 3	1. Test/inspect each 3 sorties(P). 2.Replace switch after 60 sorties (P).	I I II	E E E	3 3 3
WOW Switch Contacts (WOW/Sw)	Closed w/open command	1. Overcurrent welding 2. Arcing (Over amps) 3. Mechanical failure of contact spring	1. Potential for inadvertent launch on ground (MA and Pickle protect)	Personnel Equipment Downtime	I I II	D E E	2 3 3	1. Test/inspect each 3 sorties (P). 2.Replace switch after 60 sorties (P).	I I II	E E E	3 3 3
WOW Bypass Switch Contacts (BP/Sw) (Manual Toggle)	Open w/close command	1. Debris lodged in contacts 2. Arcing residue 3. Mechanical failure of contact spring	1. Ground tests of launch components compromised.	Personnel Equipment Downtime	I I II	D E E	2 3 3	1. Test/inspect each 3 sorties (P). 2.Replace switch after 60 sorties (P).	I I II	E E E	3 3 3
WOW Bypass Switch Contacts (BP/Sw) (Manual Toggle)	Closed w/open command	1. Overcurrent welding 2. Arcing (Over amps) 3. Mechanical failure of contact spring	1. Potential for inadvertent launch on ground (MA and Pickle protect)	Personnel Equipment Downtime	I I II	D E E	2 3 3	1. Test/inspect each 3 sorties (P). 2.Replace switch after 60 sorties (P).	I I II	E E E	3 3 3
WOW Buffer Relay Contacts	Open w/close command	1. Debris lodged in contacts 2. Arcing residue 3. Mechanical failure of contact spring	1. Lost launch-on-command capability 2. Potentially compromised jettison capability	Personnel Equipment Downtime	I I II	D E E	2 3	1. Test/inspect each 3 sorties (P). 2.Replace relay after	I I	E E	3 3
WOW Buffer Relay Contacts	Closed w/open command	1. Overcurrent welding 2. Arcing (Over amps) 3. Mechanical failure of contact spring	1. Potential for inadvertent launch on ground (MA and Pickle protect)	Personnel Equipment Downtime	I I II	D E E					
WOW Buffer Relay Coil	Open w/voltage applied	1. Burnout from prior use	1. Ground tests of launch components compromised.	Personnel Equipment Downtime	I I II	D E E		60 sorties (P).			

A Failure Modes and Effects Analysis has been performed for the WOW assembly.

Failure Probability Data…

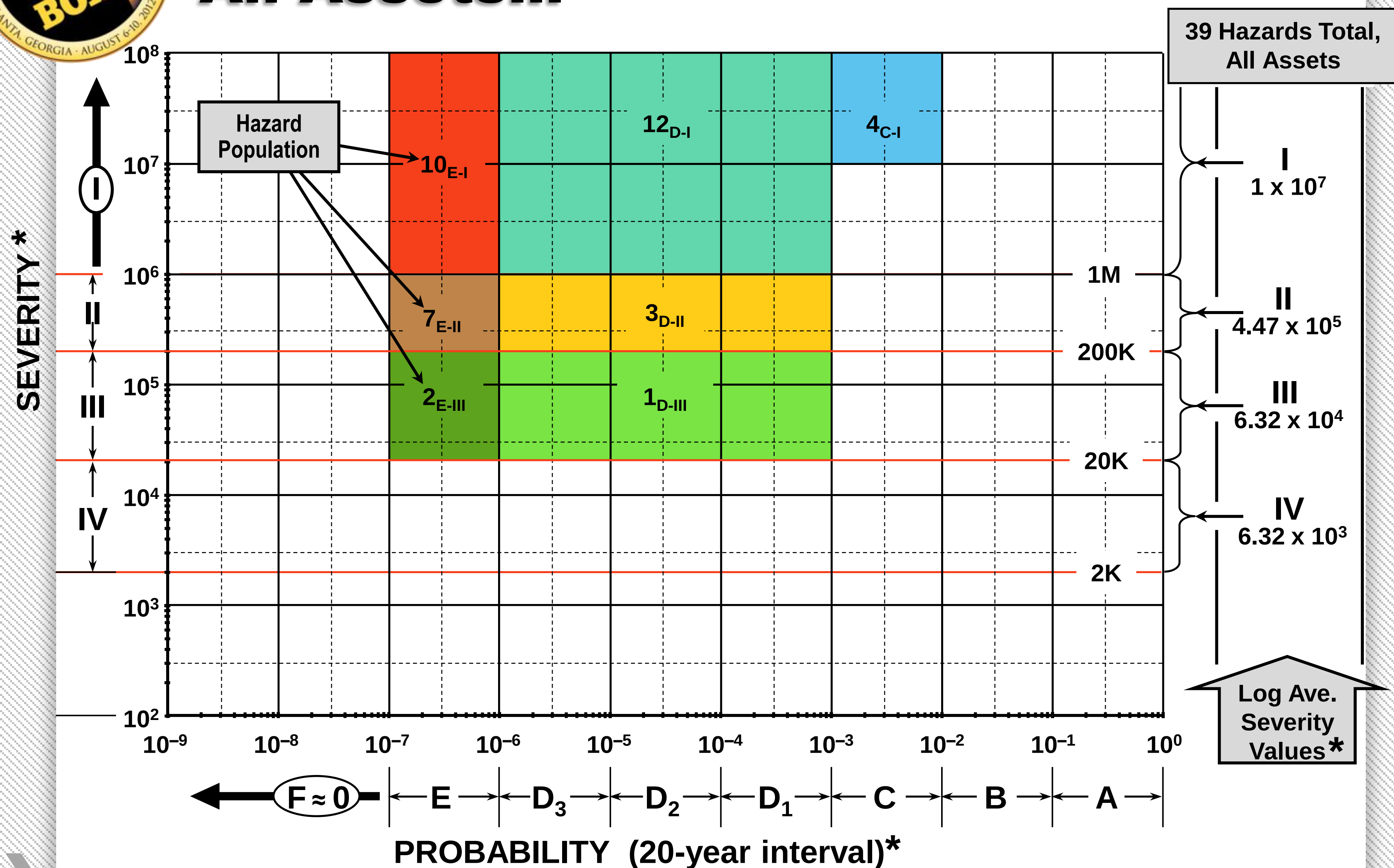
Tag / Item	Probability*	Source	Comments
1 / E3 Stimulus (off-board sources)	3.0×10^{-6}	Engineering estimate, basis: compliance with MIL-STD-464 for pyrotechnic no-fire threshold protection of <16.5 dB	MIL-STD-464: Fast Asp™ complies
2 / Master Arm "ON" (MA/Sw)	3.0×10^{-3}	Risk Analysis Report to the Rijnmond Public Authority, D.Reidel Publishing Co., 1981 ISBN 90-277-1393-6 / [Log 446]	General human error of commission
3 / Pickle Asserted	3.0×10^{-3}	Risk Analysis Report to the Rijnmond Public Authority, D.Reidel Publishing Co., 1981 ISBN 90-277-1393-6 / [Log 446]	General human error of commission
4 / WOW Switch Faults Closed (WOW/Sw)	1.0×10^{-3}	WASH 1400 (NUREG-75/014), Appendix III; US Nuclear Regulatory Commission, October 1975 / [Log 1053]	"…high" probability rating from source is used here
5 / WOW Bypass Switch Faults Closed (BP/Sw)	1.0×10^{-3}	WASH 1400 (NUREG-75/014), Appendix III; US Nuclear Regulatory Commission, October 1975 / [Log 1053]	"…high" probability rating from source is used here
6 / WOW Buffer Relay Faults Closed	1.36×10^{-6}	IEEE Std 500 [Log 3.2.6.1]	Contacts fault closed in prior use
7 / Bypass Sw Installer Error	1.8×10^{-2}	Risk Analysis Report to the Rijnmond Public Authority, D.Reidel Publishing Co., 1981 ISBN 90-277-1393-6 / [Log 442]	"Improper connection of mechanical linkage"
8 / Bypass Sw Installer Supervisor Error	3.0×10^{-3}	Reliability and Maintainability in Perspective, 3rd Edition, D.J. Smith, 1988 ISBN 0-333-46205-X / [Log 454]	"Failure of visual inspection for defined criterion"
9 / Independent Bypass Sw Inspector Error**	1.0×10^{-1}	Reliability and Maintainability in Perspective, 3rd Edition, D.J. Smith, 1988 ISBN 0-333-46205-X / [Log 460]	"Fail to recognize incorrect status on inspection"
10 / Pin Installer Error (Pin not fitted)	1.8×10^{-2}	Risk Analysis Report to the Rijnmond Public Authority, D.Reidel Publishing Co., 1981 ISBN 90-277-1393-6 / [Log 442]	Improper connection of mechanical linkage
11 / Pin Installer Supervisor Error	3.0×10^{-3}	Reliability and Maintainability in Perspective, 3rd Edition, D.J. Smith, 1988 ISBN 0-333-46205-X / [Log 454]	"Failure of visual inspection for defined criterion"
12 / Independent Pin Inspector Error**	1.0×10^{-1}	Reliability and Maintainability in Perspective, 3rd Edition, D.J. Smith, 1988 ISBN 0-333-46205-X / [Log 460]	"Fail to recognize incorrect status on inspection"

Step 3: Enter Hazards into Matrix

A	B	C	D	E	F
Haz ID	Short Title	Sev. Cat	Prob. Cat	Sev. Value	Prob. Value
PHA1-P	Uncommand Release - Personnel	I	C	$ 10,000,000	3.20E-03
PHA1-E	Uncommand Release - Equip	I	D	$ 10,000,000	3.20E-05
PHA1-D	Uncommand Release - Down	II	D	$ 447,000	3.20E-05
PHA2-P	Hung Missile - Personnel	I	C	$ 10,000,000	3.20E-03
PHA2-E	Hung Missile - Equip	I	D	$ 10,000,000	3.20E-05
PHA2-D	Hung Missile - Down	III	D	$ 63,200	3.20E-05
PHA3-P	Fail on FIRE - Personnel	I	C	$ 10,000,000	3.20E-03
PHA3-E	Fail on FIRE - Equip	I	D	$ 10,000,000	3.20E-05
PHA3-D	Fail on FIRE - Down	II	D	$ 447,000	3.20E-05
[illegible]	Fai[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]A5-E	[illegible] Buffer Open [illegible] E - E[illegible]	[illegible]	[illegible]	$ 10,[illegible]	3.20E-0[illegible]
FMEA5-D	WOW Buffer Open on CLOSE - Down	II	E	$ 447,000	3.20E-07
FMEA6-P	WOW Buffer on OPEN - Personnel	I	D	$ 10,000,000	3.20E-05
FMEA6-E	WOW Buffer on OPEN - Equip	I	E	$ 10,000,000	
FMEA6-D	WOW Buffer on OPEN - Down	II	E	$ 447,000	
FMEA7-P	WOW Buffer Coil OPEN with Volt - Pers	I	D	$ 10,000,000	
FMEA7-E	WOW Buffer Coil OPEN with Volt - Equip	I	E	$ 10,000,000	
FMEA7-D	WOW Buffer Coil OPEN with Volt - Down	II	E	$ 447,000	

I	1.00E+07
II	4.47E+05
III	6.32E+04
IV	6.32E+03
A	3.20E-01
B	3.20E-02
C	3.20E-03
D	3.20E-05
E	3.20E-07

Initial Fast Asp Risk Distribution -- All Assets...



*Matrix and scales adapted from MIL-STD-882D

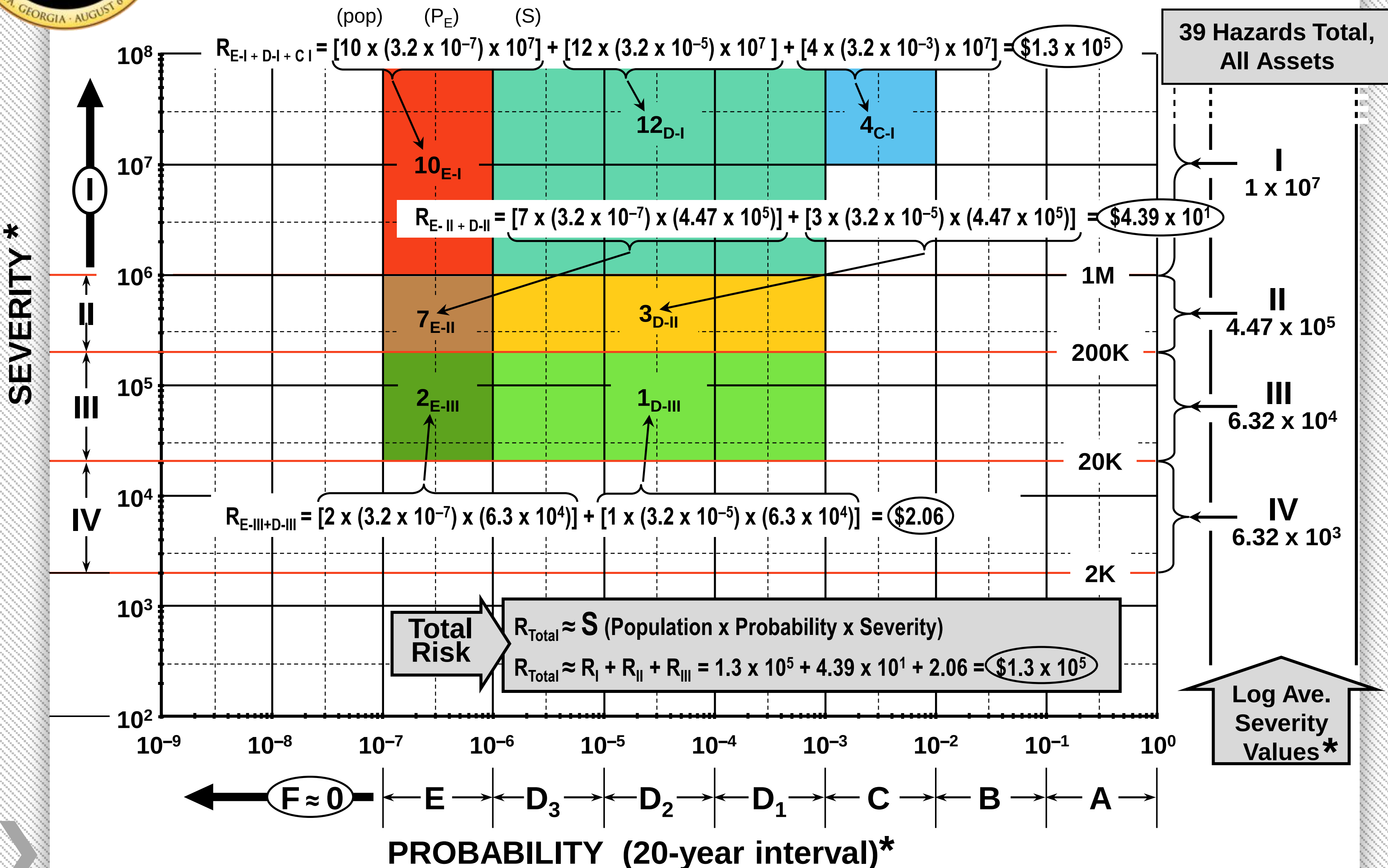
Step 4: Compute Partial Risks

A	B	C	D	E	F	G
Haz ID	Short Title	Sev. Cat	Prob. Cat	Sev. Value	Prob. Value	Partial Risk, $$
PHA1-P	Uncommand Release - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00
PHA1-E	Uncommand Release - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00
PHA1-D	Uncommand Release - Down	II	D	$ 447,000	3.20E-05	$ 14.30
PHA2-P	Hung Missile - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00
PHA2-E	Hung Missile - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00
PHA2-D	Hung Missile - Down	III	D	$ 63,200	3.20E-05	$ 2.02
PHA3-P	Fail on FIRE - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00
PHA3-E	Fail on FIRE - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00
PHA3-D	Fail on FIRE - Down	II	D	$ 447,000	3.20E-05	$ 14.30
[illegible]	Fai[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	$ [illegible]
[illegible]A5-E	[illegible]Buffer Open [illegible]E - E[illegible]	[illegible]	[illegible]	$ 10,[illegible]	3.20E-[illegible]	3.2[illegible]
FMEA5-D	WOW Buffer Open on CLOSE - Down	II	E	$ 447,000	3.20E-07	$ 0.14
FMEA6-P	WOW Buffer on OPEN - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00
FMEA6-E	WOW Buffer on OPEN - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20
FMEA6-D	WOW Buffer on OPEN - Down	II	E	$ 447,000	3.20E-07	$ 0.14
FMEA7-P	WOW Buffer Coil OPEN with Volt - Pers	I	D	$ 10,000,000	3.20E-05	$ 320.00
FMEA7-E	WOW Buffer Coil OPEN with Volt - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20
FMEA7-D	WOW Buffer Coil OPEN with Volt - Down	II	E	$ 447,000	3.20E-07	$ 0.14
						$ -
						$ -
						$ -

Step 5: Sum Risks

A	B	C	D	E		F	G	
Haz ID	Short Title	Sev. Cat	Prob. Cat	Sev. Value		Prob. Value	Partial Risk, $$	
PHA1-P	Uncommand Release - Personnel	I	C	$	10,000,000	3.20E-03	$	32,000.00
PHA1-E	Uncommand Release - Equip	I	D	$	10,000,000	3.20E-05	$	320.00
PHA1-D	Uncommand Release - Down	II	D	$	447,000	3.20E-05	$	14.30
PHA2-P	Hung Missile - Personnel	I	C	$	10,000,000	3.20E-03	$	32,000.00
PHA2-E	Hung Missile - Equip	I	D	$	10,000,000	3.20E-05	$	320.00
PHA2-D	Hung Missile - Down	III	D	$	63,200	3.20E-05	$	2.02
PHA3-P	Fail on FIRE - Personnel	I	C	$	10,000,000	3.20E-03	$	32,000.00
PHA3-E	Fail on FIRE - Equip	I	D	$	10,000,000	3.20E-05	$	320.00
PHA3-D	Fail on FIRE - Down	II	D	$	447,000	3.20E-05	$	14.30
[illegible]	Fai[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	$	[illegible]
FMEA5-E	[illegible] Buffer Open [illegible]	[illegible]	[illegible]	$	10,[illegible]	3.20E-[illegible]	[illegible]	3.2[illegible]
FMEA5-D	WOW Buffer Open on CLOSE - Down	II	E	$	447,000	3.20E-07	$	0.14
FMEA6-P	WOW Buffer on OPEN - Personnel	I	D	$	10,000,000	3.20E-05	$	320.00
FMEA6-E	WOW Buffer on OPEN - Equip	I	E	$	10,000,000	3.20E-07	$	3.20
FMEA6-D	WOW Buffer on OPEN - Down	II	E	$	447,000	3.20E-07	$	0.14
FMEA7-P	WOW Buffer Coil OPEN with Volt - Pers	I	D	$	10,000,000	3.20E-05	$	320.00
FMEA7-E	WOW Buffer Coil OPEN with Volt - Equip	I	E	$	10,000,000	3.20E-07	$	3.20
FMEA7-D	WOW Buffer Coil OPEN with Volt - Down	II	E	$	447,000	3.20E-07	$	0.14
							$	-
							$	-
							$	-
							$	131,917.98

Initial Risk Calculations All Assets...



Step 6: Compute Required Risk Measures

Expected Loss Rate (ELR)

Describes: Anticipated loss in one Average Exposure Interval (AEI)

Method: Sum risks for all hazards; assign unity probability to sum; accept as total risk.

Conditional Loss Rate (CLR)

Describes: Expected loss amount in one AEI, given that loss occurs.

Method: Sum all hazard probabilities; use $S_{CLR} = R_T / P_{CLR}$ to compute severity.

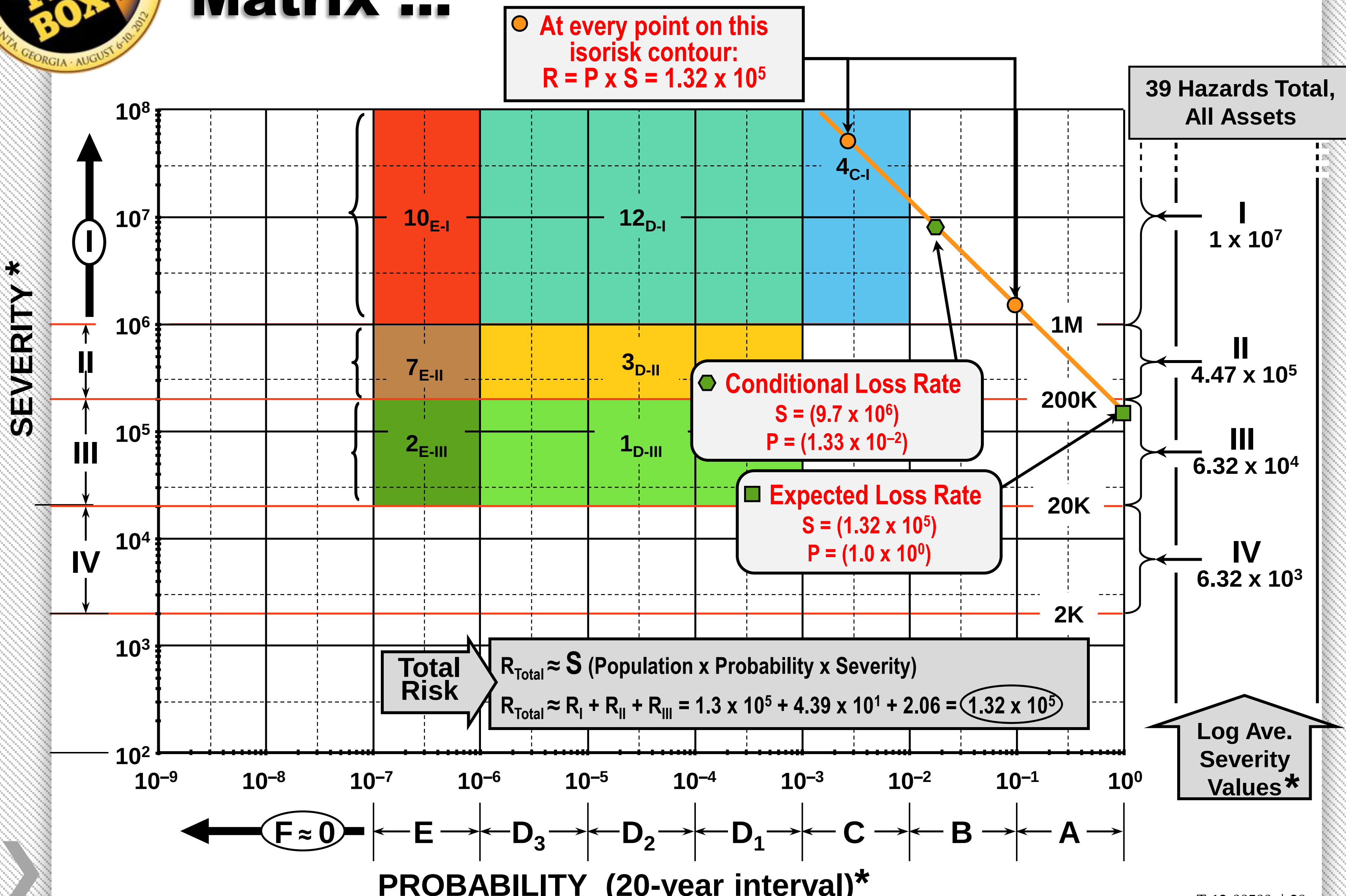
"Summing Risk," System Safety Society Journal, Nov.-Dec. 2005

Computing Risk Measures

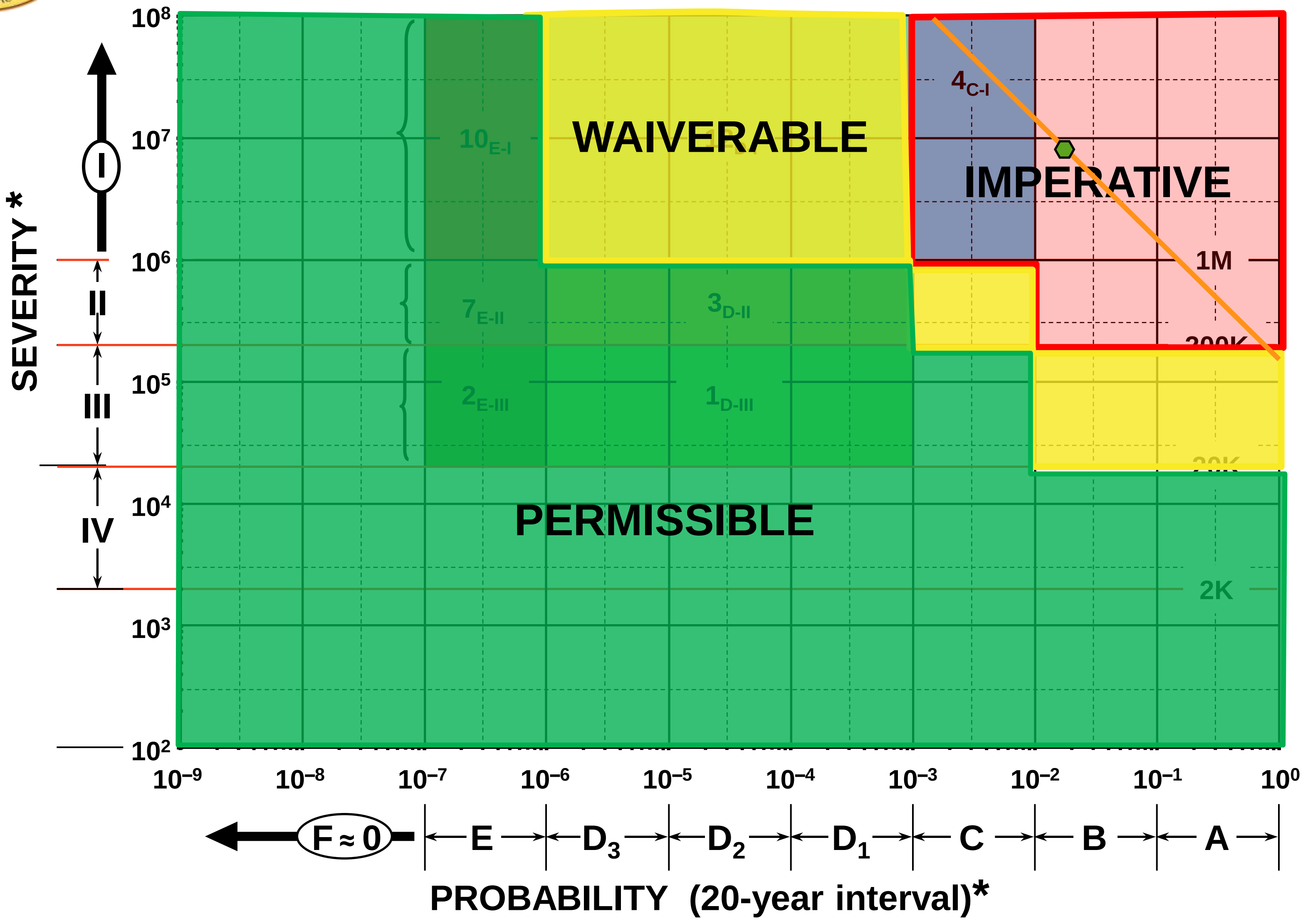
A	B	C	D	E	F	G
Haz ID	Short Title	Sev. Cat	Prob. Cat	Sev. Value	Prob. Value	Partial Risk, $$
PHA1-P	Uncommand Release - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00
PHA1-E	Uncommand Release - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00
PHA1-D	Uncommand Release - Down	II	D	$ 447,000	3.20E-05	$ 14.30
PHA2-P	Hung Missile - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00
PHA2-E	Hung Missile - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00
PHA2-D	Hung Missile - Down	III	D	$ 63,200	3.20E-05	$ 2.02
PHA3-P	Fail on FIRE - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00
PHA3-E	Fail on FIRE - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00
PHA3-D	Fail on FIRE - Down	II	D	$ 447,000	3.20E-05	$ 14.30
[illegible]	Fai[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	$ [illegible]
[illegible]	[illegible] Buffer Open [illegible]	[illegible]	[illegible]	$ 10,[illegible]	3.20E-[illegible]	$ 3.2[illegible]
FMEA5-D	WOW Buffer Open on CLOSE - Down	II	E	$ 447,000	3.20E-07	$ 0.14
FMEA6-P	WOW Buffer on OPEN - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00
FMEA6-E	WOW Buffer on OPEN - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20
FMEA6-D	WOW Buffer on OPEN - Down	II	E	$ 447,000	3.20E-07	$ 0.14
FMEA7-P	WOW Buffer Coil OPEN with Volt - Pers	I	D	$ 10,000,000	3.20E-05	$ 320.00
FMEA7-E	WOW Buffer Coil OPEN with Volt - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20
FMEA7-D	WOW Buffer Coil OPEN with Volt - Down	II	E	$ 447,000	3.20E-07	$ 0.14
						$ -
						$ -
						$ -
						$ 131,917.98

	S	P
Expected Loss Rate	$ 131,918	1.00E+00
Maximum Loss	$ 10,000,000	1.32E-02
Most Probable Loss	$ 10,000,000	1.32E-02
Conditional Loss Rate	$ 9,956,038	1.33E-02

Returning Summed Risk to the RAC Matrix …



Application to Risk Levels for Approval/Acceptance



Conclusion

- » Risk summing provides the responsible decision-maker with a clear picture of total system risk.
- » Details of risk summing methodology are provided in the "Risk Summing Guidebook."
- » The Guidebook presents complete examples and a formatted spreadsheet matrix containing all necessary calculations.
- » Assumptions have been made during initial implementation for ease of communication and to simplify communication of methodology.