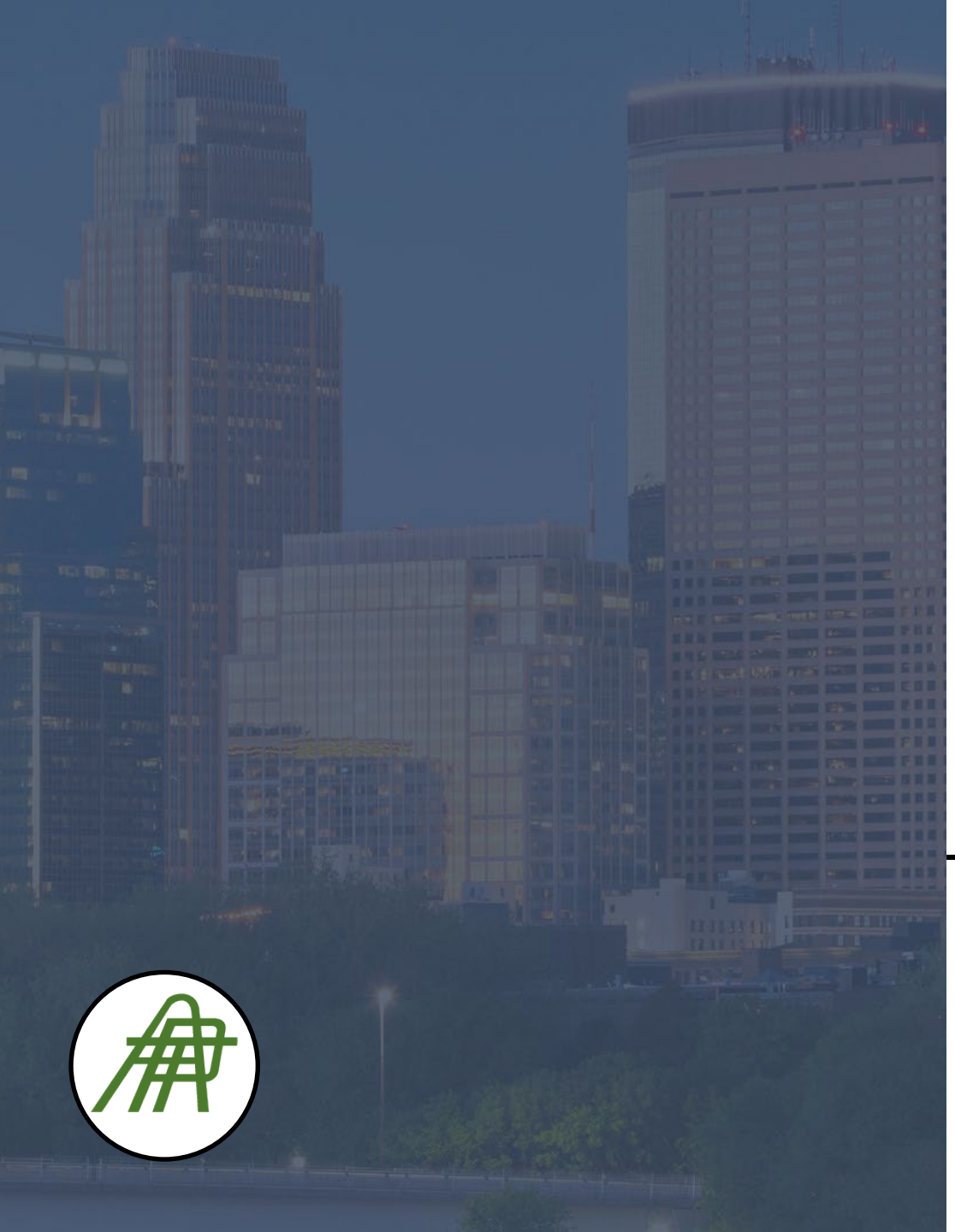


INTERNATIONAL SYSTEM SAFETY
ANNUAL SUMMIT AND TRAINING

AI-DRIVEN SAFETY: PROMISES & PITFALLS

MINNEAPOLIS, MN | AUG. 26-30, 2024

Mathematical Techniques to Improve the Utility of a Hazard Risk Matrix

Don Swallom
A-P-T Research, Inc.
Huntsville, Alabama, USA

Topics for this Tutorial

- Purpose of a Hazard Risk Matrix
- Understanding the Attributes of a well-designed risk assessment matrix
- How to Assign a Risk Assessment Code
- Understanding Probability
- Building an Expanded Matrix
- Plotting Accidents on a Matrix
- Using Relative Risk Values
- Building Hazard Risk Profiles
- Impact on Software Safety Matrices

Source of the DOD Hazard Risk Matrix

Purpose of a Hazard Risk Matrix

- Determine who accepts the risk of a particular hazard

"…The Program Manager will use the methodology in MIL-STD-882E…Prior to exposing people, equipment, or the environment to known system-related ESOH hazards, the Program Manager will document that the associated risks have been accepted by the following acceptance authorities: the CAE for high risks, Program Executive Officer-level for serious risks, and the Program Manager for medium and low risks…" - Department of Defense Instruction 5000.02, January 7, 2015.

Purpose of a Hazard Risk Matrix

- Inform the risk acceptor of the nature of the risk.
- “It’s a 1D, Serious” does not really do that.

“The standard for risk management is leadership at the appropriate level of authority making **informed** decisions to control hazards or accept risks.”

Army Regulation 385-10

The Army Safety Program

29 February 2000

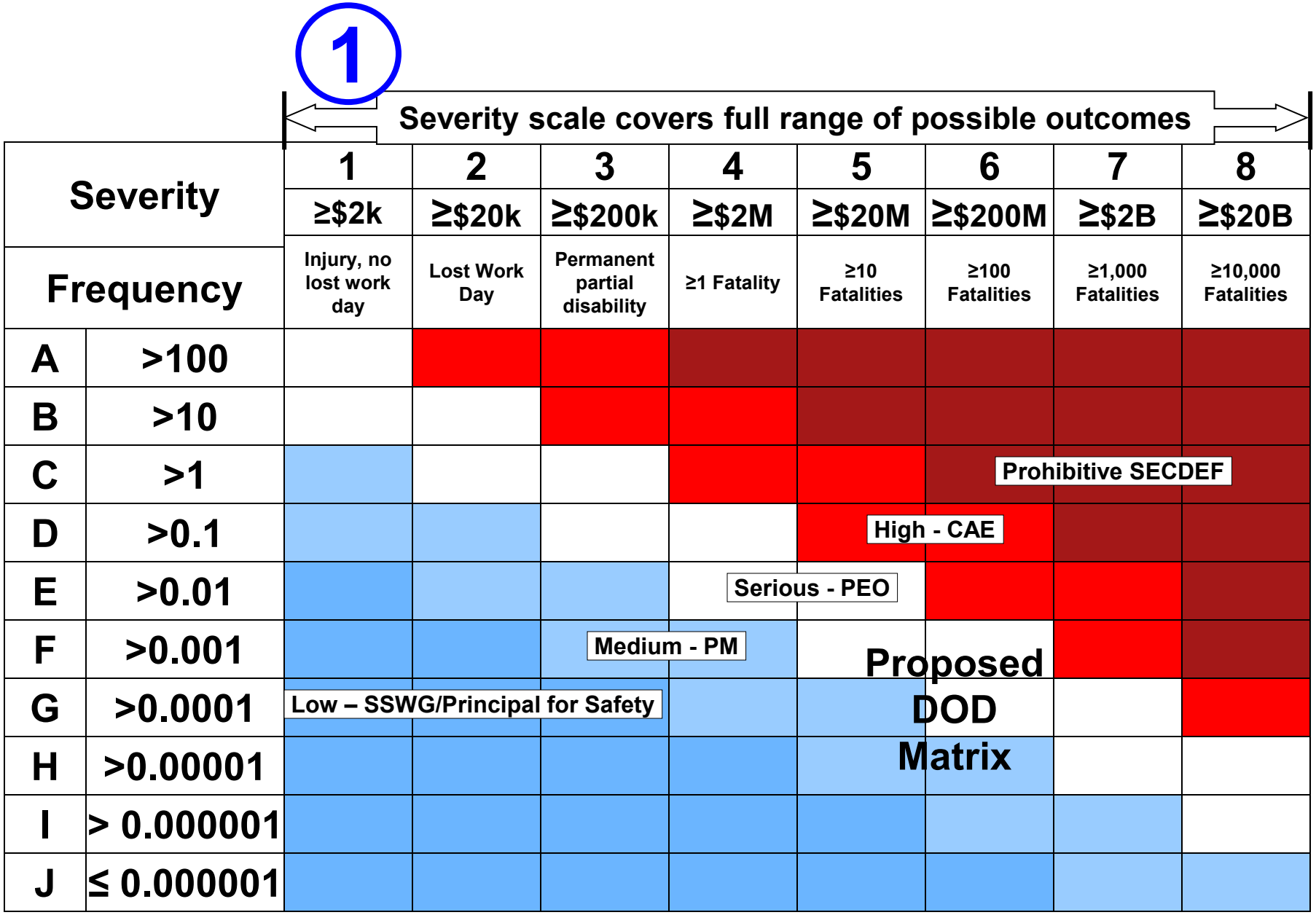
Topics for this Tutorial

- Purpose of a Hazard Risk Matrix
- **Understanding the Attributes of a well-designed risk assessment matrix**
- How to Assign a Risk Assessment Code
- Understanding Probability
- Building an Expanded Matrix
- Plotting Accidents on a Matrix
- Using Relative Risk Values
- Building Hazard Risk Profiles
- Impact on Software Safety Matrices

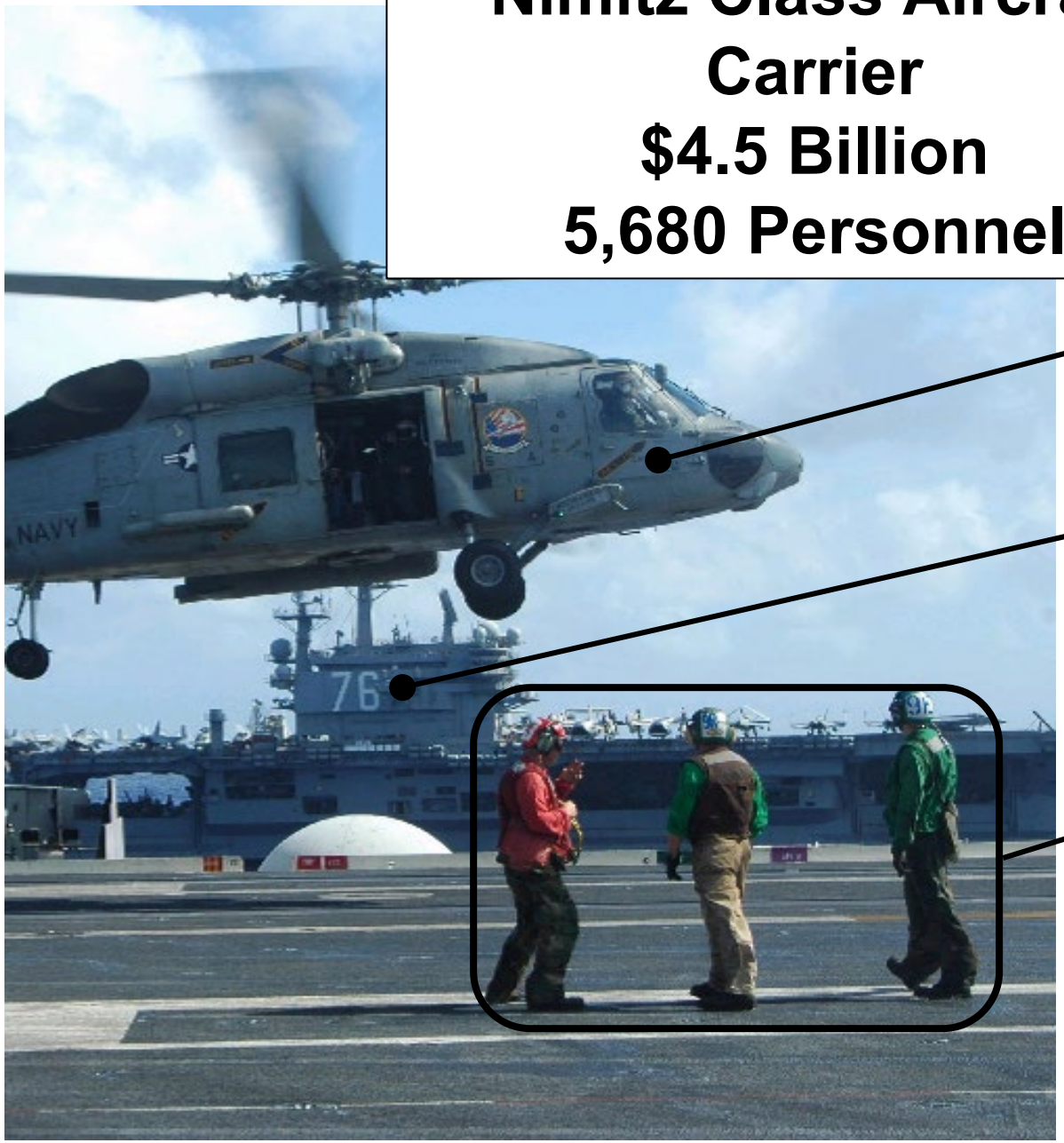
Probability versus Frequency of Occurrence

- Frequency of occurrence is often substituted for probability and exposure interval
- Frequency has the exposure interval "built in," for example, mishaps per 100,000 flight hours (aircraft) or mishaps per 1,000,000 firings (missiles) or mishaps per 1,000 troops per year

Attributes of a well-designed risk assessment matrix



Nimitz Class Aircraft
Carrier
$4.5 Billion
5,680 Personnel



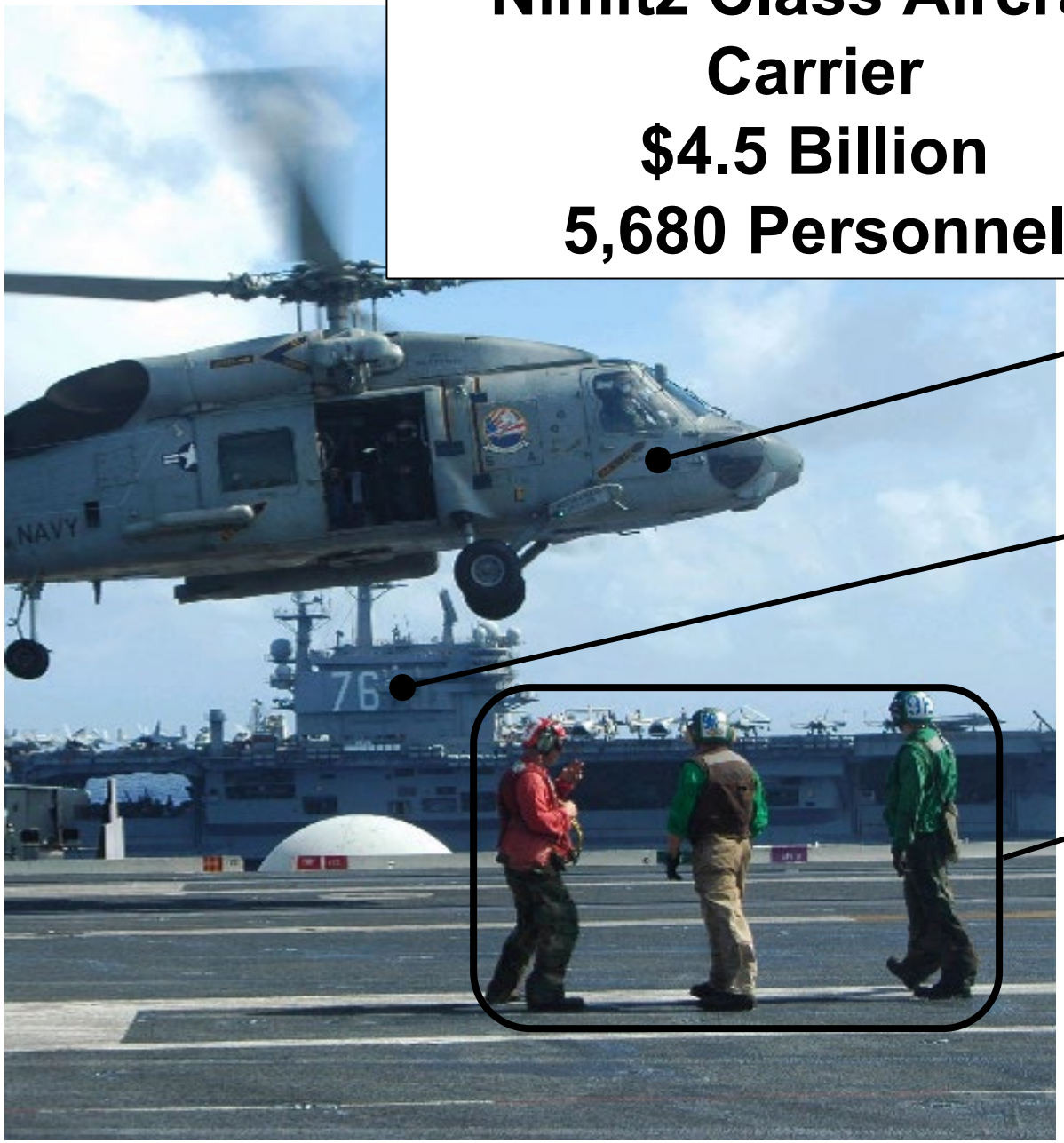
Today

Severity 1

Severity 1

Severity 1

Nimitz Class Aircraft
Carrier
$4.5 Billion
5,680 Personnel



Severity 5

Severity 7

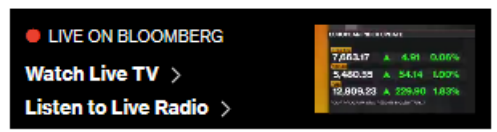
Severity 4

Politics

Navy Seeks $30 Million to Fix Gear That Hobbled Its New Carrier

By Anthony Capaccio
July 25, 2018, 10:04 AM CDT

- Congress asked to shift funds to repair Ford aircraft carrier
- Huntington Ingalls continues talks with General Electric



LISTEN TO ARTICLE

▶ 1:25

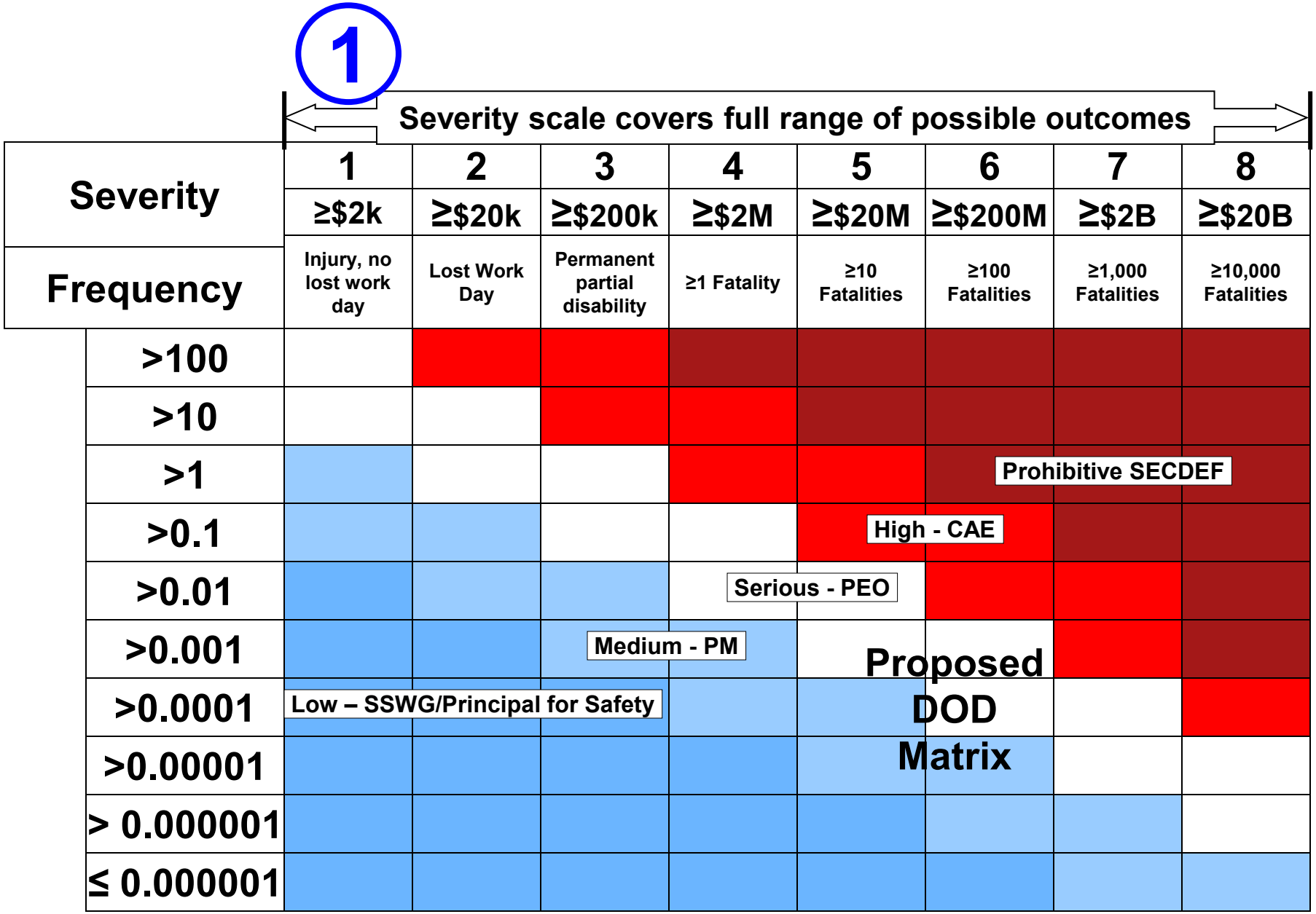
SHARE THIS ARTICLE

Facebook
Twitter
LinkedIn
Email

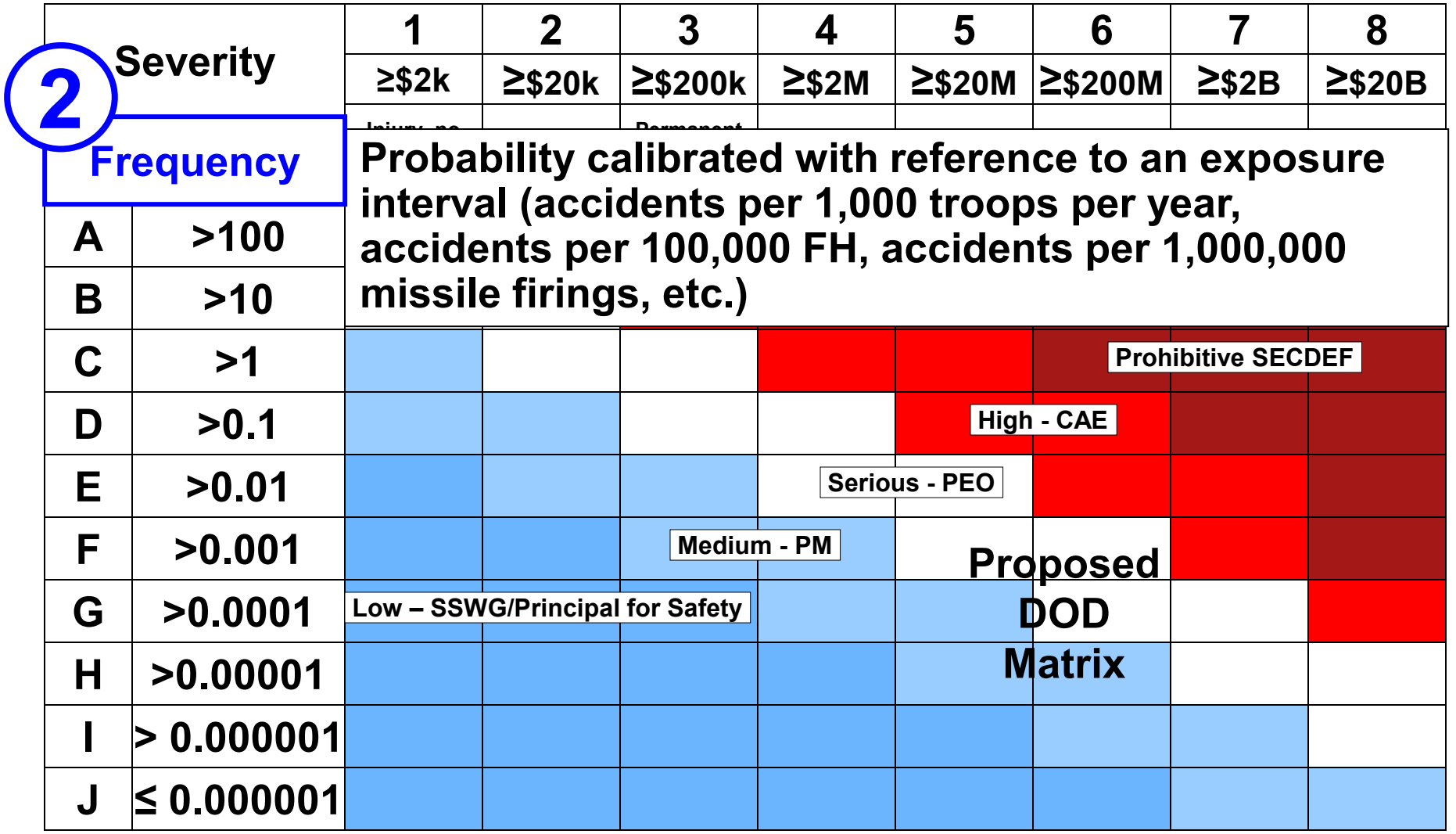
The Navy is asking Congress to shift $30 million from other accounts to start repairing a damaged gear on the service's costliest warship, the Gerald R. Ford aircraft carrier.

The request for funds to repair the $13 billion carrier is part of a Pentagon package asking congressional approval to shift $4.7 billion in previously approved Army, Air Force and Navy funding into new programs or higher-priority projects. The package must be approved by all four congressional defense committees, where it's pending.

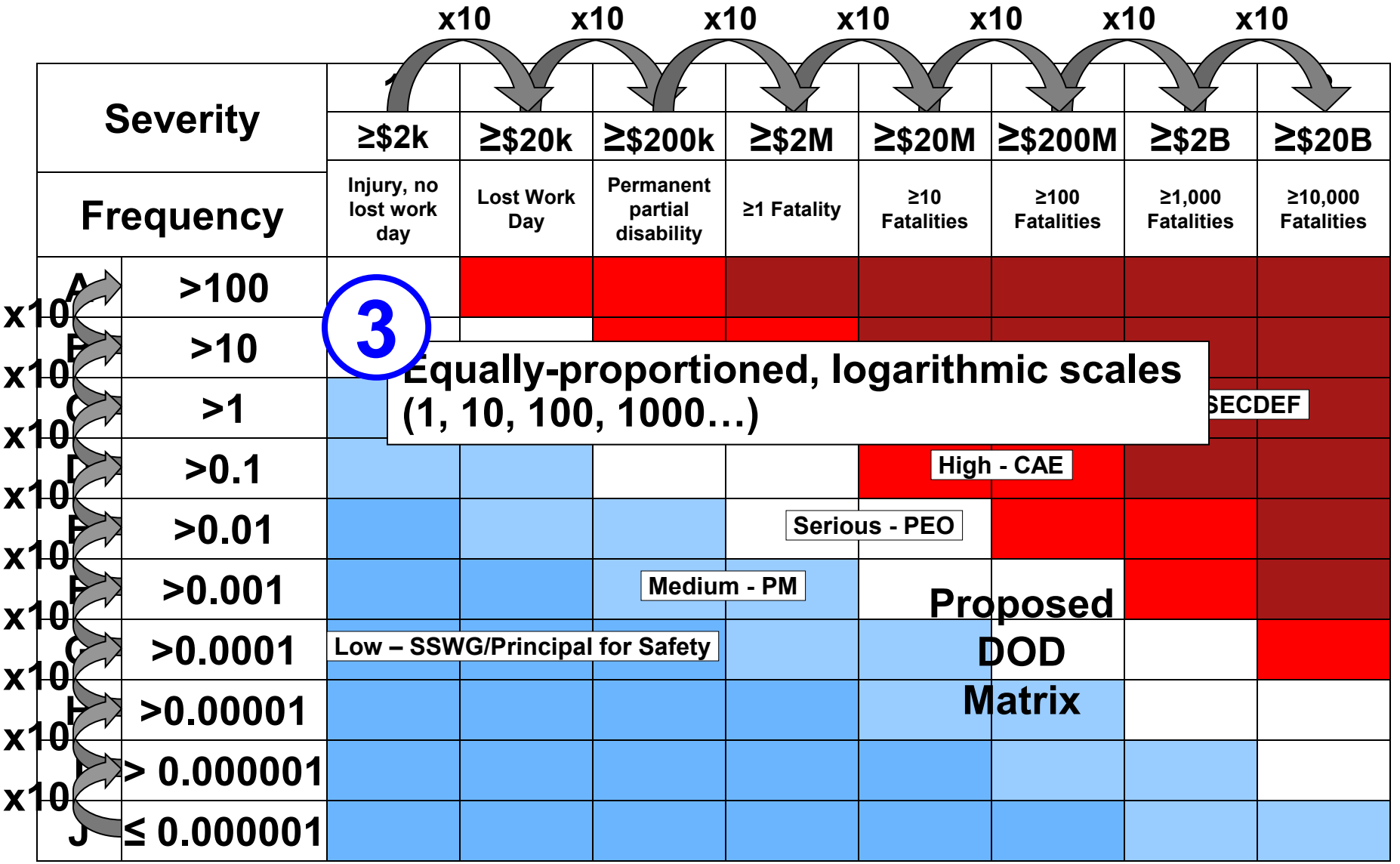
Attributes of a well-designed risk assessment matrix



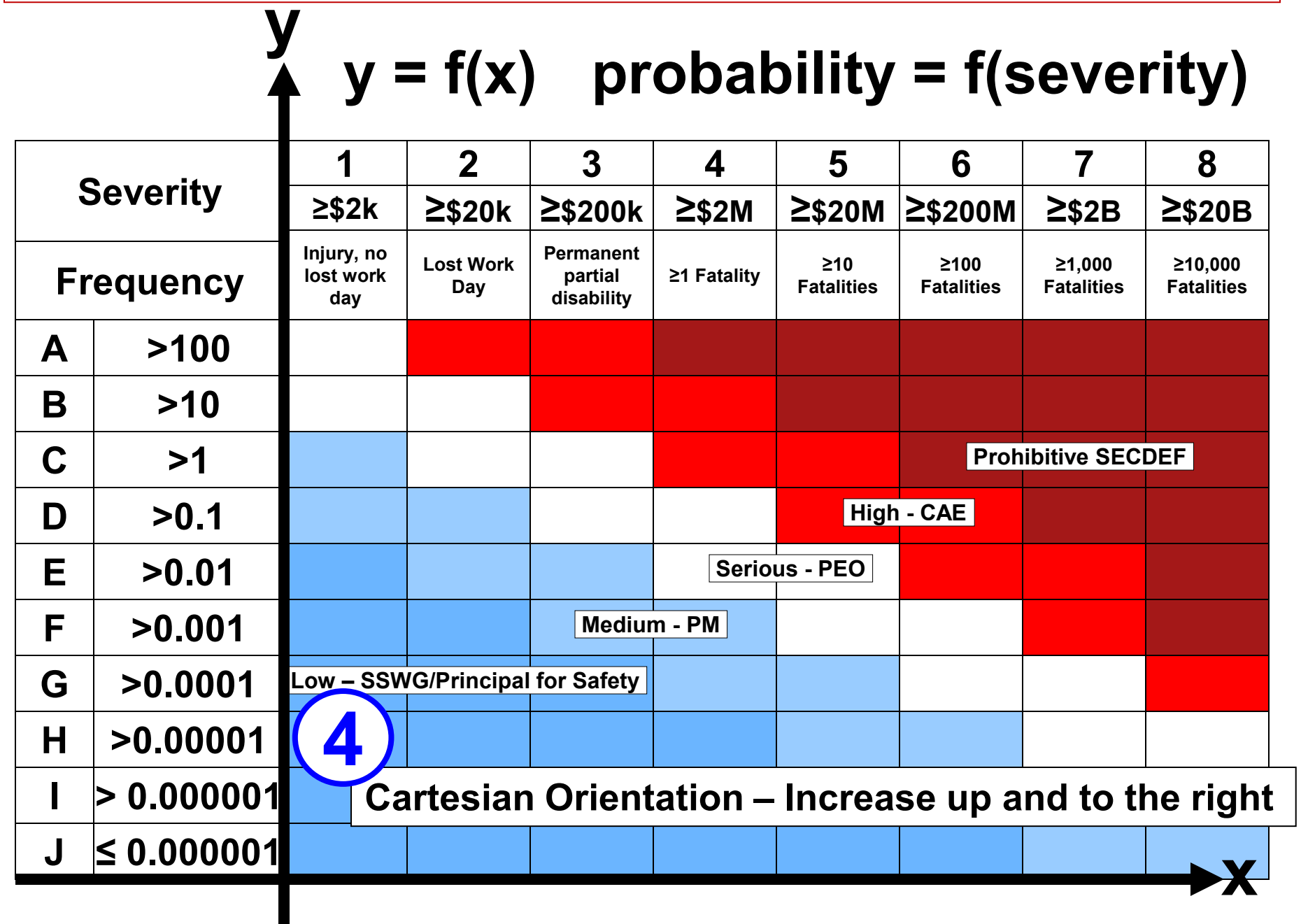
Attributes of a well-designed risk assessment matrix



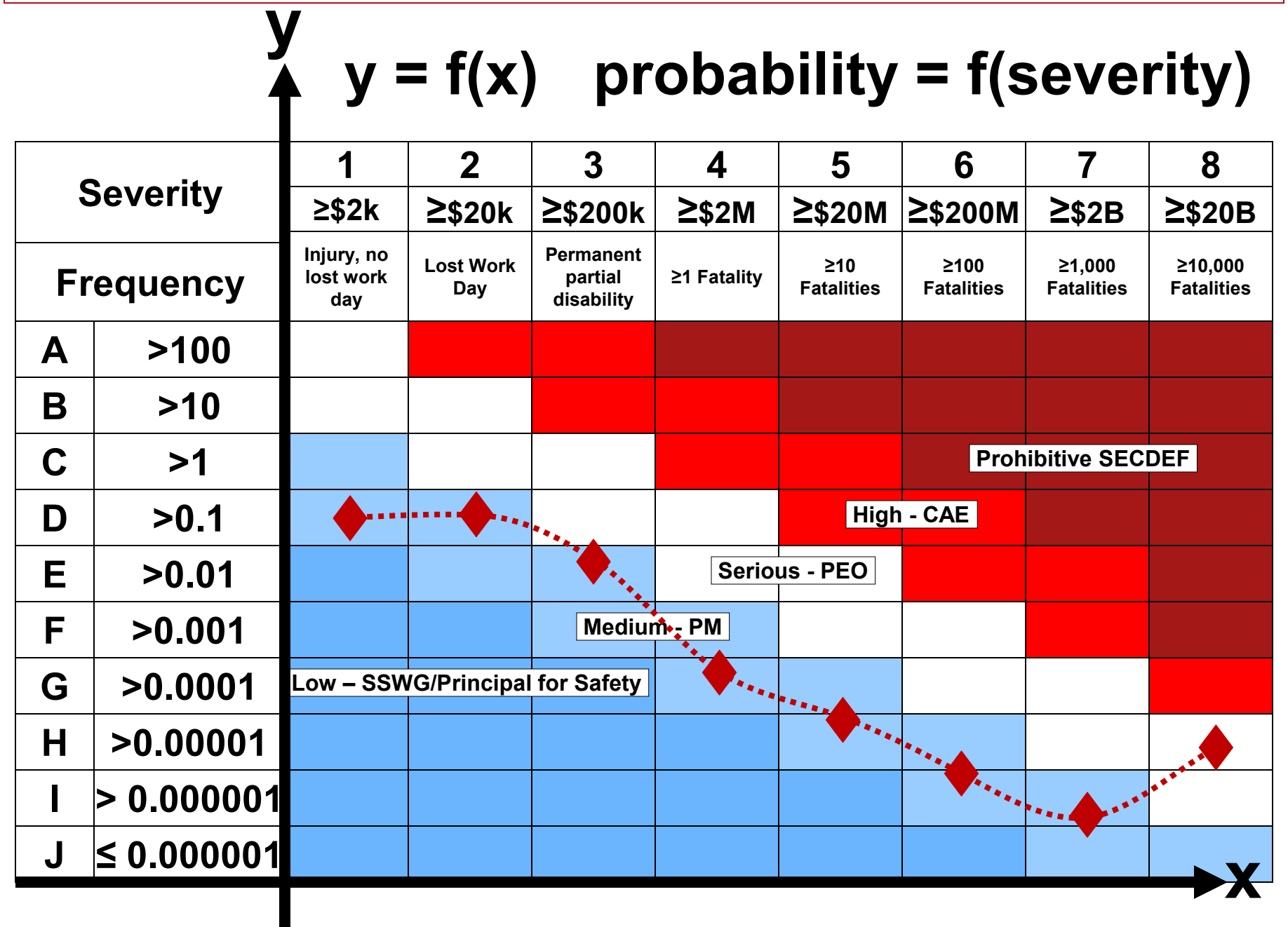
Attributes of a well-designed risk assessment matrix



Attributes of a well-designed risk assessment matrix

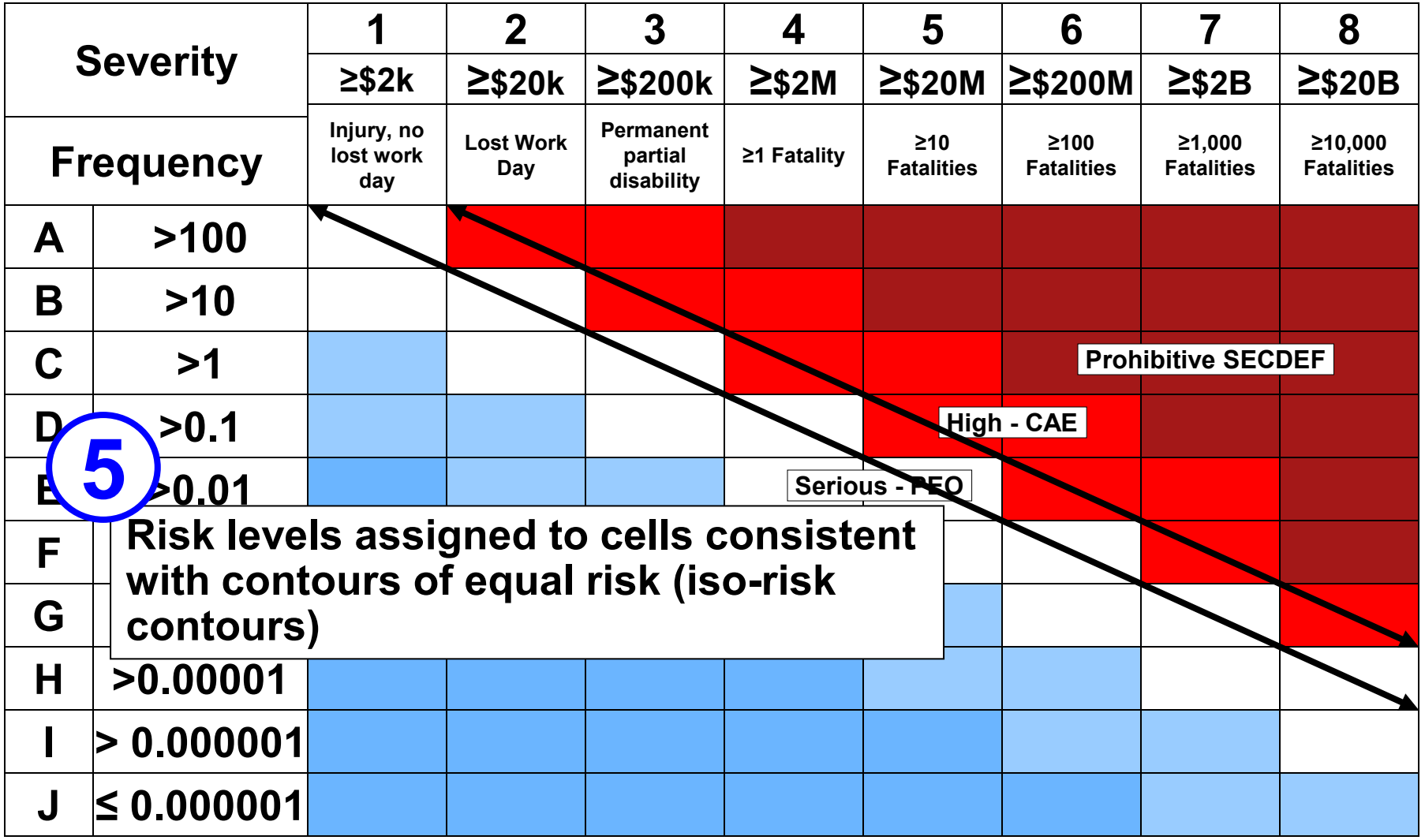


Attributes of a well-designed risk assessment matrix

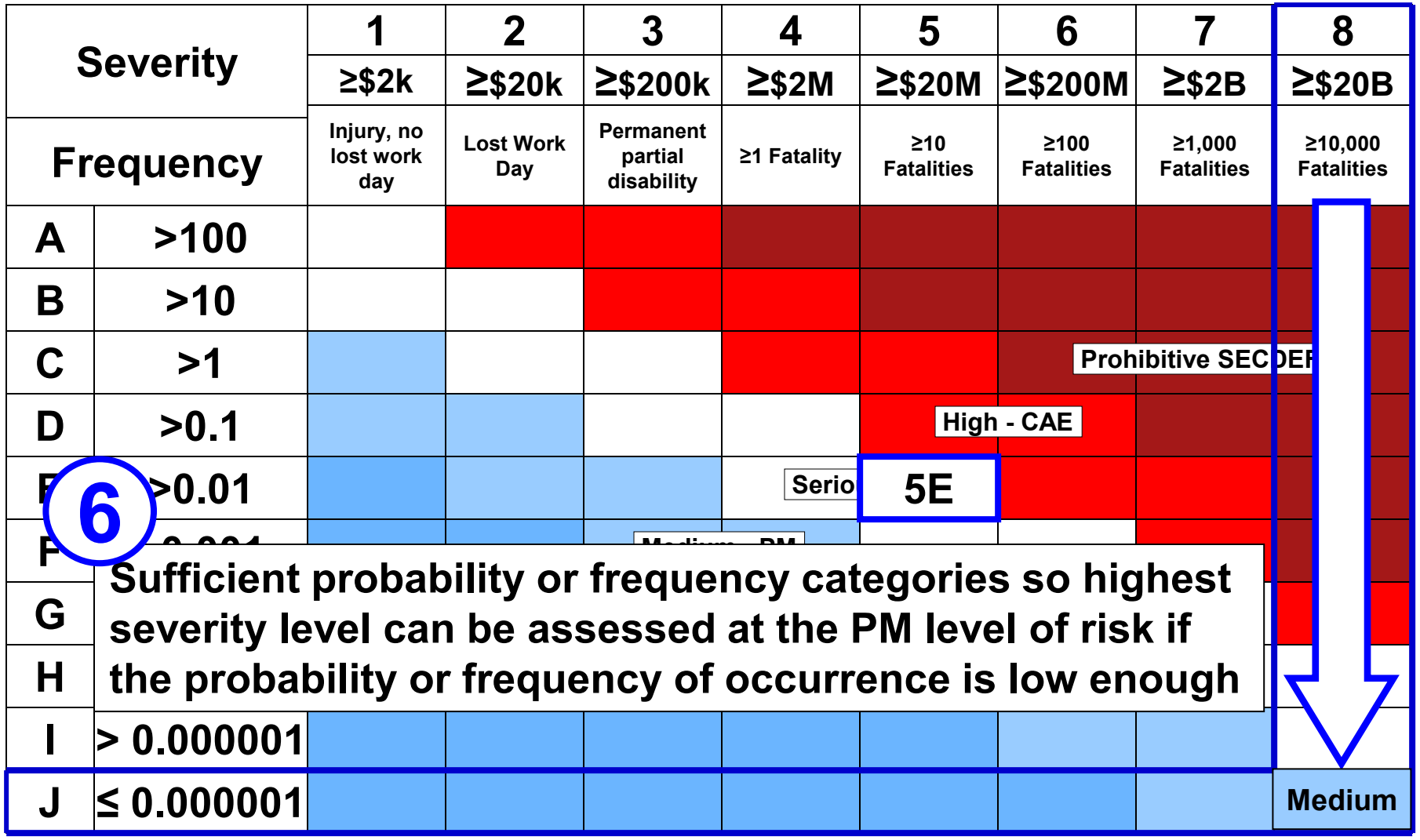


Severity		1	2	3	4	5	6	7	8
		≥$2k	≥$20k	≥$200k	≥$2M	≥$20M	≥$200M	≥$2B	≥$20B
Frequency		Injury, no lost work day	Lost Work Day	Permanent partial disability	≥1 Fatality	≥10 Fatalities	≥100 Fatalities	≥1,000 Fatalities	≥10,000 Fatalities
A	>100								
B	>10								
C	>1								
D	>0.1								
E	>0.01								
F	>0.001								
G	>0.0001								
H	>0.00001								
I	> 0.000001								
J	≤ 0.000001								

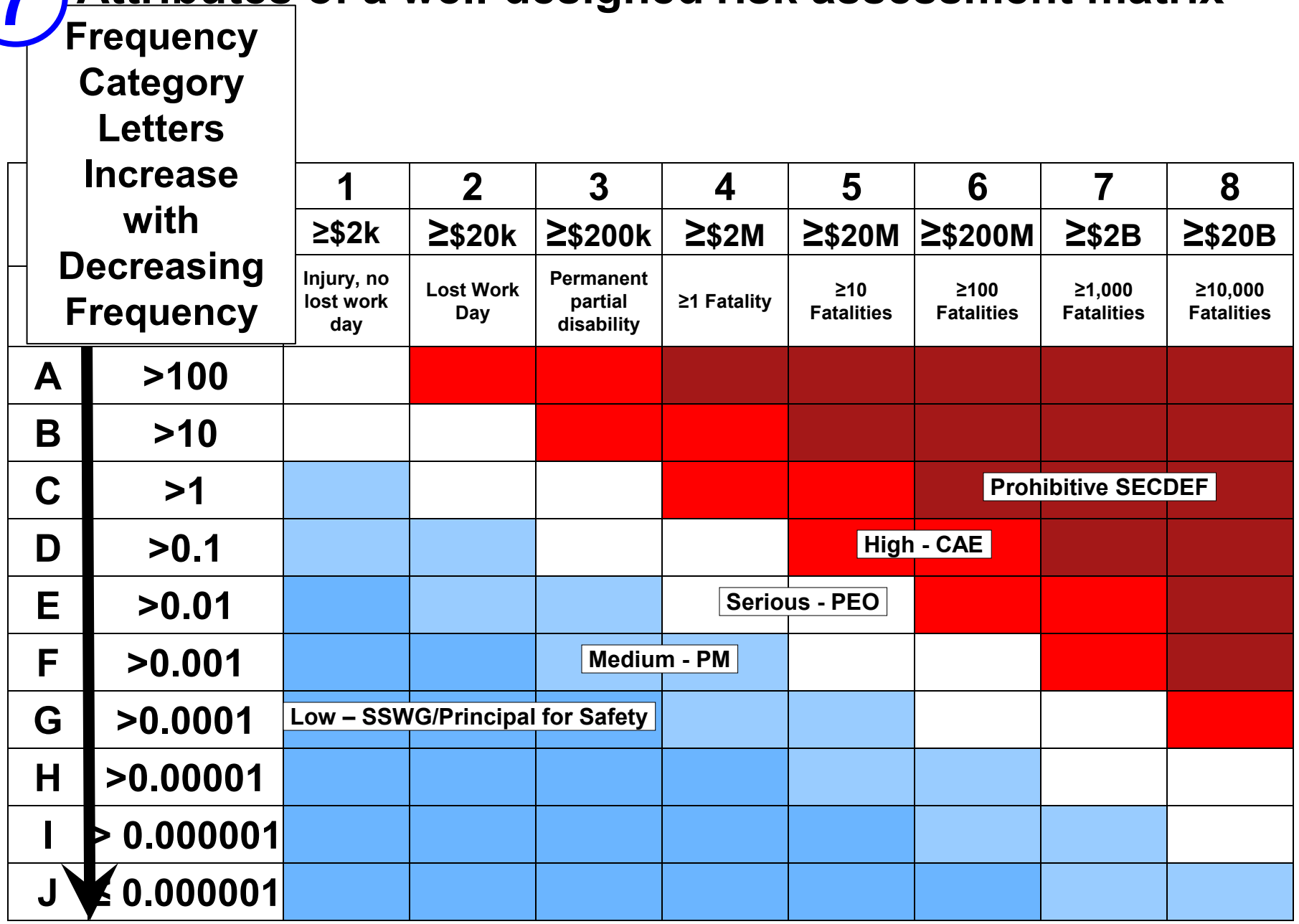
Attributes of a well-designed risk assessment matrix



Attributes of a well-designed risk assessment matrix



7 Attributes of a well-designed risk assessment matrix



8 Attributes of a well-designed risk assessment matrix

A risk assessment code for hazards whose risk has been eliminated. Suggest: 0R "Zero R" as in Zero Risk in lieu of F.

Severity		1	2	3	4	5	6	7	8
		≥$2k	≥$20k	≥$200k	≥$2M	≥$20M	≥$200M	≥$2B	≥$20B
Frequency		Injury, no lost work day	Lost Work Day	Permanent partial disability	≥1 Fatality	≥10 Fatalities	≥100 Fatalities	≥1,000 Fatalities	≥10,000 Fatalities
A	>100								
B	>10								
C	>1						Prohibitive SECDEF		
D	>0.1					High - CAE			
E	>0.01				Serious - PEO				
F	>0.001			Medium - PM					
G	>0.0001	Low – SSWG/Principal for Safety							
H	>0.00001								
I	> 0.000001								
J	≤ 0.000001								

Attributes of a well-designed risk assessment matrix

Severity		1	2	3	4	5	6	7	8
		≥$2k	≥$20k	≥$200k	≥$2M	≥$20M	≥$200M	≥$2B	≥$20B
Frequency		Injury, no lost work day	Lost Work Day	Permanent partial disability	≥1 Fatality	≥10 Fatalities	≥100 Fatalities	≥1,000 Fatalities	≥10,000 Fatalities
A	>100								
B	>10								
C	>1						Prohibitive SECDEF		
D	>0.1					High - CAE			
E	>0.01				Serio	5E			
F	>0.001			Medium - PM					
G	>0.0001	Low – SSWG/Principal for Safety							
	>0.00001								
J	≤ 0.000001								

9

Easily tailored with reporting of risk consistent with other systems within the family of systems.

Attributes of a well-designed risk assessment matrix

Severity		1	2	3	4	5
		≥$2k	≥$20k	≥$200k	≥$2M	≥$20M
Frequency		Injury, no lost work day	Lost Work Day	Permanent partial disability	≥1 Fatality	≥10 Fatalities
A	>100				Prohibitive SECDEF	
B	>10					
C	>1					
D	>0.1					High - CAE
E	>0.01				Serio	5E
F	>0.001			Medium - PM		
G	>0.0001	Low – SSWG/Principal for Safety				

9

Easily tailored with reporting of risk consistent with other systems within the family of systems.

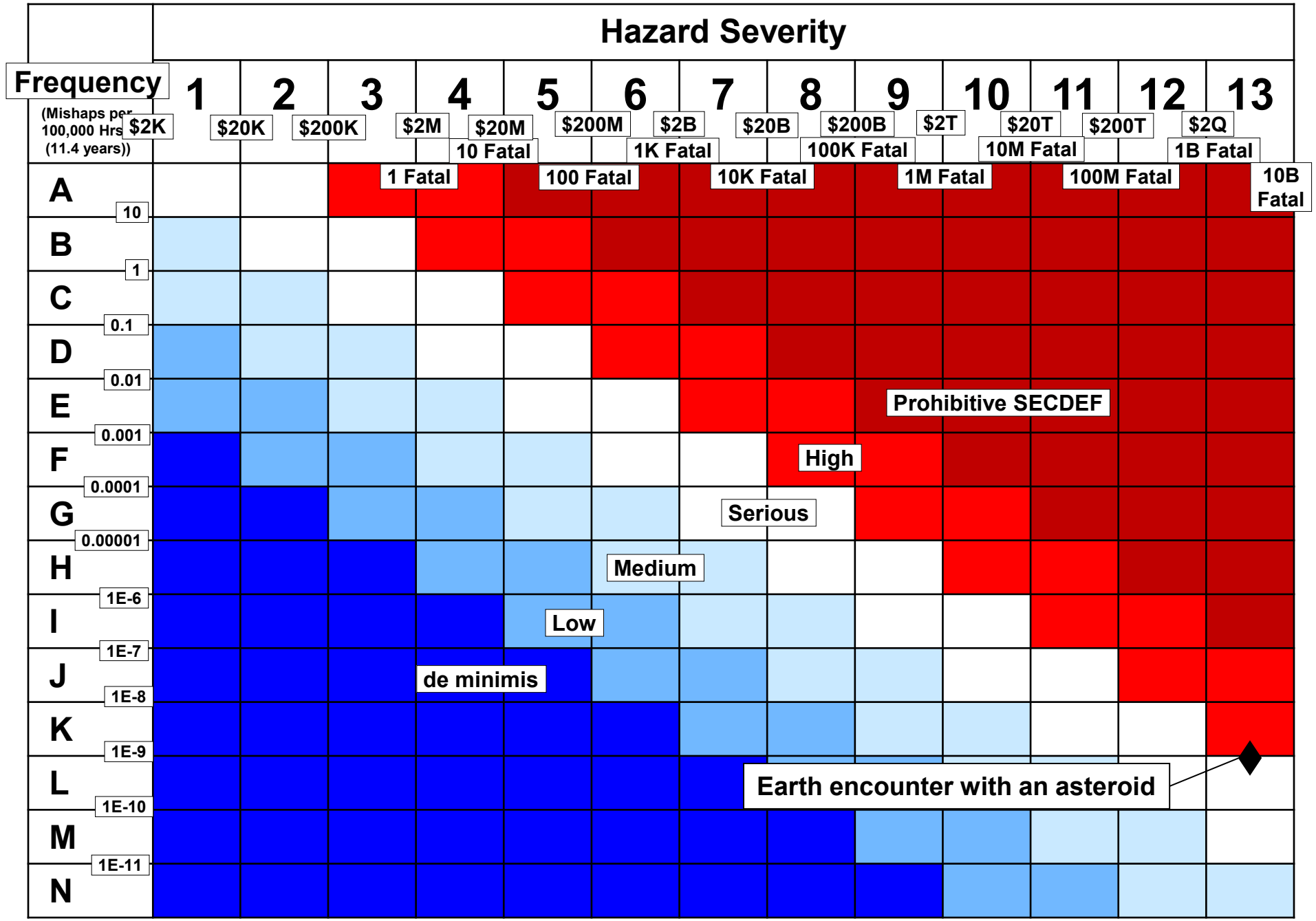
Attributes of a well-designed risk assessment matrix

10

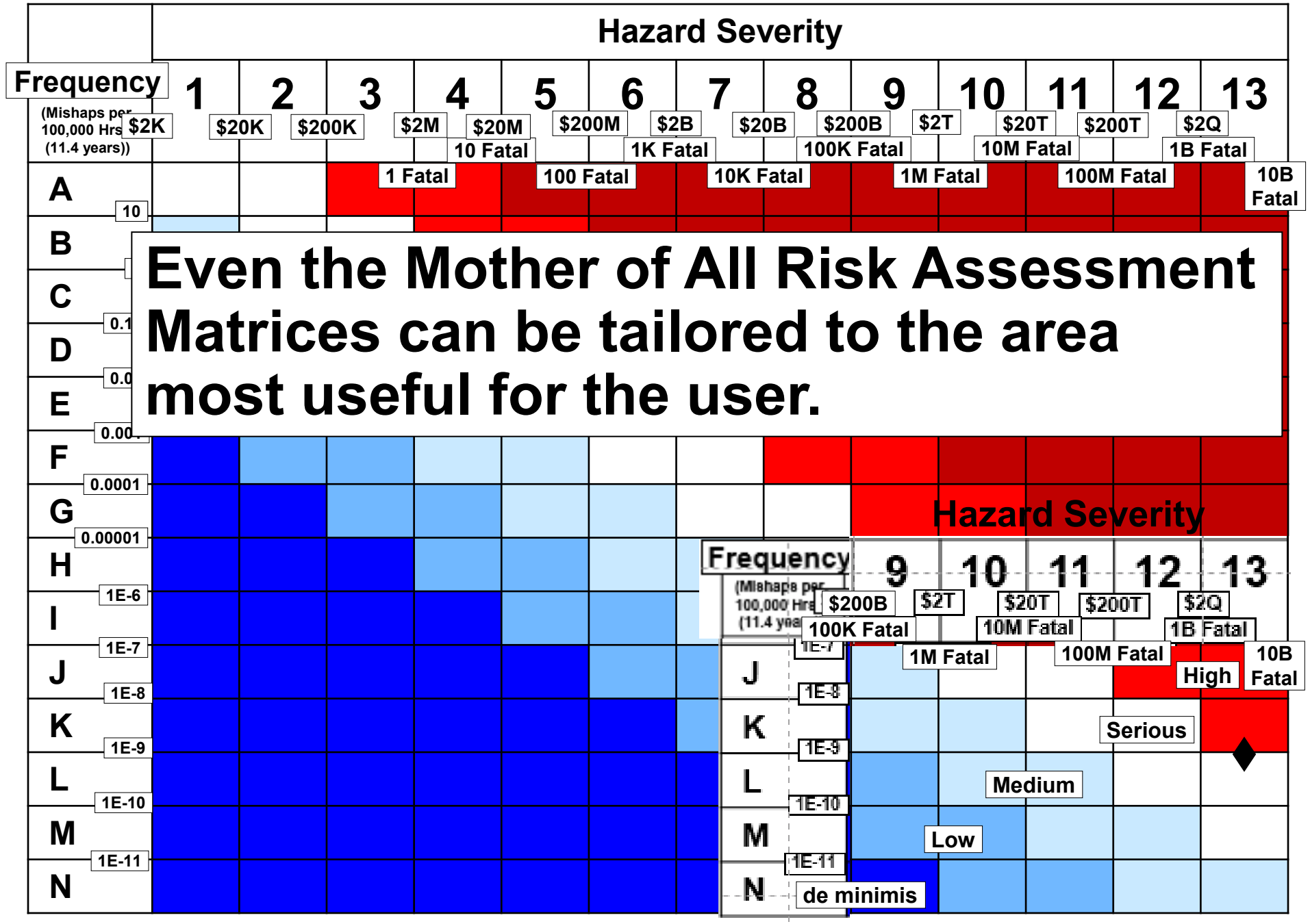
Severity Category numbers increase with increasing Severity

Severity		1	2	3	4	5	6	7
		≥$2k	≥$20k	≥$200k	≥$2M	≥$20M		
Frequency		Injury, no lost work day	Lost Work Day	Permanent partial disability	≥1 Fatality	≥10 Fatalities		
A	>100				Prohibitive SECDEF			
B	>10							
C	>1							
D	>0.1					High - CAE		
E	>0.01				Serio	5E		
F	>0.001			Medium - PM				
G	>0.0001	Low – SSWG/Principal for Safety						

Mother of All Risk Assessment Matrices (Spaceship Earth)

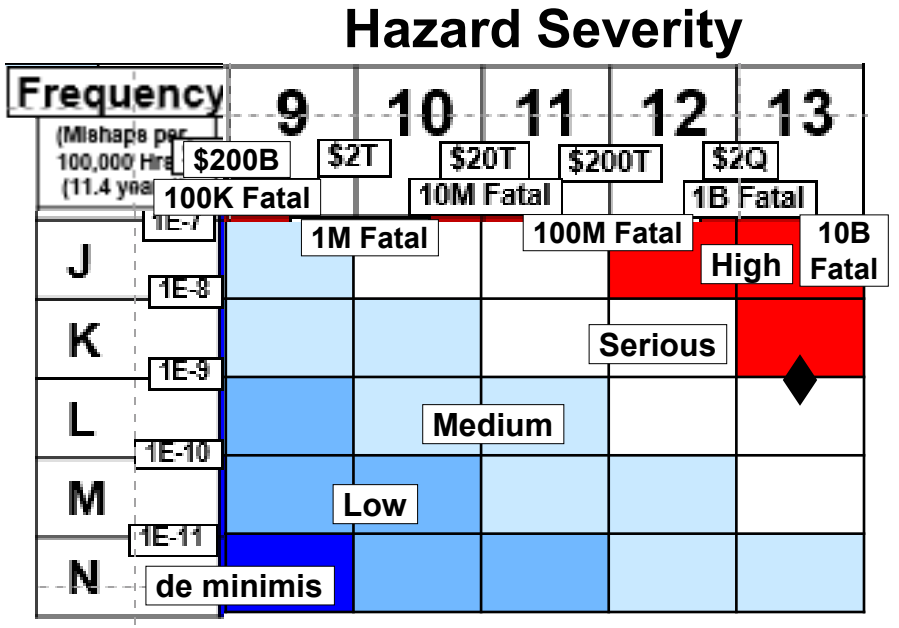


Mother of All Risk Assessment Matrices (Spaceship Earth)



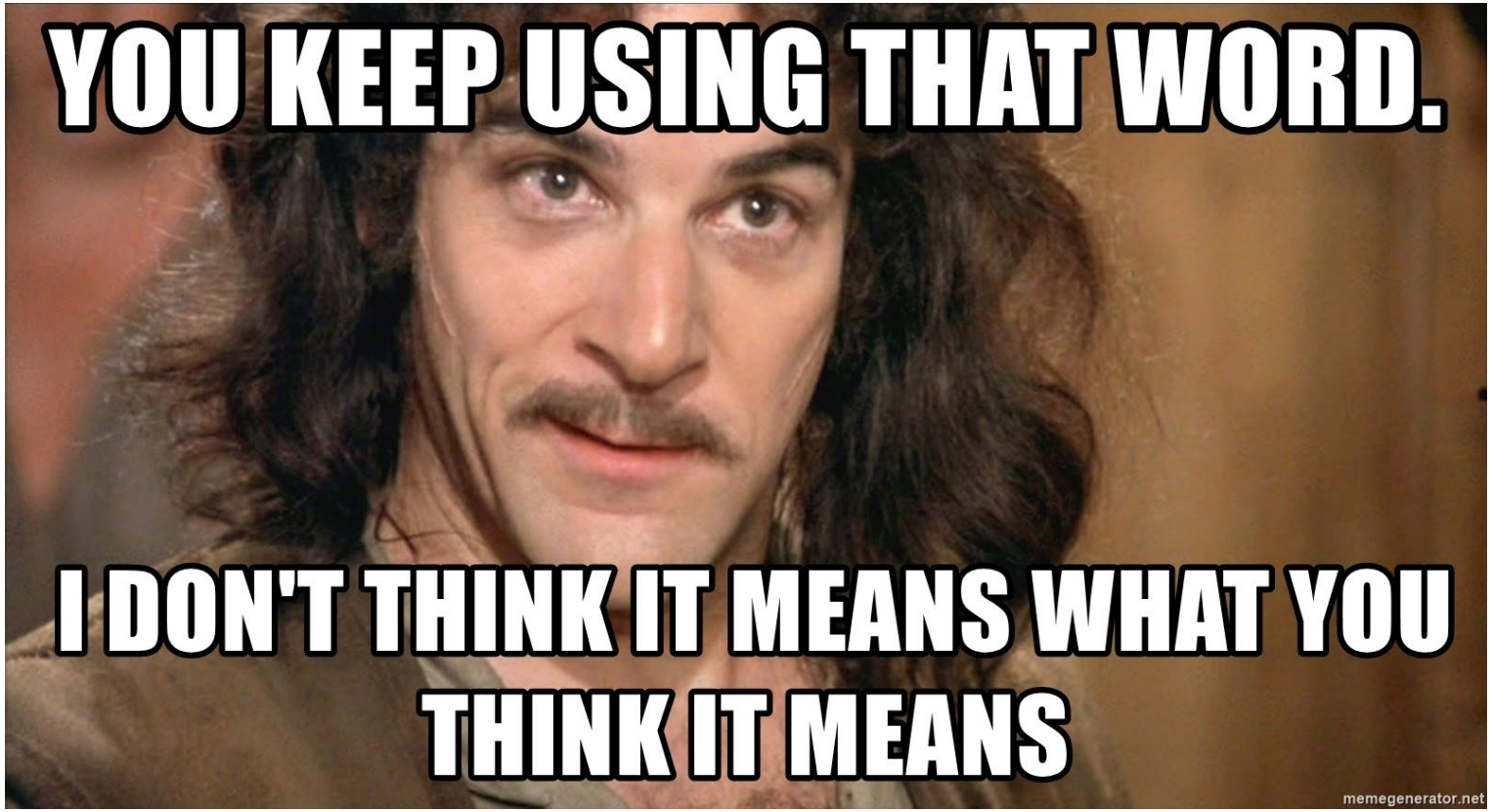
Mother of All Risk Assessment Matrices (Spaceship Earth)

Even the Mother of All Risk Assessment Matrices can be tailored to the area most useful for the user.



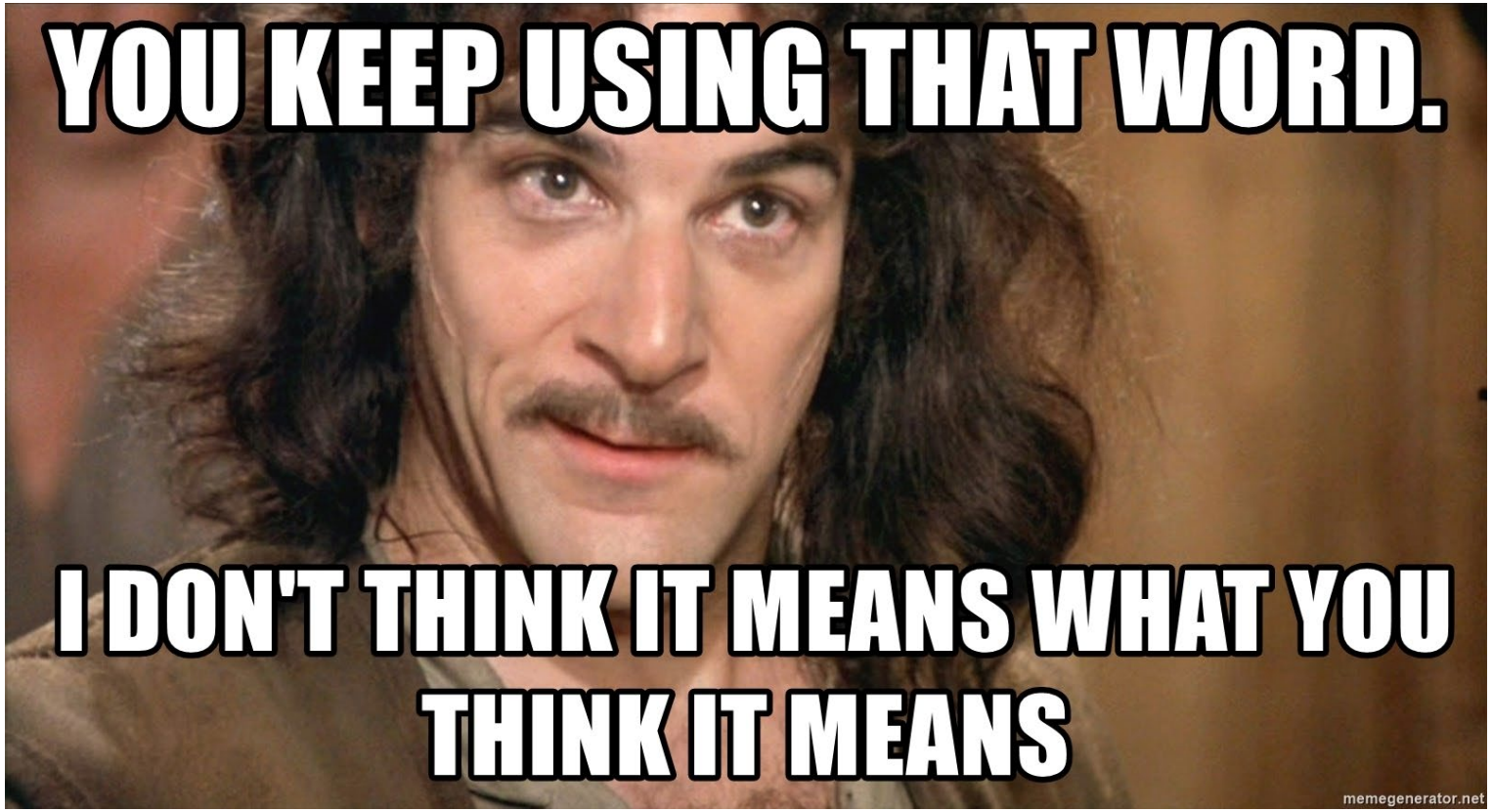
Additional Recommendation

- Eliminate one-word labels for Severity (Catastrophic, Critical, Marginal, Negligible) and Probability (Frequent, Probable, Occasional, Remote, Improbable)

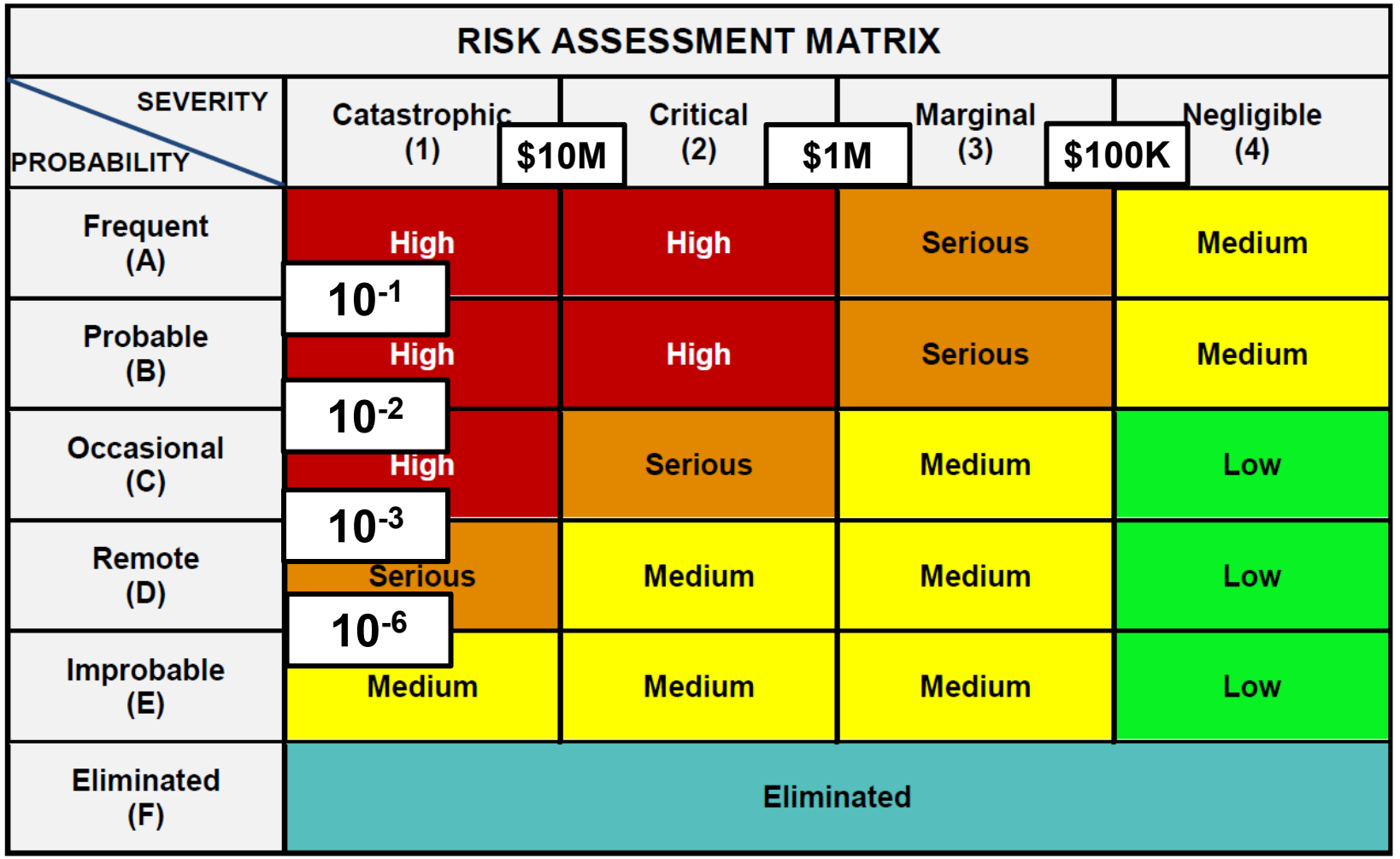


Additional Recommendation

- Just use Severity 1, Severity 2, Probability C, etc.

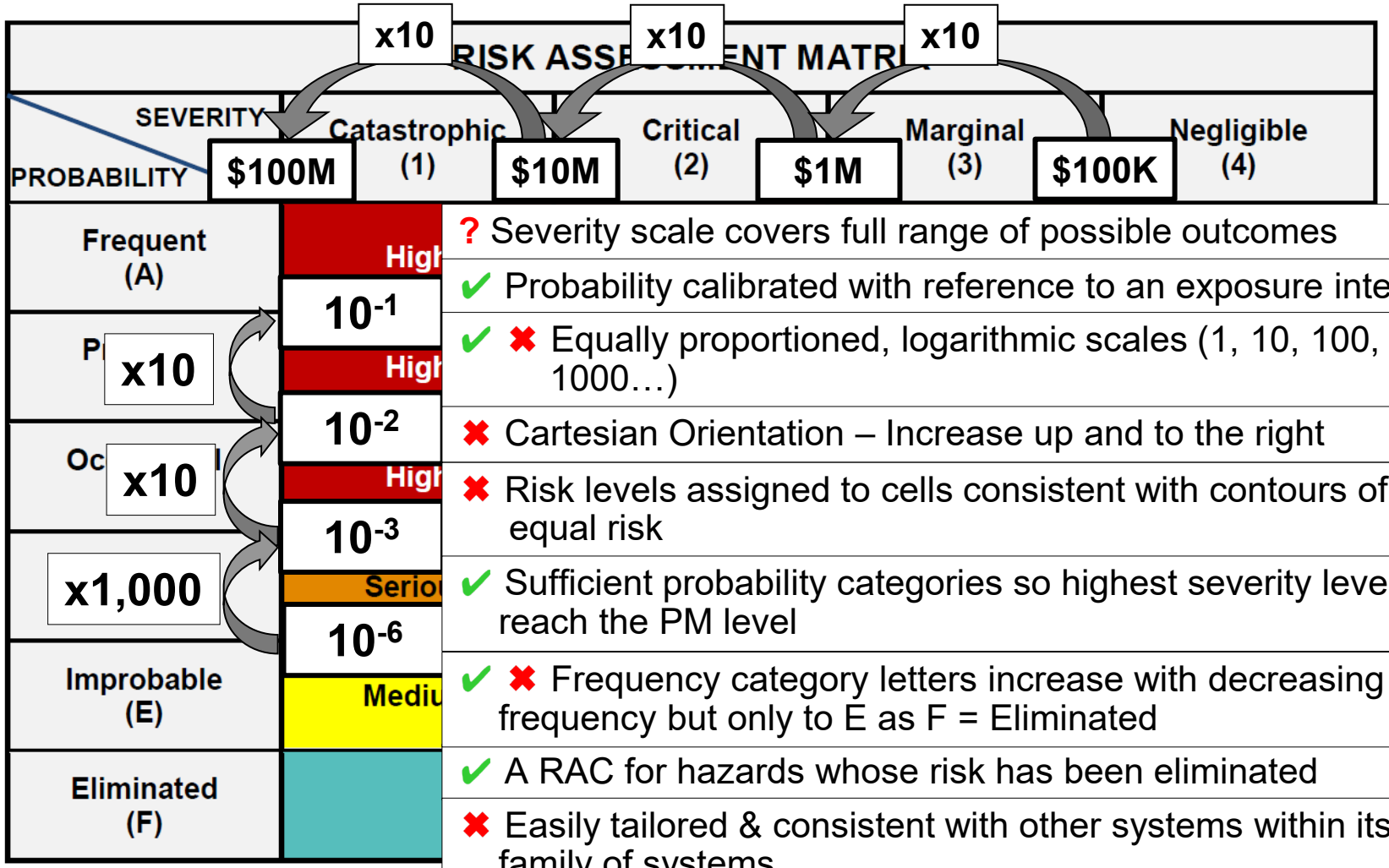


MIL-STD-882E Matrix



29

MIL-STD-882E Matrix



? Severity scale covers full range of possible outcomes
✔ Probability calibrated with reference to an exposure interval
✔ ✖ Equally proportioned, logarithmic scales (1, 10, 100, 1000…)
✖ Cartesian Orientation – Increase up and to the right
✖ Risk levels assigned to cells consistent with contours of equal risk
✔ Sufficient probability categories so highest severity level reach the PM level
✔ ✖ Frequency category letters increase with decreasing frequency but only to E as F = Eliminated
✔ A RAC for hazards whose risk has been eliminated
✖ Easily tailored & consistent with other systems within its family of systems
✖ Severity Category numbers increase with increasing Severity

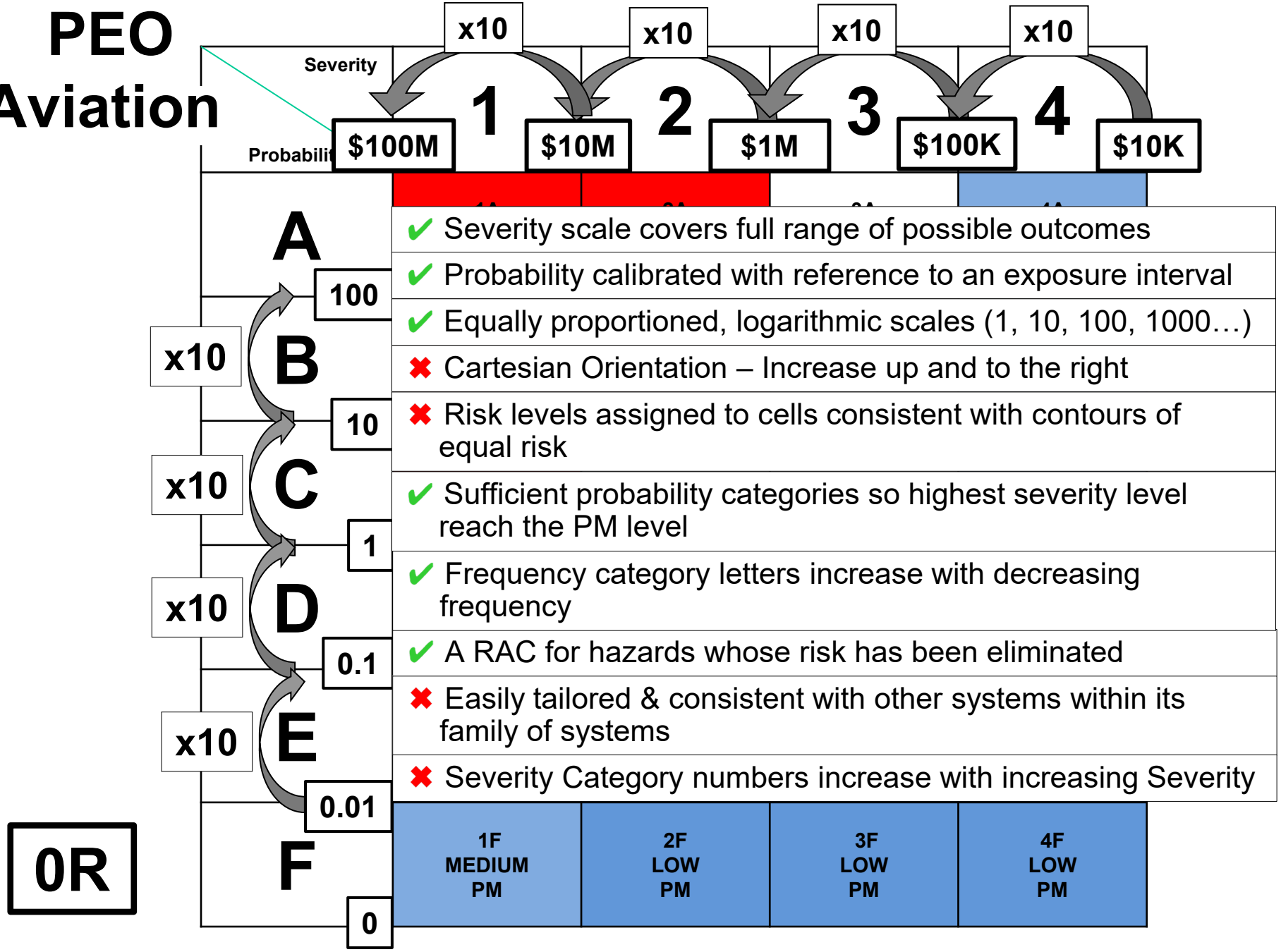
30

PEO Aviation

Probability \ Severity	1 $10M	2 $1M	3 $100K	4 $10K
A 100	1A HIGH AAE	2A HIGH AAE	3A SERIOUS PEO	4A MEDIUM PM
B 10	1B HIGH AAE	2B HIGH AAE	3B SERIOUS PEO	4B MEDIUM PM
C 1	1C HIGH AAE	2C SERIOUS PEO	3C SERIOUS PEO	4C MEDIUM PM
D 0.1	1D SERIOUS PEO	2D SERIOUS PEO	3D MEDIUM PM	4D MEDIUM PM
E 0.01	1E SERIOUS PEO	2E MEDIUM PM	3E MEDIUM PM	4E LOW PM
F 0	1F MEDIUM PM	2F LOW PM	3F LOW PM	4F LOW PM

0R

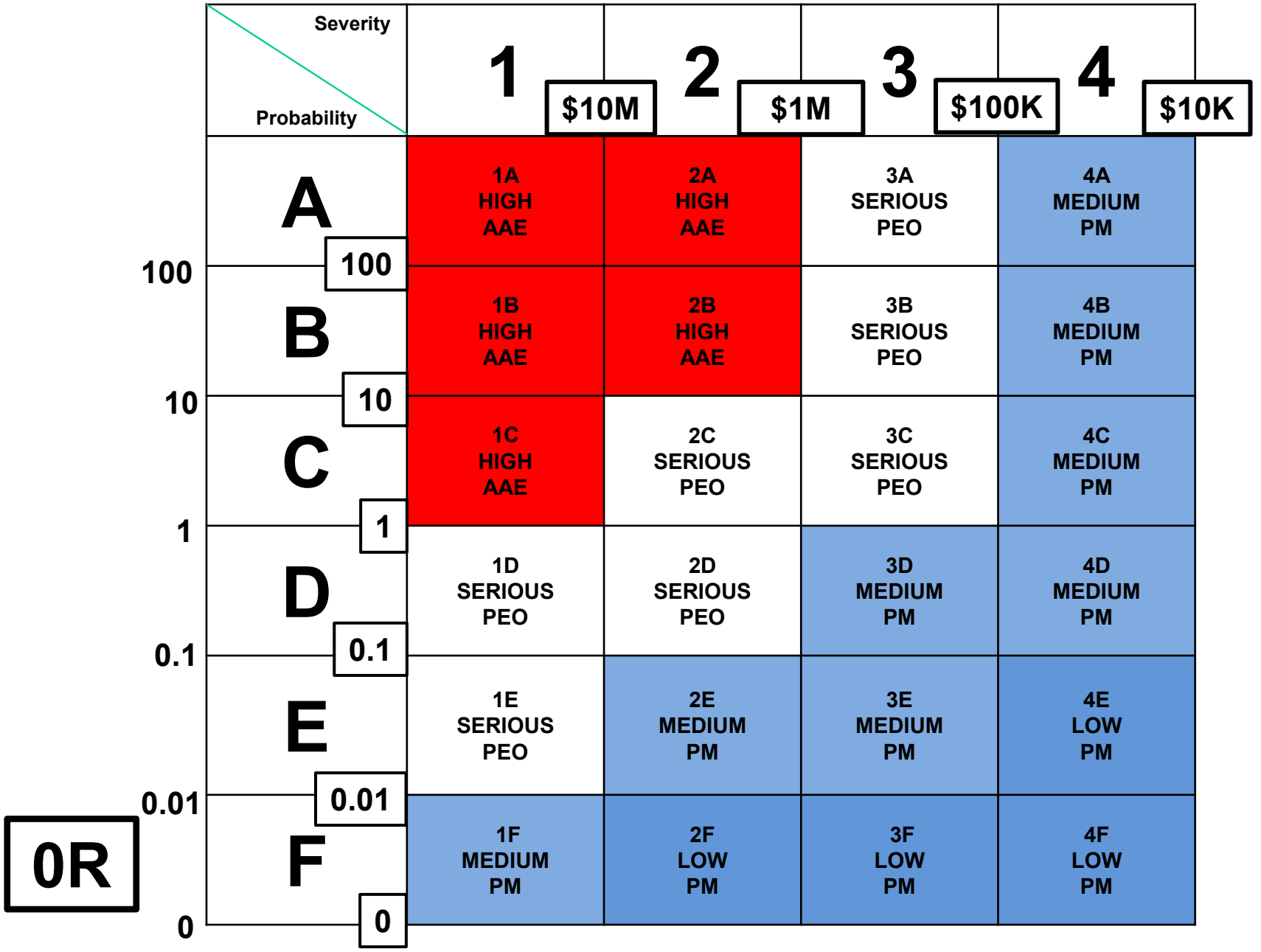
PEO Aviation

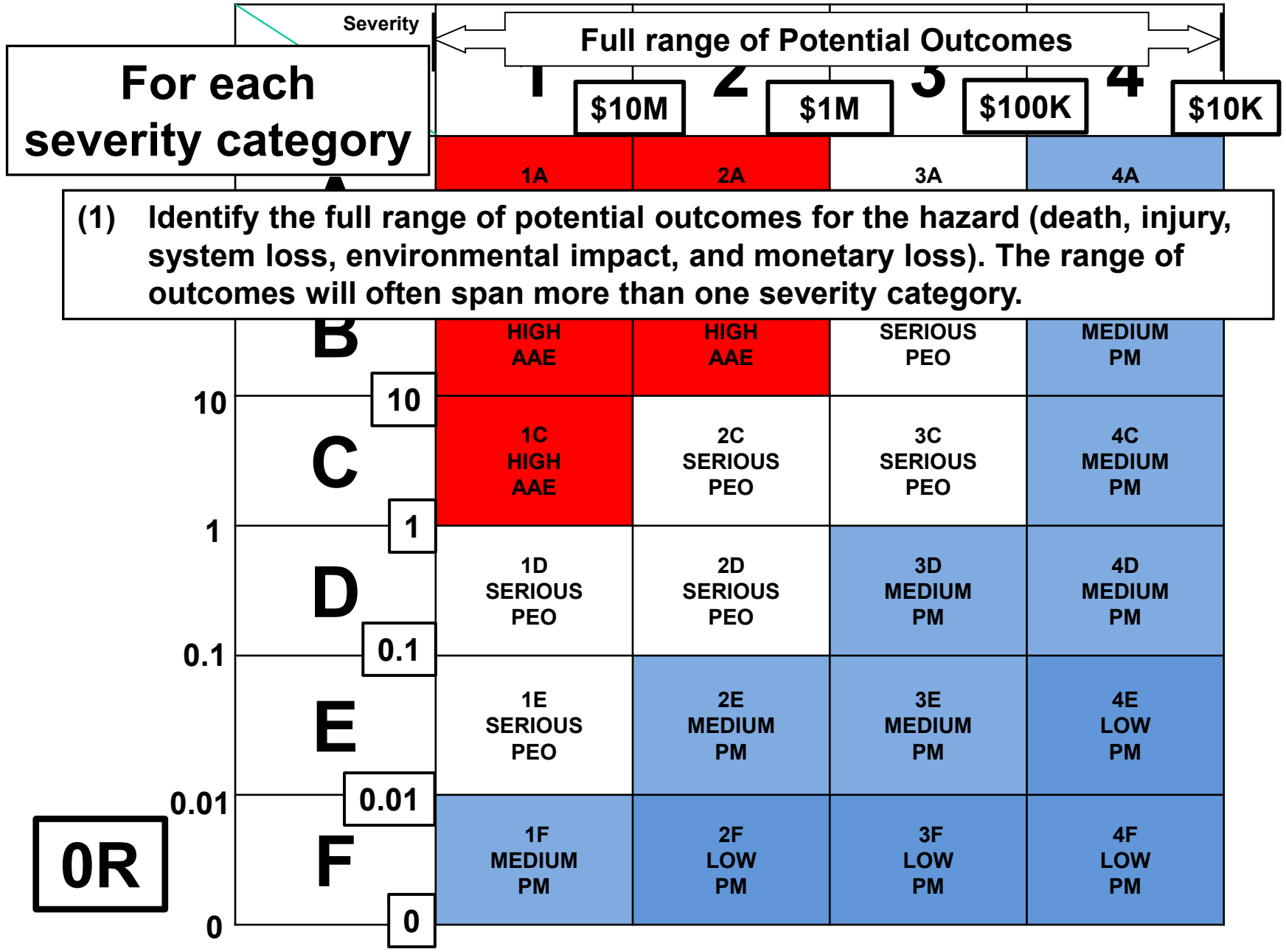


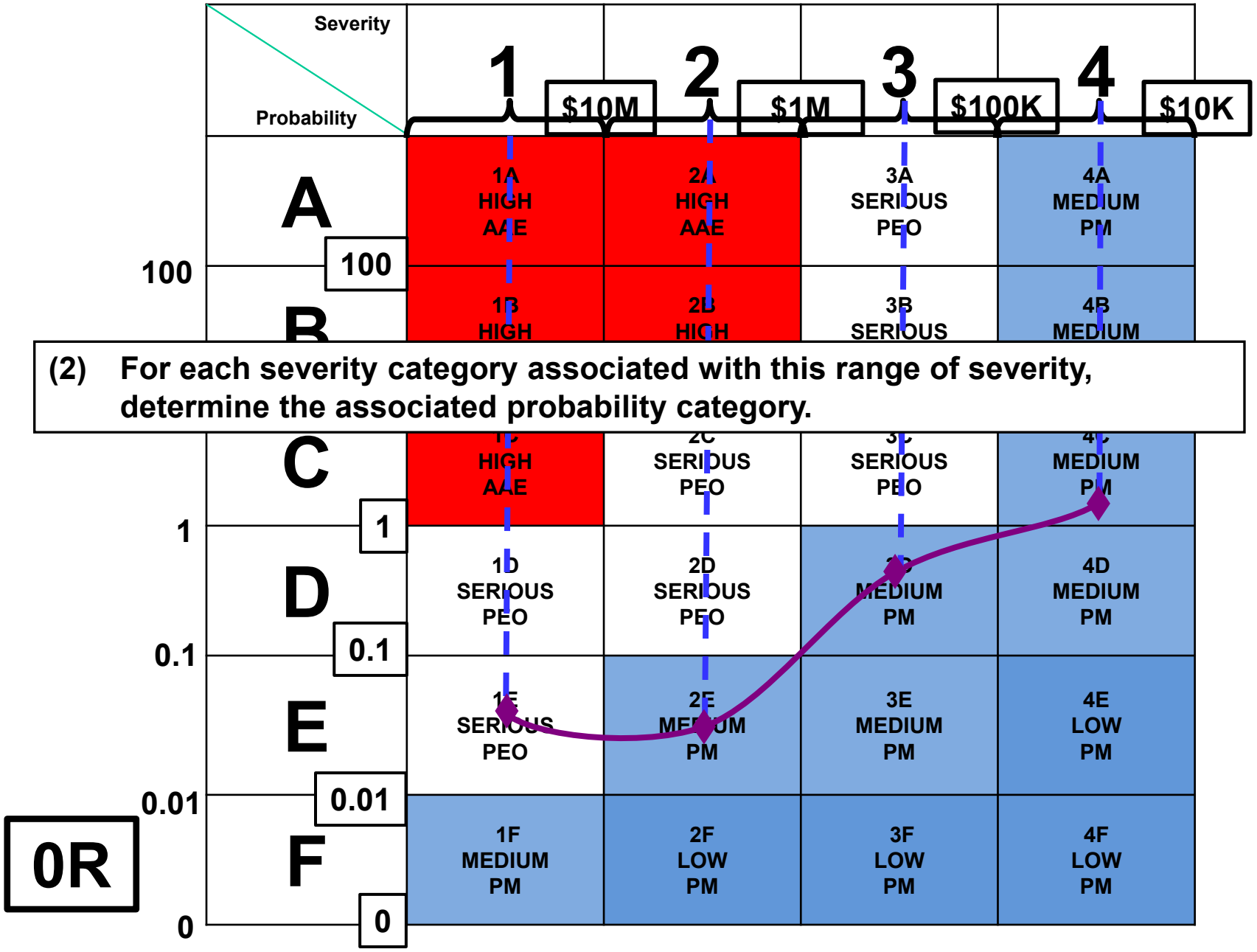
0R

Topics for this Tutorial

- Purpose of a Hazard Risk Matrix
- Understanding the Attributes of a well-designed risk assessment matrix
- **How to Assign a Risk Assessment Code**
- Understanding Probability
- Building an Expanded Matrix
- Plotting Accidents on a Matrix
- Using Relative Risk Values
- Building Hazard Risk Profiles
- Impact on Software Safety Matrices

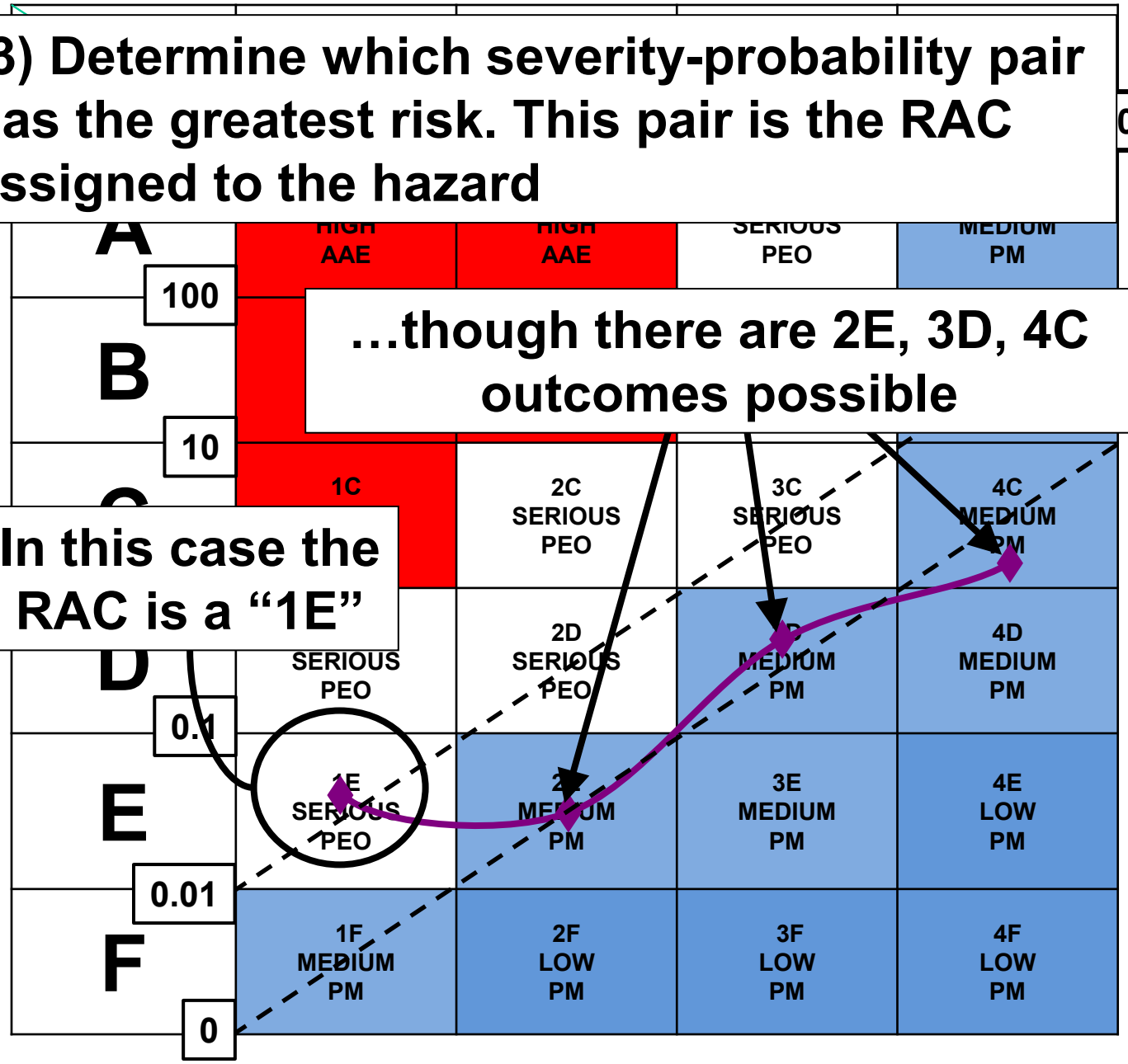

Severity
Probability
1
$10M
2
$1M
3
$100K
4
$10K
A
100
B
10
C
1
D
0.1
E
0.01
F
0
0R
1A HIGH AAE
2A HIGH AAE
3A SERIOUS PEO
4A MEDIUM PM
1B HIGH AAE
2B HIGH AAE
3B SERIOUS PEO
4B MEDIUM PM
1C HIGH AAE
2C SERIOUS PEO
3C SERIOUS PEO
4C MEDIUM PM
1D SERIOUS PEO
2D SERIOUS PEO
3D MEDIUM PM
4D MEDIUM PM
1E SERIOUS PEO
2E MEDIUM PM
3E MEDIUM PM
4E LOW PM
1F MEDIUM PM
2F LOW PM
3F LOW PM
4F LOW PM


For each severity category
(1) Identify the full range of potential outcomes for the hazard (death, injury, system loss, environmental impact, and monetary loss). The range of outcomes will often span more than one severity category.
Severity
Full range of Potential Outcomes
1
$10M
2
$1M
3
$100K
4
$10K
1A
2A
3A
4A
B
HIGH AAE
HIGH AAE
SERIOUS PEO
MEDIUM PM
10
10
C
1C HIGH AAE
2C SERIOUS PEO
3C SERIOUS PEO
4C MEDIUM PM
1
1
D
1D SERIOUS PEO
2D SERIOUS PEO
3D MEDIUM PM
4D MEDIUM PM
0.1
0.1
E
1E SERIOUS PEO
2E MEDIUM PM
3E MEDIUM PM
4E LOW PM
0.01
0.01
F
1F MEDIUM PM
2F LOW PM
3F LOW PM
4F LOW PM
0
0
0R



(2) For each severity category associated with this range of severity, determine the associated probability category.

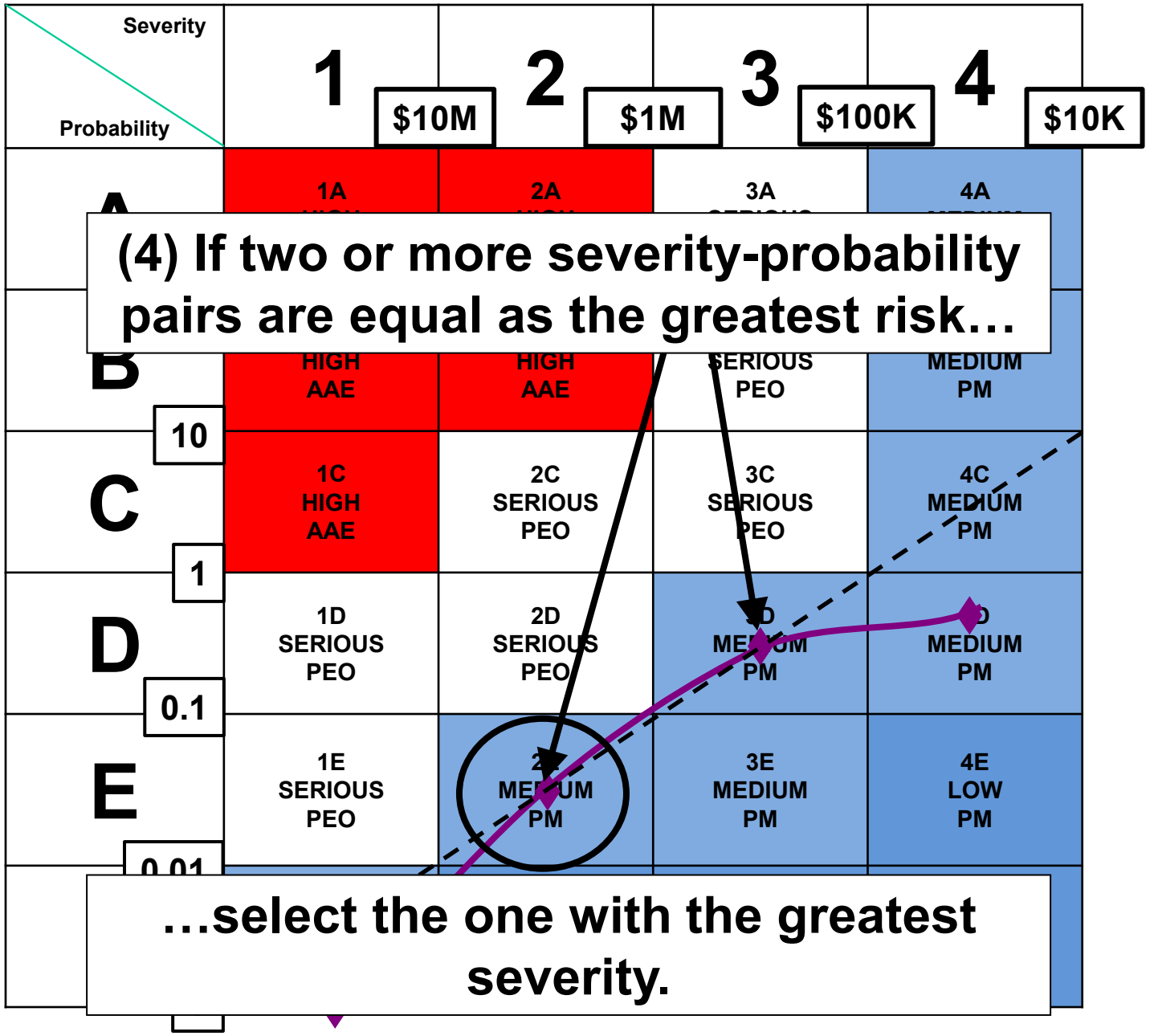
(3) Determine which severity-probability pair has the greatest risk. This pair is the RAC assigned to the hazard



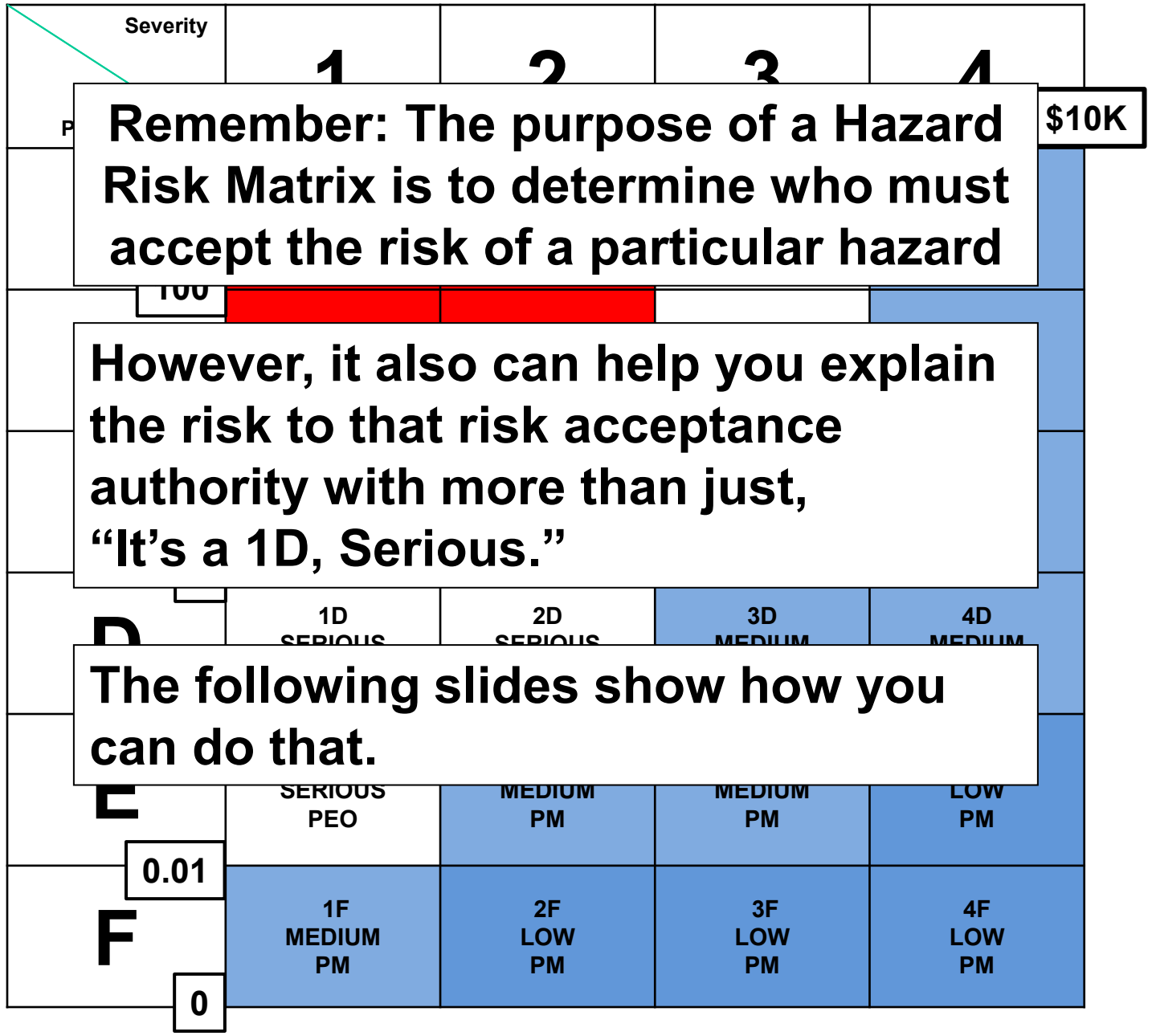
…though there are 2E, 3D, 4C outcomes possible

In this case the RAC is a "1E"

0R


Severity
Probability
1
$10M
2
$1M
3
$100K
4
$10K
A
1A
2A
3A
4A
B
10
HIGH
AAE
HIGH
AAE
SERIOUS
PEO
MEDIUM
PM
C
1
1C
HIGH
AAE
2C
SERIOUS
PEO
3C
SERIOUS
PEO
4C
MEDIUM
PM
D
0.1
1D
SERIOUS
PEO
2D
SERIOUS
PEO
MEDIUM
PM
MEDIUM
PM
E
0.01
1E
SERIOUS
PEO
MEDIUM
PM
3E
MEDIUM
PM
4E
LOW
PM
(4) If two or more severity-probability pairs are equal as the greatest risk…
…select the one with the greatest severity.

0R



Remember: The purpose of a Hazard Risk Matrix is to determine who must accept the risk of a particular hazard

However, it also can help you explain the risk to that risk acceptance authority with more than just, "It's a 1D, Serious."

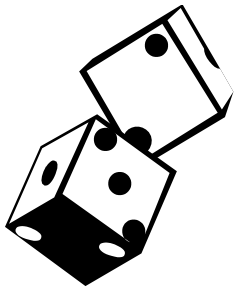
The following slides show how you can do that.

0R

Topics for this Tutorial

- Purpose of a Hazard Risk Matrix
- Understanding the Attributes of a well-designed risk assessment matrix
- How to Assign a Risk Assessment Code
- **Understanding Probability**
- Building an Expanded Matrix
- Plotting Accidents on a Matrix
- Using Relative Risk Values
- Building Hazard Risk Profiles
- Impact on Software Safety Matrices

Understanding Probability

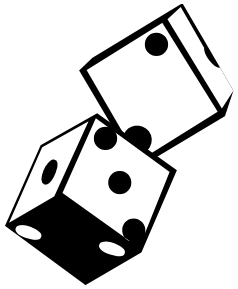


Probability:

“A number expressing the likelihood that a specific event will occur, expressed as the ratio of the number of actual occurrences to the number of possible occurrences.”

- The American Heritage® Dictionary of the English Language, Fourth Edition

Understanding Probability



Math Definition:

- **Repeat a random experiment “n” number of times.**
- **If a specific outcome has occurred “f” times in these n trials, the number “f” is the frequency of the outcome.**
- **The ratio f/n is the relative frequency of the outcome.**
- **A relative frequency is usually very unstable for small values of “n,” but it tends to stabilize about some number “p” as “n” increases.**
- **The number “p” is the probability of the outcome.**

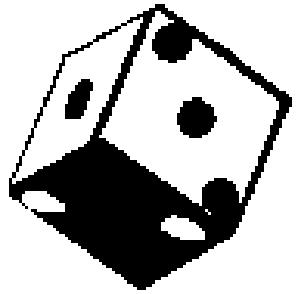
$$p = f / n$$

for very large values of n

Understanding Probability

Simple example:

Probability of rolling a “3” with one die.



Roll #1 - “5”, f/n = 0/1 = 0

Roll #2 - “2”, f/n = 0/2 = 0

Roll #3 - “3”, f/n = 1/3 = .333…

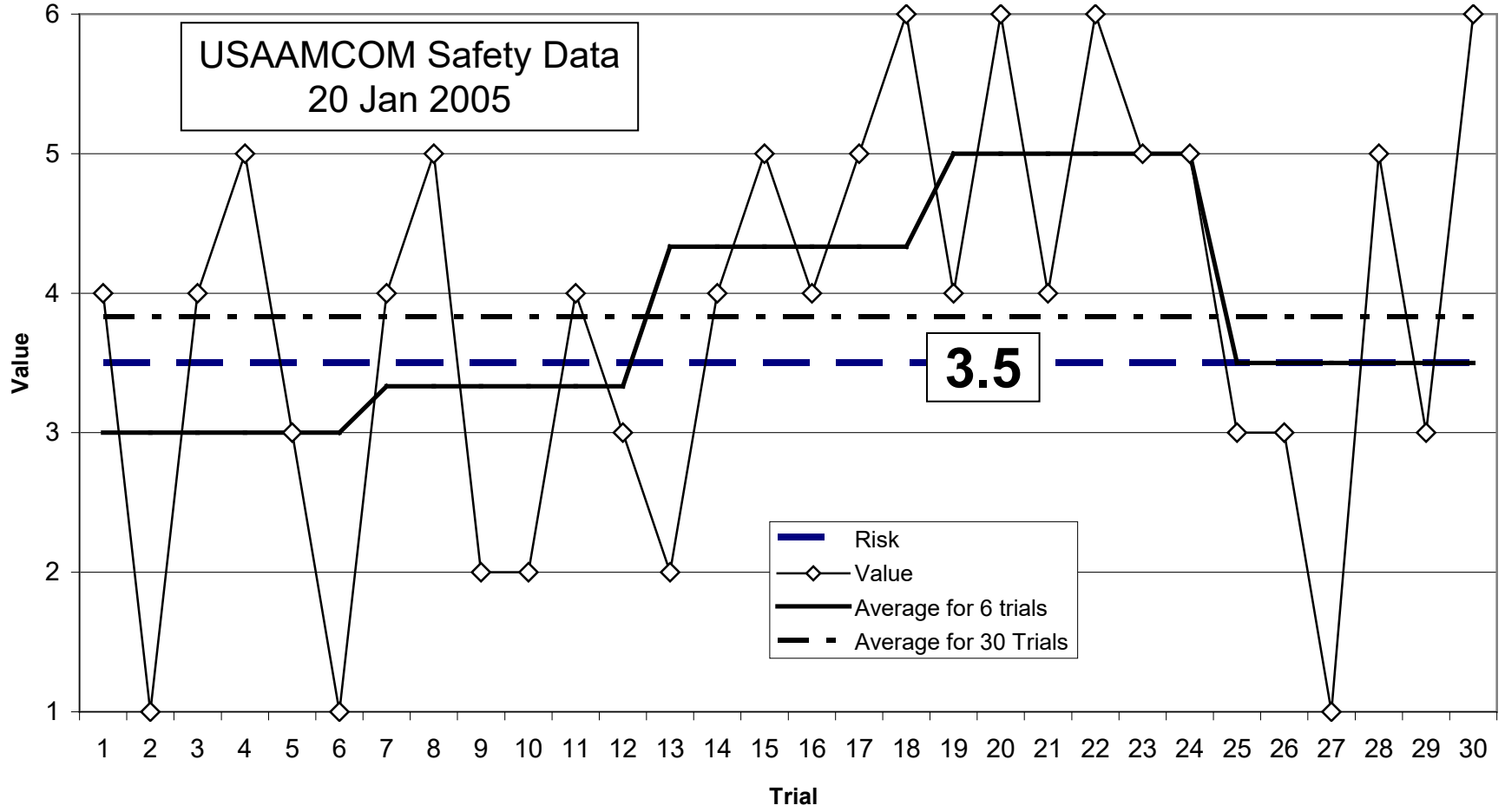
Roll #4 - “4”, f/n = 1/4 = .25

Roll #1,000: 163 “3”s, f/n = 163/1000 = .163

Rolls approach infinity f/n = .166666….

Rolling Dice

Roll a single die 30 times. The expected value of each roll is 3.5. What you actually get is somewhat different.



Understanding Probability

Hazard: Helicopter strikes wire; results in Class A mishap

Probability: 4.406E-06 occurrences per flight hour

1 Flight Hr, no mishap, rate = 0

1,000 Flight Hrs, no mishap, rate = 0

176,182 Flight Hrs, 1st mishap, rate = 5.676E-06 /flt hr

274,539 Flight Hrs, 2nd mishap, rate = 7.285E-06 /flt hr

700,462 Flt Hrs, 3rd mishap, rate = 4.283E-06 /flt hr

10,000,000 Flt Hrs, 46 mishaps, rate = 4.600E-06 /flt hr

1,000,000,000 Hrs, 4407 mishaps, rate = 4.407E-06 /flt hr

Flight hours approach infinity, rate = 4.406E-06 /flt hr

Topics for this Tutorial

- Purpose of a Hazard Risk Matrix
- Understanding the Attributes of a well-designed risk assessment matrix
- How to Assign a Risk Assessment Code
- Understanding Probability
- **Building an Expanded Matrix**
- Plotting Accidents on a Matrix
- Using Relative Risk Values
- Building Hazard Risk Profiles
- Impact on Software Safety Matrices

PEO Aviation Risk Decision Authority Matrix

Probability \ Severity	1 $10M	2 $1M	3 $100K	4 $10K
A 100	1A HIGH AAE	2A HIGH AAE	3A SERIOUS PEO	4A MEDIUM PM
B 10	1B HIGH AAE	2B HIGH AAE	3B SERIOUS PEO	4B MEDIUM PM
C 1	1C HIGH AAE	2C SERIOUS PEO	3C SERIOUS PEO	4C MEDIUM PM
D 0.1	1D SERIOUS PEO	2D SERIOUS PEO	3D MEDIUM PM	4D MEDIUM PM
E 0.01	1E SERIOUS PEO	2E MEDIUM PM	3E MEDIUM PM	4E LOW PM
F 0	1F MEDIUM PM	2F LOW PM	3F LOW PM	4F LOW PM

0R

Applying Probability Classifications to a military helicopter

Fleet Size = 368 aircraft

Utilization = 240 hours/year

Life = 12 years/aircraft

Aircraft Life = 240 x 12
= 2,880 hours

Fleet Exposure Hours = 368 x 240 x 12
= 1,059,840 hours

Fleet Hours per Year = 368 x 240
= 88,320 hours

US Army PEO Aviation Enhanced Matrix

	Events per Flight Hour	Flight Hours per Event	Events per 100,000 Flt Hrs
Frequent **A**	10^{-3}	1,000	100
Probable **B**	10^{-4}	10,000	10
Occasional **C**	10^{-5}	100,000	1
Remote **D**	10^{-6}	1,000,000	0.1
Improbable **E**	10^{-7}	10,000,000	0.01
Very Improbable **F**	0		0
Zero Risk **0R**			

US Army PEO Aviation Enhanced Matrix

	Events per Flight	Flight Hours per	Events per 100,000	Events per	Years per
Probable B	10^{-4}	10,000	10	8.832	0.113
Occasional C	10^{-5}	100,000	1	0.8832	1.13
Remote D	10^{-6}	1,000,000	0.1	0.0883	11.3
Improbable E	10^{-7}	10,000,000	0.01	0.00883	113
Very Improbable F	0		0	0	
Zero Risk 0R					

$$\frac{88{,}320 \text{ ~~flt hrs~~}}{\text{Year}} \times \frac{10 \text{ Events}}{100{,}000 \text{ ~~flt hrs~~}} = \frac{8.832 \text{ Events}}{\text{Year}}$$

US Army PEO Aviation Enhanced Matrix

	Events per Flight Hour	Flight Hours per Event	Events per 100,000 Flt Hrs	Events per Year	Years per Event
Frequent **A**	10^{-3}	1,000	100	88.32	0.0113
Probable **B**	10^{-4}	10,000	10	8.832	0.113
Occasional **C**	10^{-5}	100,000	1	0.8832	1.13
Remote **D**	10^{-6}	1,000,000	0.1	0.0883	11.3
Improbable **E**	10^{-7}	10,000,000	0.01	0.00883	113
Very Improbable **F**	0		0	0	
Zero Risk **0R**					

US Army PEO Aviation Enhanced Matrix

$$\frac{1{,}059{,}840 \text{ ~~flt hrs~~}}{1 \text{ fleet life}} \times \frac{10 \text{ Events}}{100{,}000 \text{ ~~flt hrs~~}} = \frac{105.98 \text{ Events}}{1 \text{ Fleet Life}}$$

	Events per Flight	Flight Hours per	Events per 100,000	Events per	Years per	Event per Fleet	Fleet Life per
Probable B	10^{-4}	10,000	10	8.832	0.113	105.98	0.00944
Occasional C	10^{-5}	100,000	1	0.8832	1.13	10.598	0.0944
Remote D	10^{-6}	1,000,000	0.1	0.0883	11.3	1.0598	0.944
Improbable E	10^{-7}	10,000,000	0.01	0.00883	113	0.106	9.44
Very Improbable F	0		0	0		0	
Zero Risk 0R							

US Army PEO Aviation Enhanced Matrix

	Events per Flight Hour	Flight Hours per Event	Events per 100,000 Flt Hrs	Events per Year	Years per Event	Event per Fleet Life	Fleet Life per Event
Frequent **A**	10^{-3}	1,000	100	88.32	0.0113	1,060	0.000944
Probable **B**	10^{-4}	10,000	10	8.832	0.113	105.98	0.00944
Occasional **C**	10^{-5}	100,000	1	0.8832	1.13	10.598	0.0944
Remote **D**	10^{-6}	1,000,000	0.1	0.0883	11.3	1.0598	0.944
Improbable **E**	10^{-7}	10,000,000	0.01	0.00883	113	0.106	9.44
Very Improbable **F**	0		0	0		0	
Zero Risk **0R**							

US Army PEO Aviation Enhanced Matrix

	Events per Flight Hour	Flight Hours per Event	Events per 100,000 Flt Hrs	Events per Year	Years per Event	Event per Fleet Life	Fleet Life per Event
Frequent **A**	10^{-3}	1,000	100	88.32	0.0113	1,060	0.000944
Probable **B**	10^{-4}	10,000	10	8.832	0.113	105.98	0.00944
Occasional **C**	10^{-5}	100,000	1	0.8832	1.13	10.598	0.0944
Remote **D**	10^{-6}	1,000,000	0.1	0.0883	11.3	1.0598	0.944
Improbable **E**	10^{-7}	10,000,000	0.01	0.00883	113	0.106	9.44
Very Improbable **F**	0		0	0		0	
Zero Risk **0R**							

Numbers greater than 1 are easier to comprehend

US Army PEO Aviation Enhanced Matrix

Input
Calculated

Assumptions		
Fleet Size:	368	aircraft
Utilization:	240.0	hours/yr
Aircraft Life:	12	years
Calculations		
Aircraft Exposure Hours:	2,880	hours
Fleet Exposure Hours:	1,059,840	hours
Fleet Hours per Year:	88,320	hours

	Events per Flight Hour	Flight Hours per Event	Events per 100,000 Flt Hrs	1 $10M	2 $1M	3 $100K	4	Fleet-wide Events per Year	Fleet-wide Years per Event	Fleet-wide Event per Fleet Life	Fleet-wide Fleet Life per Event
A	10^{-3}	1,000	100	1A	2A	3A	4A	88.32	0.0113	1,060	0.000944
B	10^{-4}	10,000	10	1B	2B	3B	4B	8.832	0.113	105.98	0.00944
C	10^{-5}	100,000	1	1C	2C	3C	4C	0.8832	1.13	10.598	0.0944
D	10^{-6}	1,000,000	0.1	1D	2D	3D	4D	0.0883	11.3	1.0598	0.944
E	10^{-7}	10,000,000	0.01	1E	2E	3E	4E	0.00883	113	0.106	9.44
F	0		0	1F	2F	3F	4F	0		0	
0R											

High AAE

Serious PEO

Medium PM

Low PM

Consequences of Risk Acceptance

Assumptions		
Fleet Size:	368	aircraft
Utilization:	240.0	hours/yr
Aircraft Life:	12	years
Calculations		
Aircraft Exposure Hours:	2,880	hours
Fleet Exposure Hours:	1,059,840	hours
Fleet Hours per Year:	88,320	hours

	Events per Flight Hour	Flight Hours per Event	Events per 100,000 Flt Hrs	1	2	3	4	Fleet-wide: Events per Year	Years per Event	Event per Fleet Life	Fleet Life per Event
				$10M	$1M		$100K				
A	10^{-3}	1,000	100	1A	2A	3A	4A	88.32	0.0113	1,060	0.000944
B	10^{-4}	10,000	10	1B	2B	3B	4B	8.832	0.113	105.98	0.00944
C	10^{-5}	100,000	1	1C	2C	3C	4C	0.8832	1.13	10.598	0.0944
D	10^{-6}	1,000,000	0.1	1D	2D	3D	4D	0.0883	11.3	1.0598	0.944
E	10^{-7}	10,000,000	0.01	1E	2E	3E	4E	0.00883	113	0.106	9.44
F	0		0	1F	2F	3F	4F	0		0	
0R											

High AAE

Serious PEO

Medium PM

Low PM

2 - 10

Consequences of Risk Acceptance

Consequences of Risk Acceptance:
On the order of 2 to 10 Class A accidents due to this hazard over the remaining life cycle of the aircraft.

									Fleet-wide			
				Aircraft Exposure Hours:		2,880 hours						
				Fleet Exposure Hours:		1,059,840 hours						
				Fleet Hours per Year:		88,320 hours						
	Events per Flight Hour	Flight Hours per Event	Events per 100,000 Flt Hrs	1	2	3	4		Events per Year	Years per Event	Event per Fleet Life	Fleet Life per Event
					$10M	$1M	$100K					
A	10^{-3}	1,000	100	1A	2A	3A	4A		88.32	0.0113	1,060	0.000944
B	10^{-4}	10,000	10	1B	2B	3B	4B		8.832	0.113	105.98	0.00944
C	10^{-5}	100,000	1	1C	2C	3C	4C		0.8832	1.13	10.598	0.0944
D	10^{-6}	1,000,000	0.1	1D	2D	3D	4D		0.0883	11.3	1.0598	0.944
E	10^{-7}	10,000,000	0.01	1E	2E	3E	4E		0.00883	113	0.106	9.44
F	0		0	1F	2F	3F	4F		0		0	
0R												

High AAE

Serious PEO

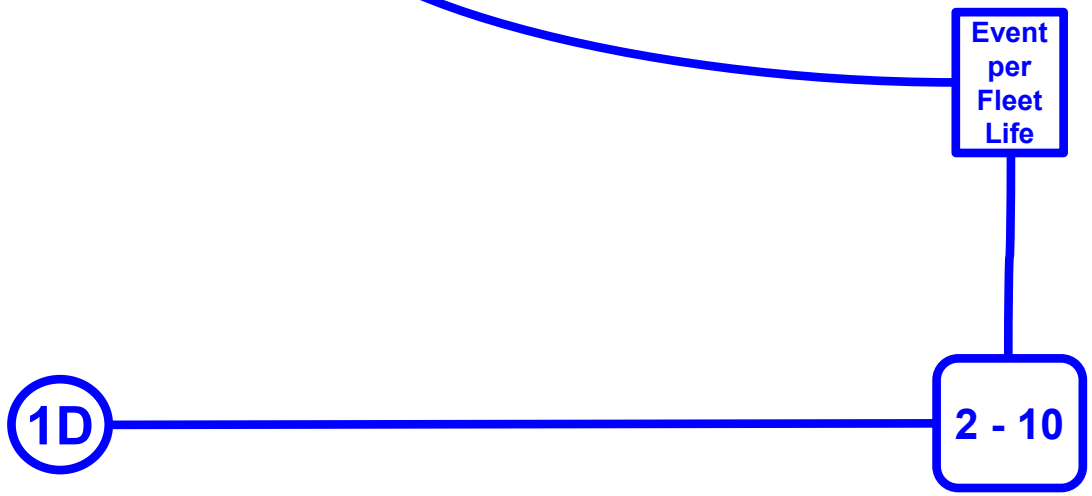
Medium PM

Low PM

2 - 10

Consequences of Risk Acceptance

Consequences of Risk Acceptance:
On the order of 2 to 10 Class A accidents due to this hazard over the remaining life cycle of the aircraft.

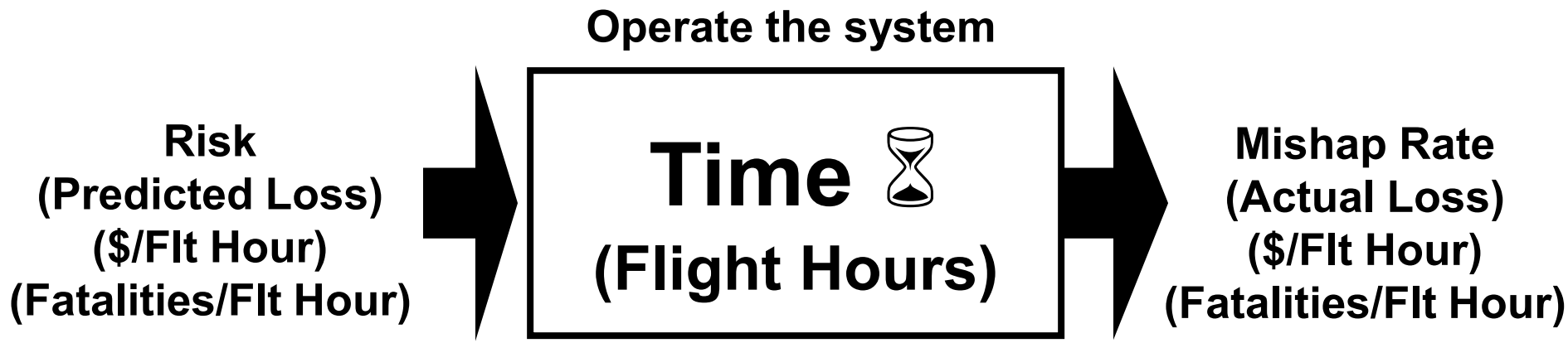


Topics for this Tutorial

- Purpose of a Hazard Risk Matrix
- Understanding the Attributes of a well-designed risk assessment matrix
- How to Assign a Risk Assessment Code
- Understanding Probability
- Building an Expanded Matrix
- **Plotting Accidents on a Matrix**
- Using Relative Risk Values
- Building Hazard Risk Profiles
- Impact on Software Safety Matrices

Mishap Risk & Mishap Loss

Mishap Risk over Time results in Mishap Loss



Mishap History

Based on this relationship between mishap risk and mishap loss, we can plot mishap histories on a risk matrix as follows:

$$\text{Severity} = \frac{\text{Total Cost from Class A mishaps}}{\text{Total Number of Class A mishaps}}$$

$$= \frac{\$361,671,038}{59} = \$\ 6,130,018$$

$$\text{Probability} = \frac{\text{Total Number of Class A mishaps}}{\text{Total Hours Flown}}$$

$$= \frac{59}{1,588,597} = 3.714 \text{ mishaps / 100,000 Flt Hrs}$$

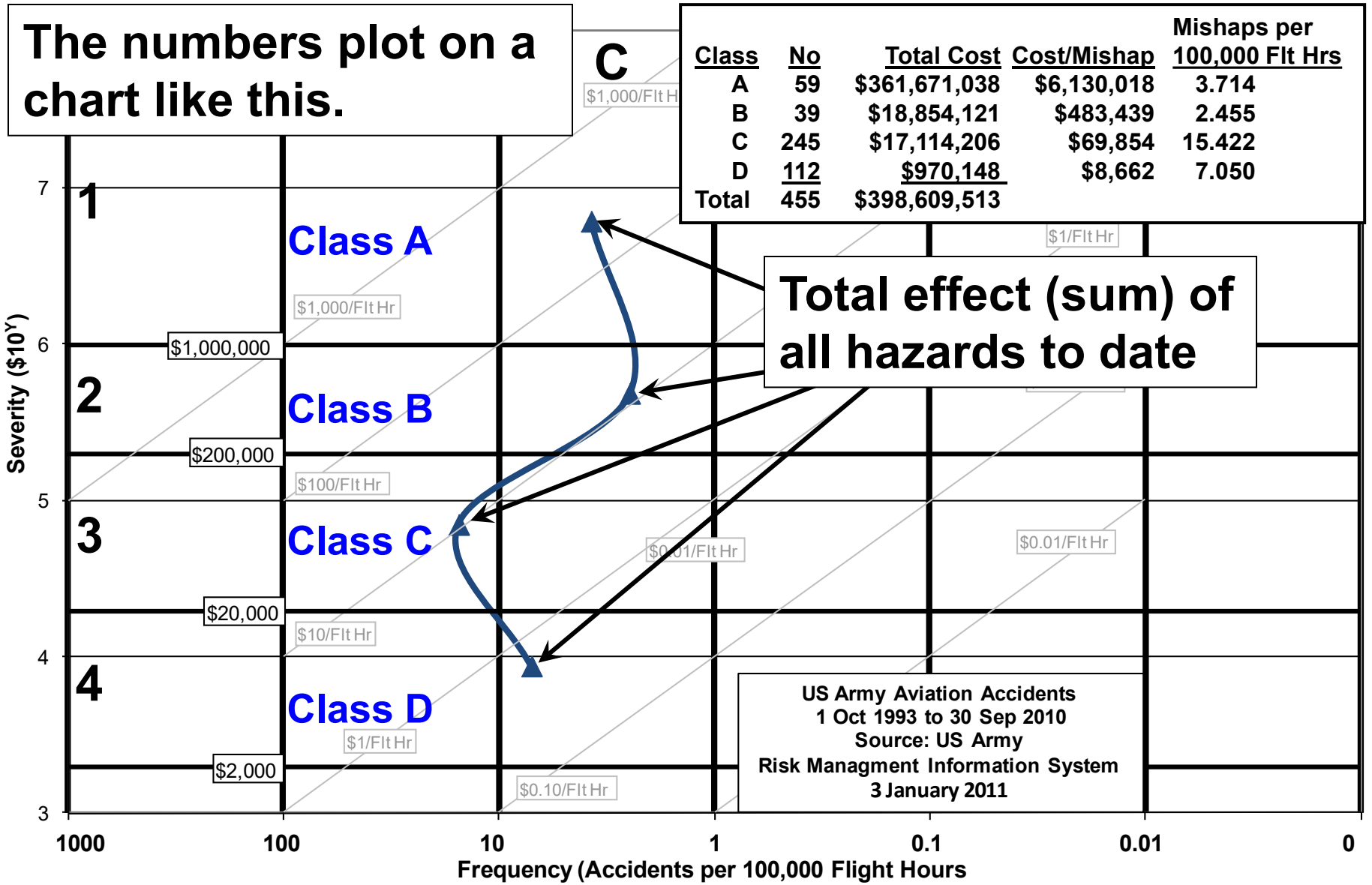
Mishap History

Class	No	Total Cost	Cost/Mishap	Mishaps per 100,000 Flt Hrs
A	59	$361,671,038	$6,130,018	3.714
B	39	$18,854,121	$483,439	2.455
C	245	$17,114,206	$69,854	15.422
D	112	$970,148	$8,662	7.050
Total	455	$398,609,513		

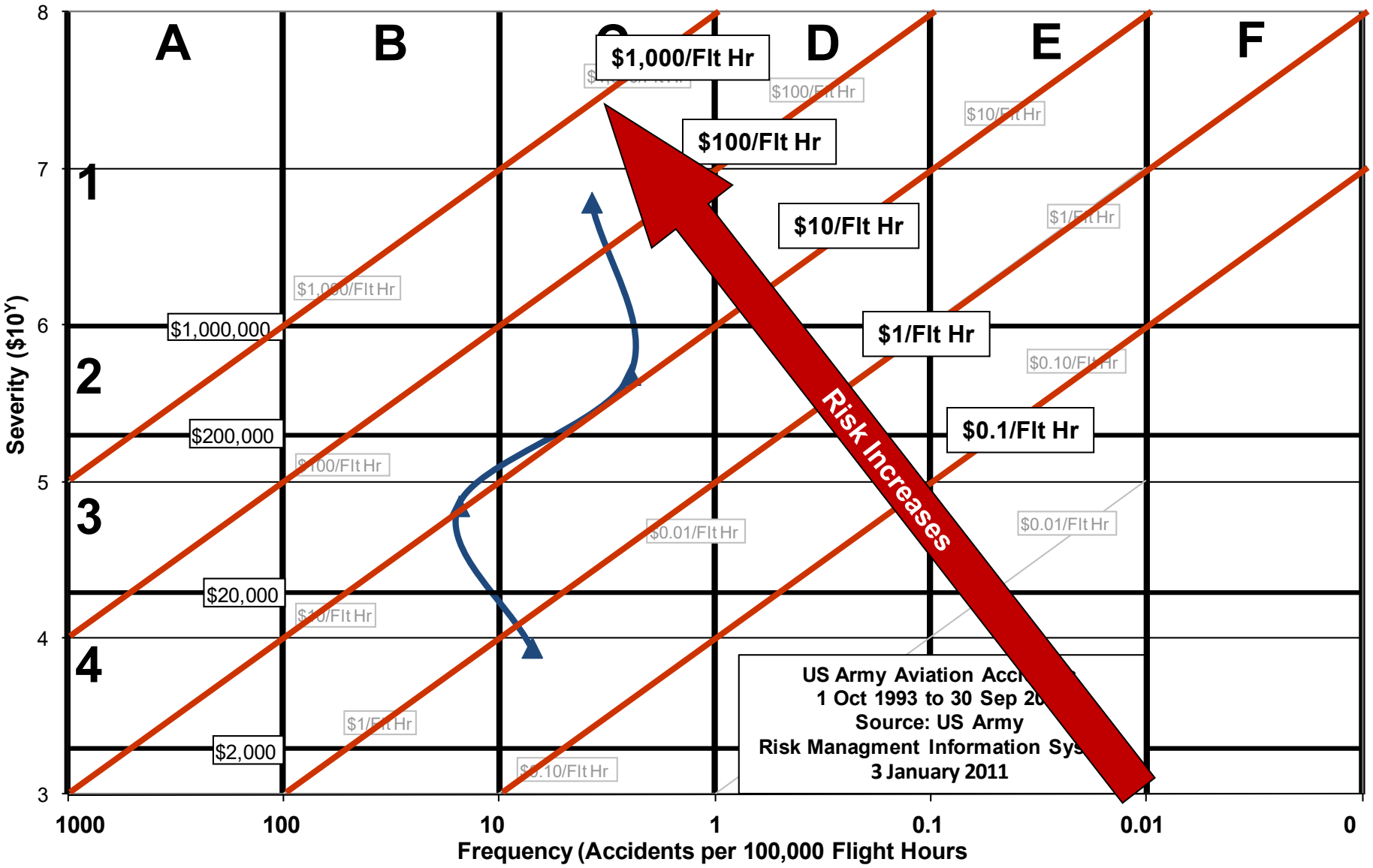
Mishaps

The numbers plot on a chart like this.

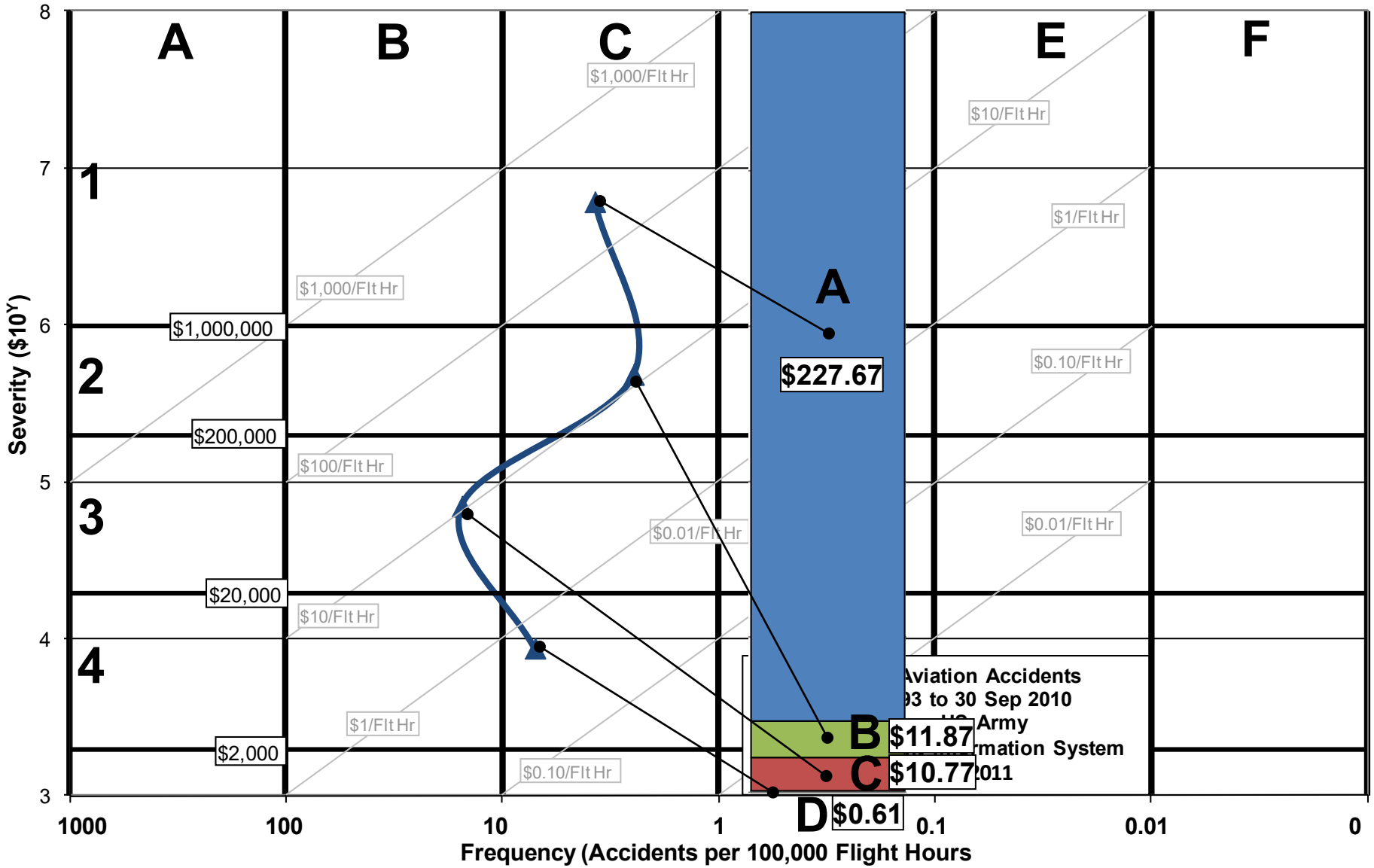
Class	No	Total Cost	Cost/Mishap	Mishaps per 100,000 Flt Hrs
A	59	$361,671,038	$6,130,018	3.714
B	39	$18,854,121	$483,439	2.455
C	245	$17,114,206	$69,854	15.422
D	112	$970,148	$8,662	7.050
Total	455	$398,609,513		



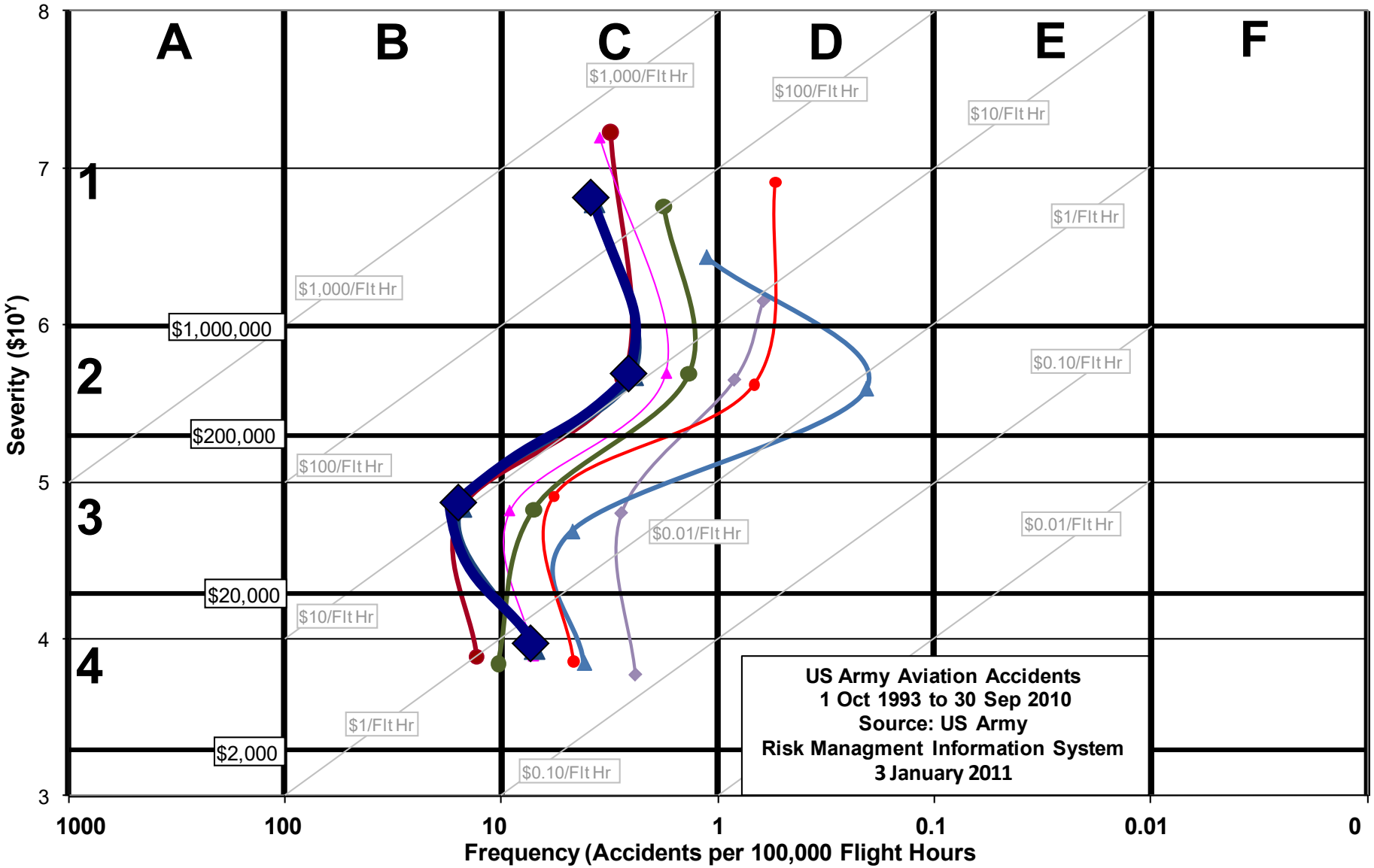
Mishaps


A
B
C
D
E
F
1
2
3
4
$1,000/Flt Hr
$100/Flt Hr
$10/Flt Hr
$1/Flt Hr
$0.1/Flt Hr
Risk Increases
$1,000,000
$200,000
$20,000
$2,000
Severity ($10^Y)
8
7
6
5
4
3
1000
100
10
1
0.1
0.01
0
Frequency (Accidents per 100,000 Flight Hours
US Army Aviation Acci
1 Oct 1993 to 30 Sep 20
Source: US Army
Risk Managment Information Sys
3 January 2011

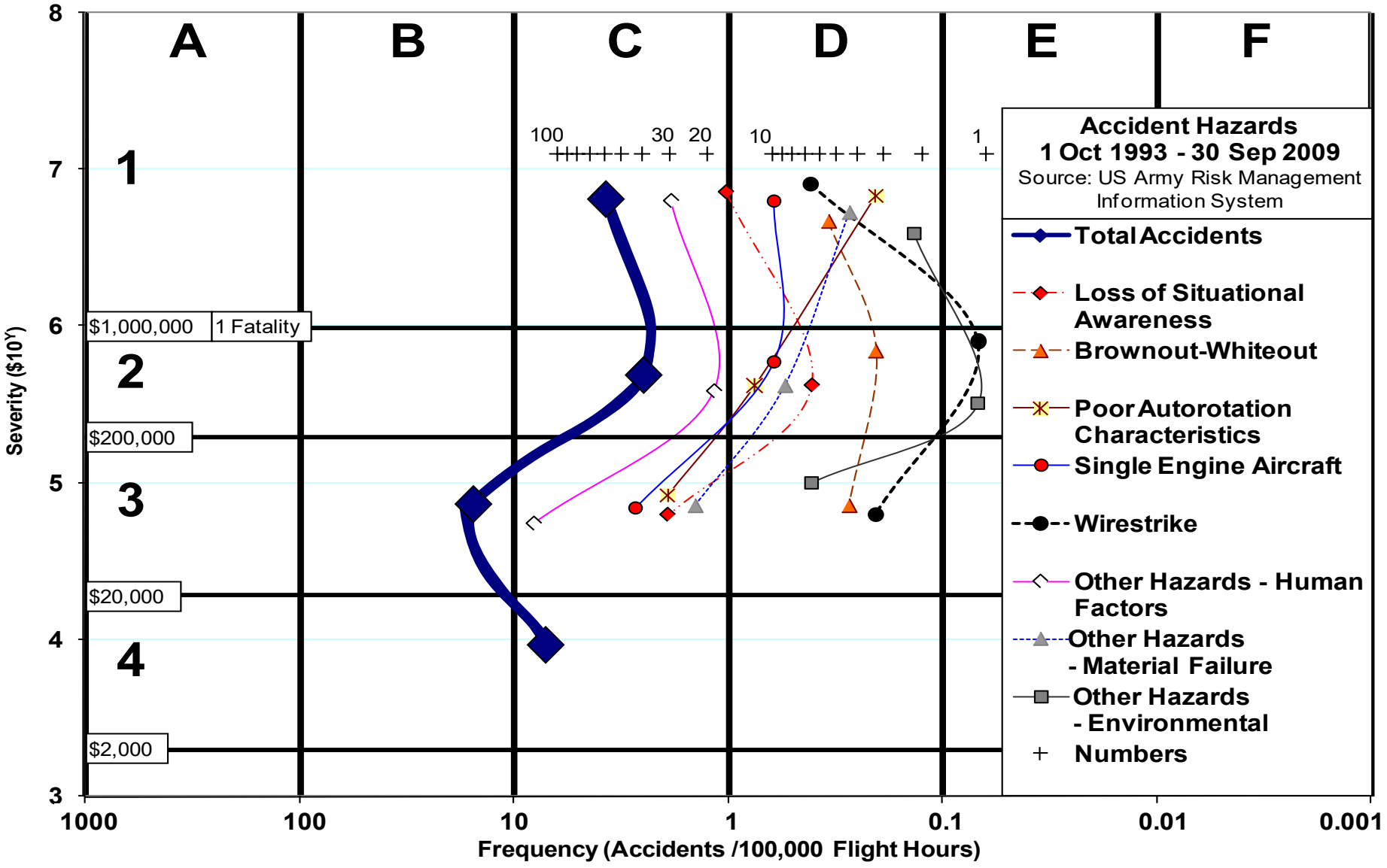
Mishaps


A
B
C
E
F
1
2
3
4
$1,000/Flt Hr
$10/Flt Hr
$1/Flt Hr
$0.10/Flt Hr
$0.01/Flt Hr
$100/Flt Hr
$1,000,000
$200,000
$20,000
$2,000
A
$227.67
B
$11.87
C
$10.77
D
$0.61
Aviation Accidents
93 to 30 Sep 2010
Army
rmation System
011
Severity ($10^Y)
8
7
6
5
4
3
1000
100
10
1
0.1
0.01
0
Frequency (Accidents per 100,000 Flight Hours

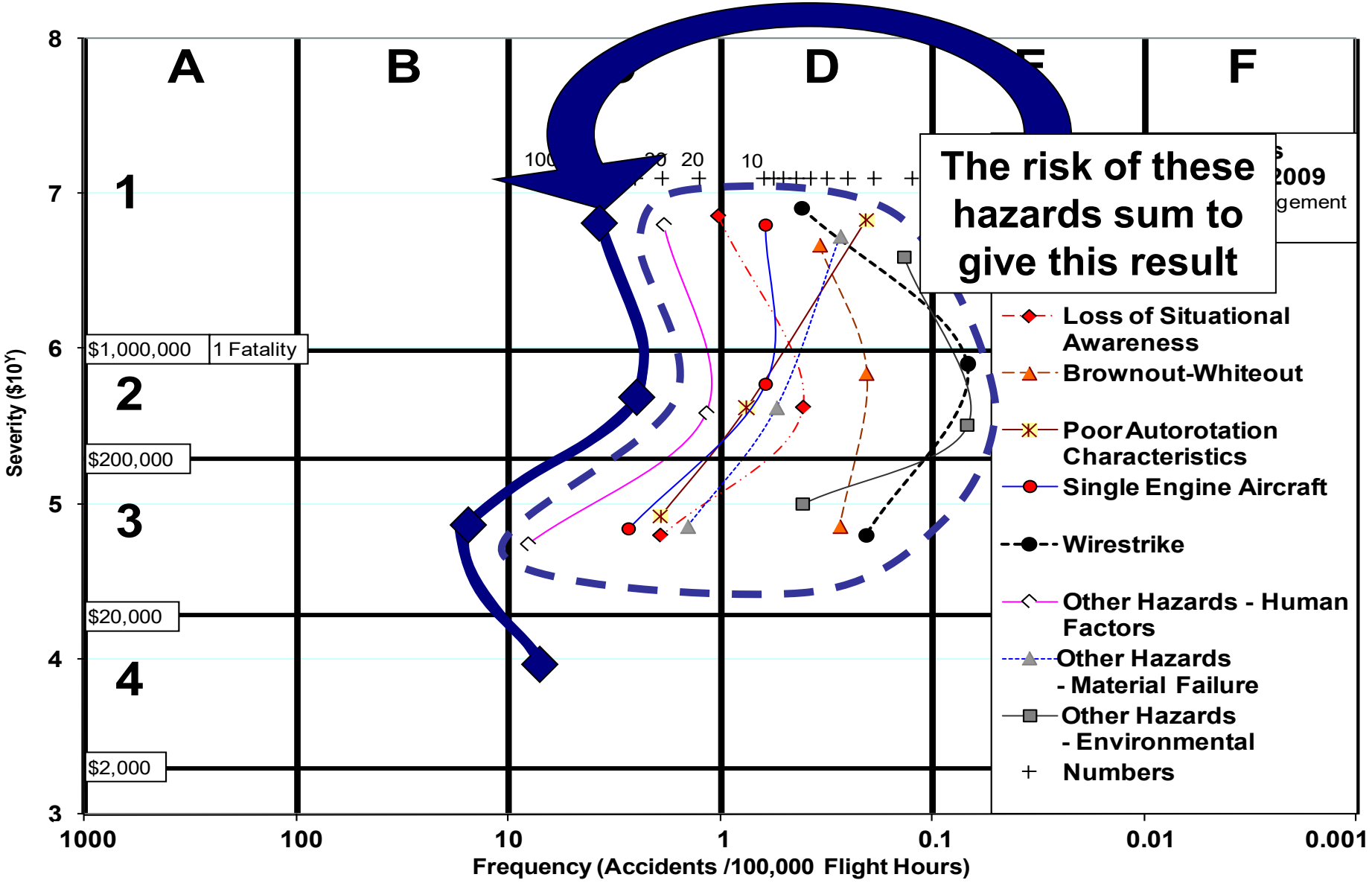
US Army Aviation Mishaps



US Army Aviation Mishaps



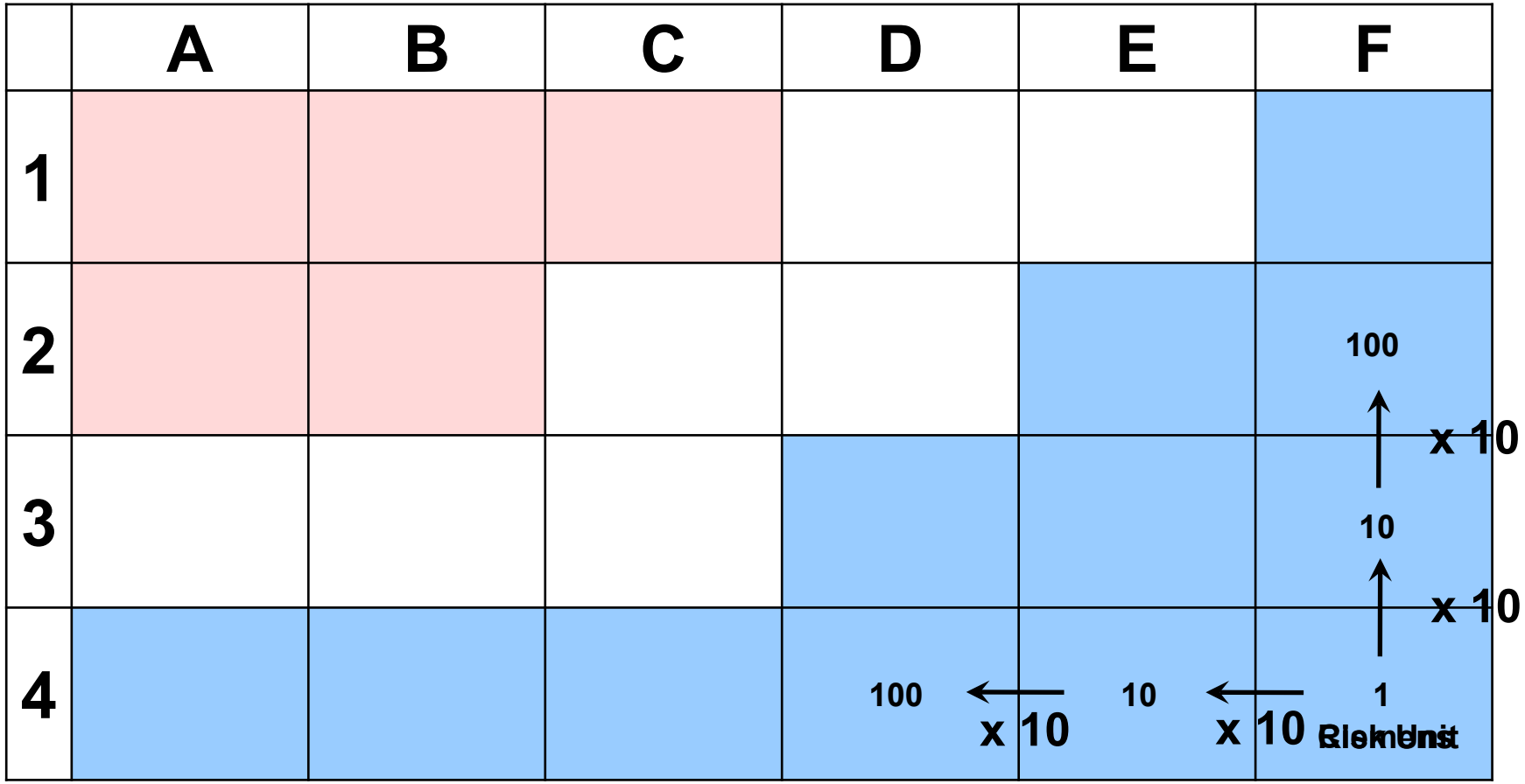
US Army Aviation Mishaps



Topics for this Tutorial

- Purpose of a Hazard Risk Matrix
- Understanding the Attributes of a well-designed risk assessment matrix
- How to Assign a Risk Assessment Code
- Understanding Probability
- Building an Expanded Matrix
- Plotting Accidents on a Matrix
- **Using Relative Risk Values**
- Building Hazard Risk Profiles
- Impact on Software Safety Matrices

Matrix Relative Risk Values
(Risk Units)(Clemens)



Matrix Relative Risk Values (Clemens)

	A	B	C	D	E	F
1	100,000,000	10,000,000	1,000,000	100,000	10,000	1,000
2	10,000,000	1,000,000	100,000	10,000	1,000	100
3	1,000,000	100,000	10,000	1,000	100	10
4	100,000	10,000	1,000	100	10	1

Helo A Hazard Distribution

	A	B	C	D	E	F
1				5	14	65
2				4	6	2
3			1	7	5	4
4				2	1	

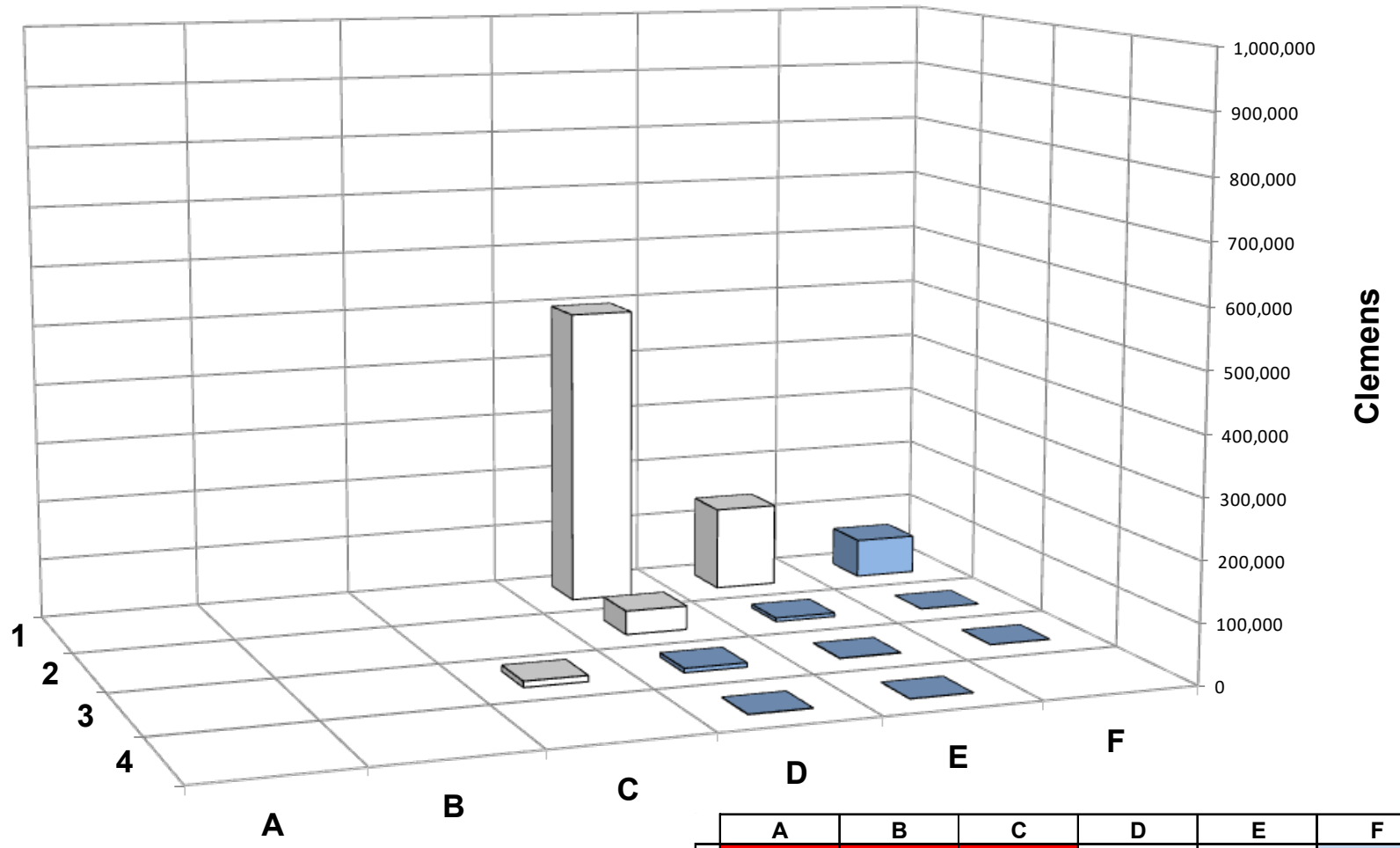
Helo A Matrix
Relative Values (Clemens)

	A	B	C	D	E	F
1				5 x 100,000 = 500,000	14 x 10,000 = 140,000	65 x 1,000 = 65,000
2				4 x 10,000 = 40,000	6 x 1,000 = 6,000	2 x 100 = 200
3			1 x 10,000 = 10,000	7 x 1,000 = 7,000	5 x 100 = 500	4 x 10 = 40
4				2 x 100 = 200	1 x 10 = 10	

Helo A Matrix
Relative Values (Clemens)

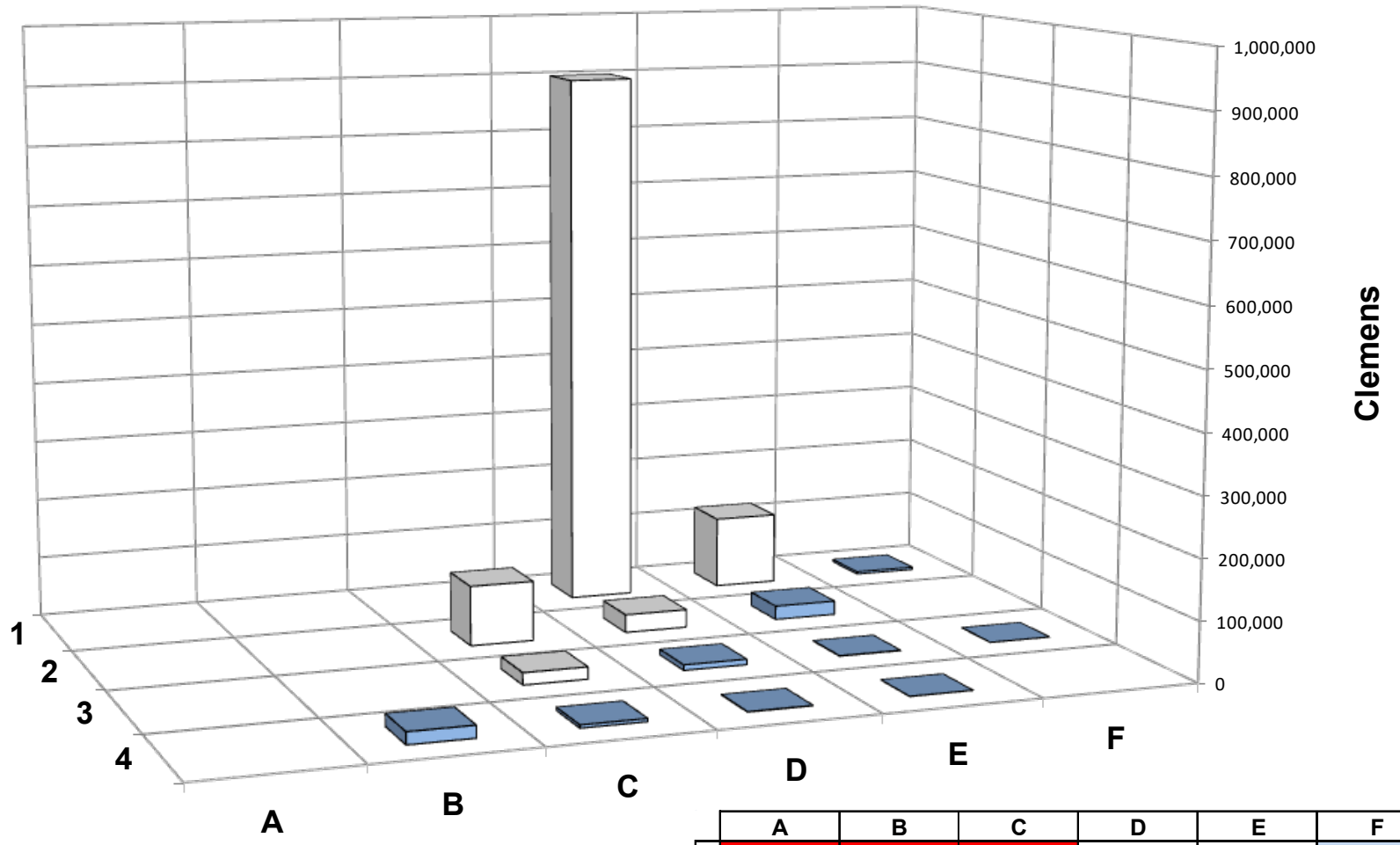
	A	B	C	D	E	F
1				500,000	140,000	65,000
2				40,000	6,000	200
3			10,000	7,000	500	40
4				200	10	

Helicopter A



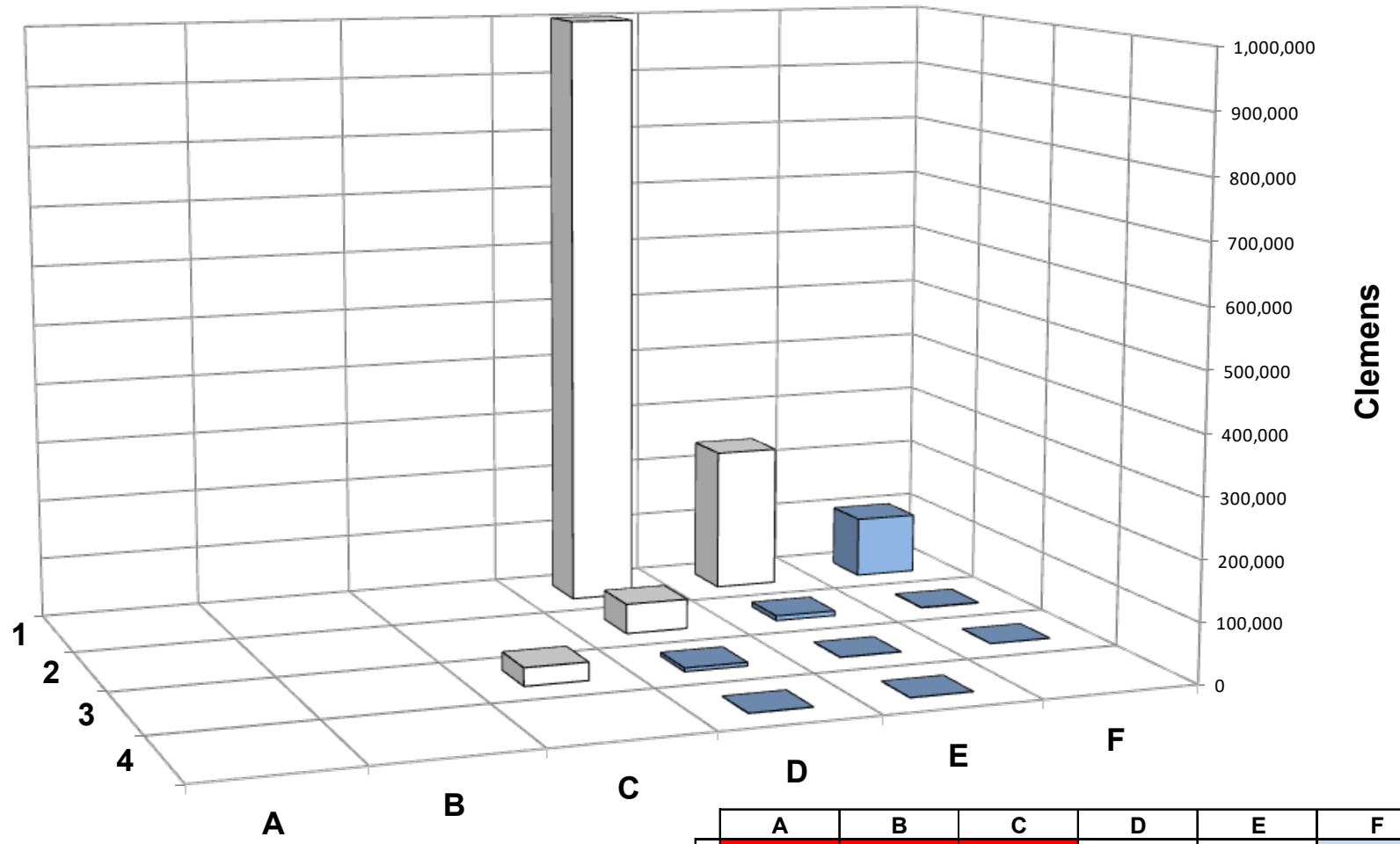
	A	B	C	D	E	F
1				5	14	65
2				4	6	2
3			1	7	5	4
4				2	1	

Helicopter B



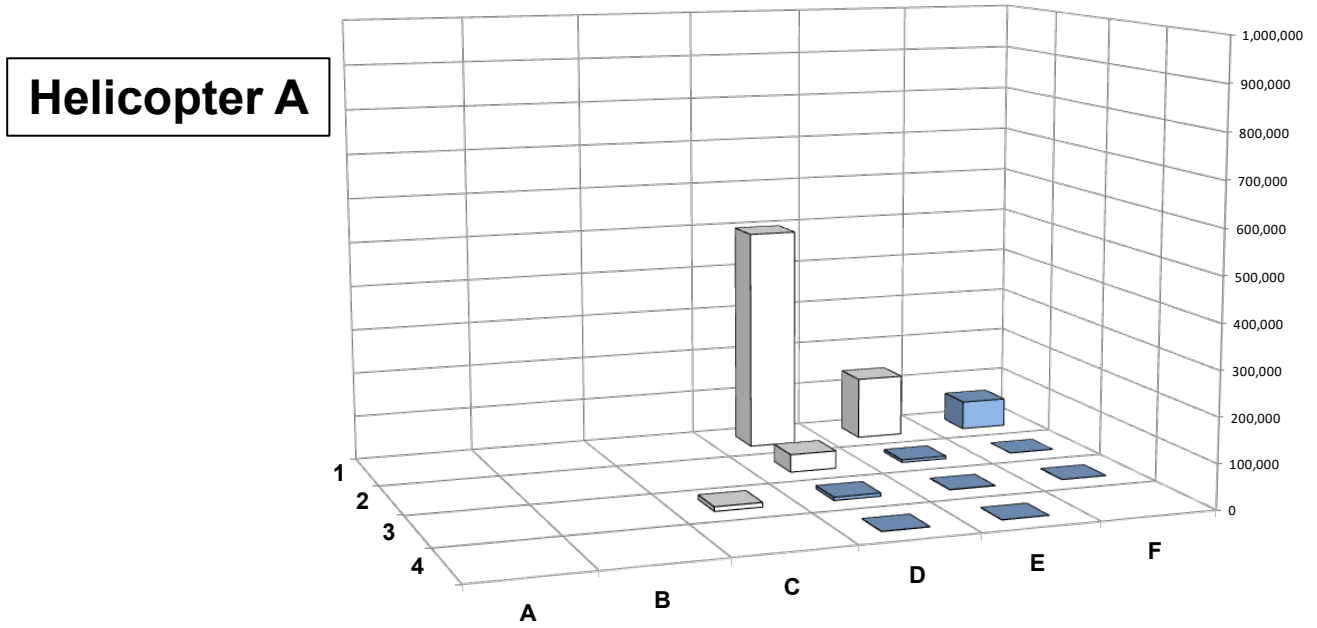
	A	B	C	D	E	F
1				9	12	4
2			1	3	23	
3			2	9	6	1
4		2	5	5	2	

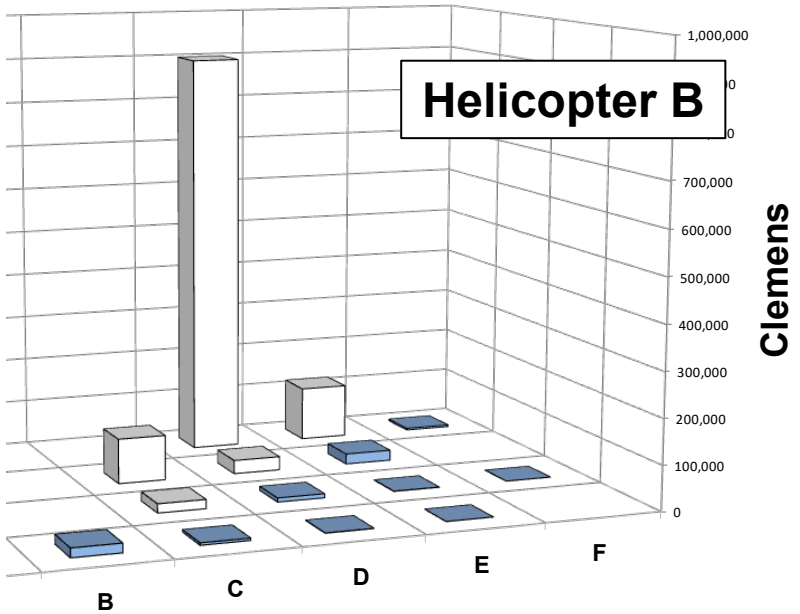
Helicopter C

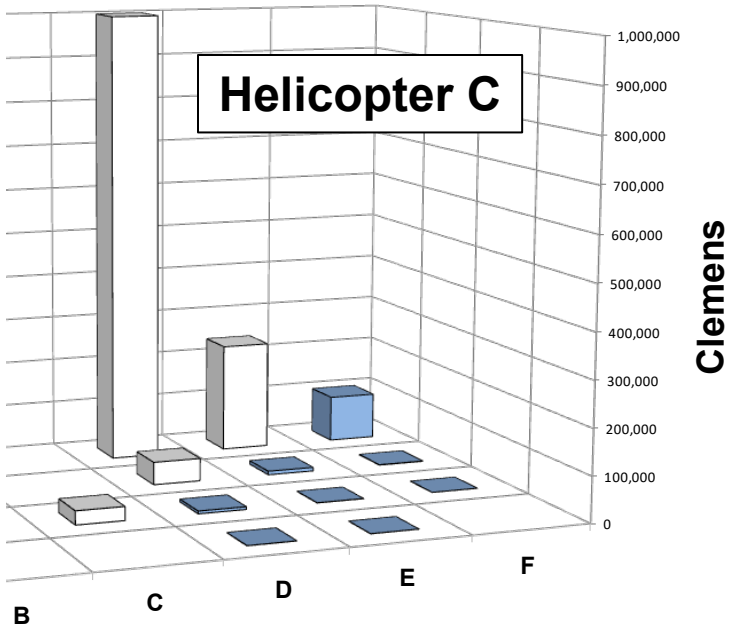


	A	B	C	D	E	F
1				10	24	102
2				5	8	8
3			3	6	3	2
4				1	1	

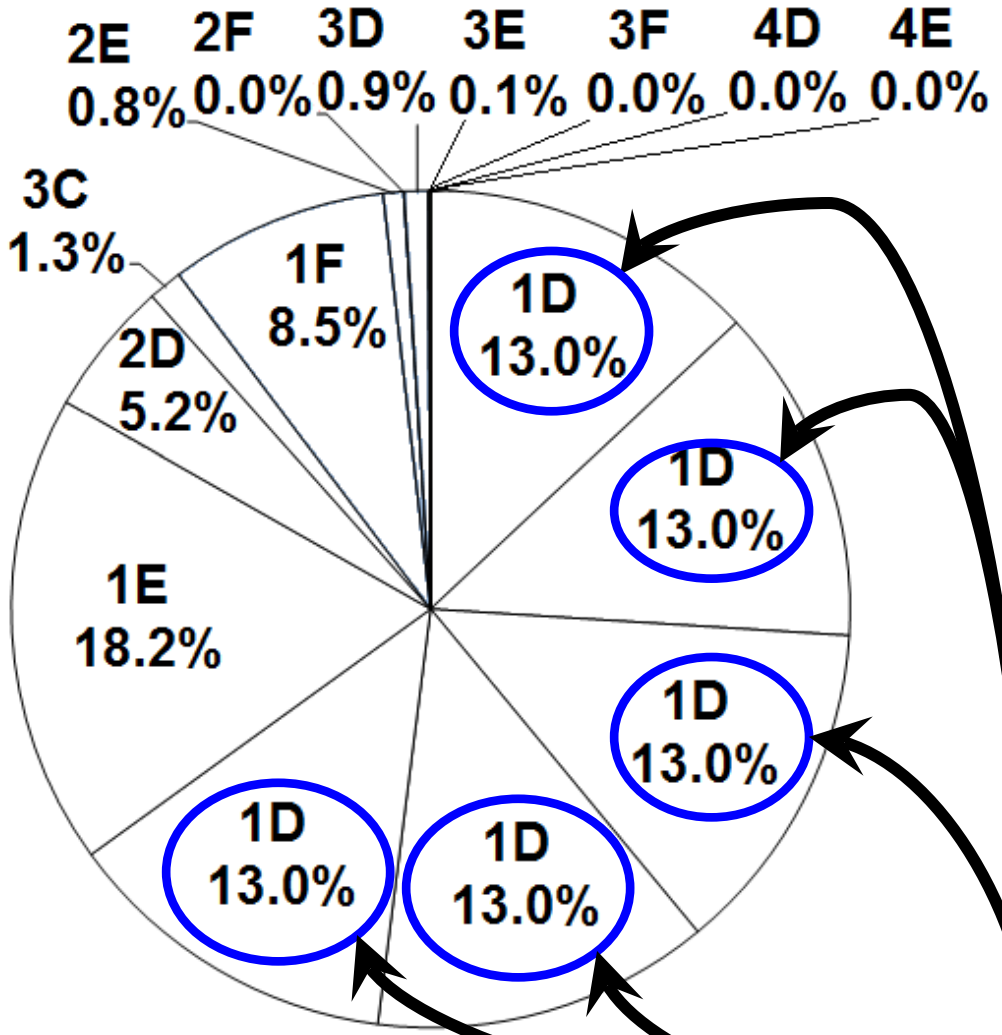
Side by Side Relative Risk by RAC





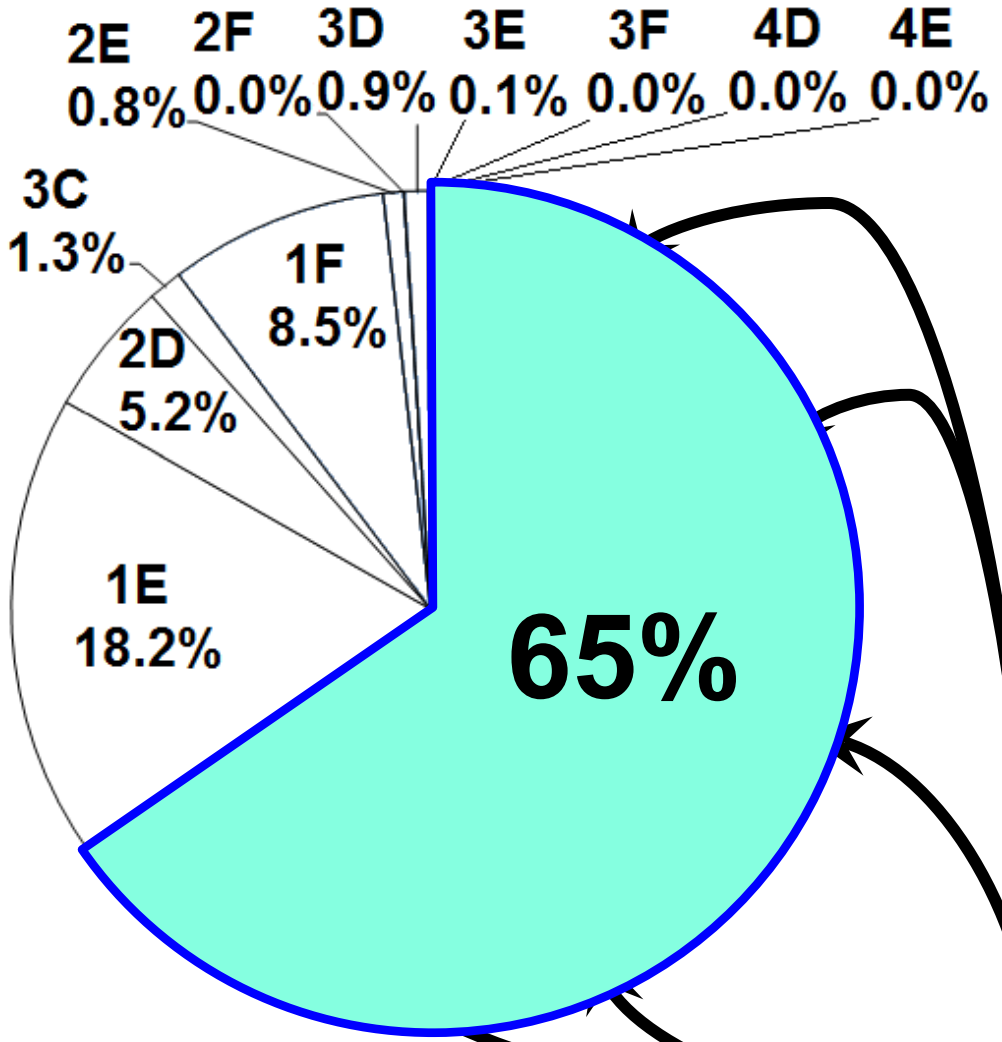


Risk Pie Chart by RAC



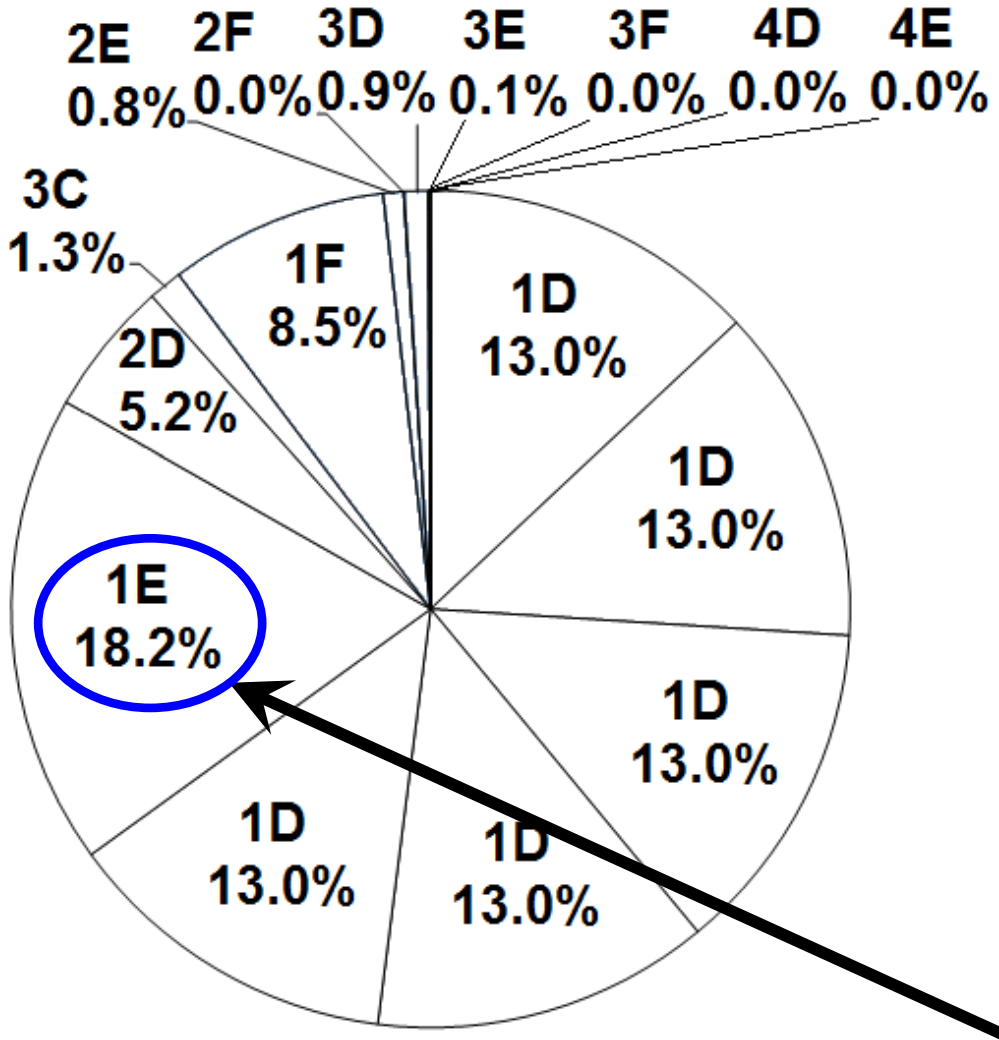
	A	B	C	D	E	F
1				5	14	65
2				4	6	2
3			1	7	5	4
4				2	1	

Risk Pie Chart by RAC



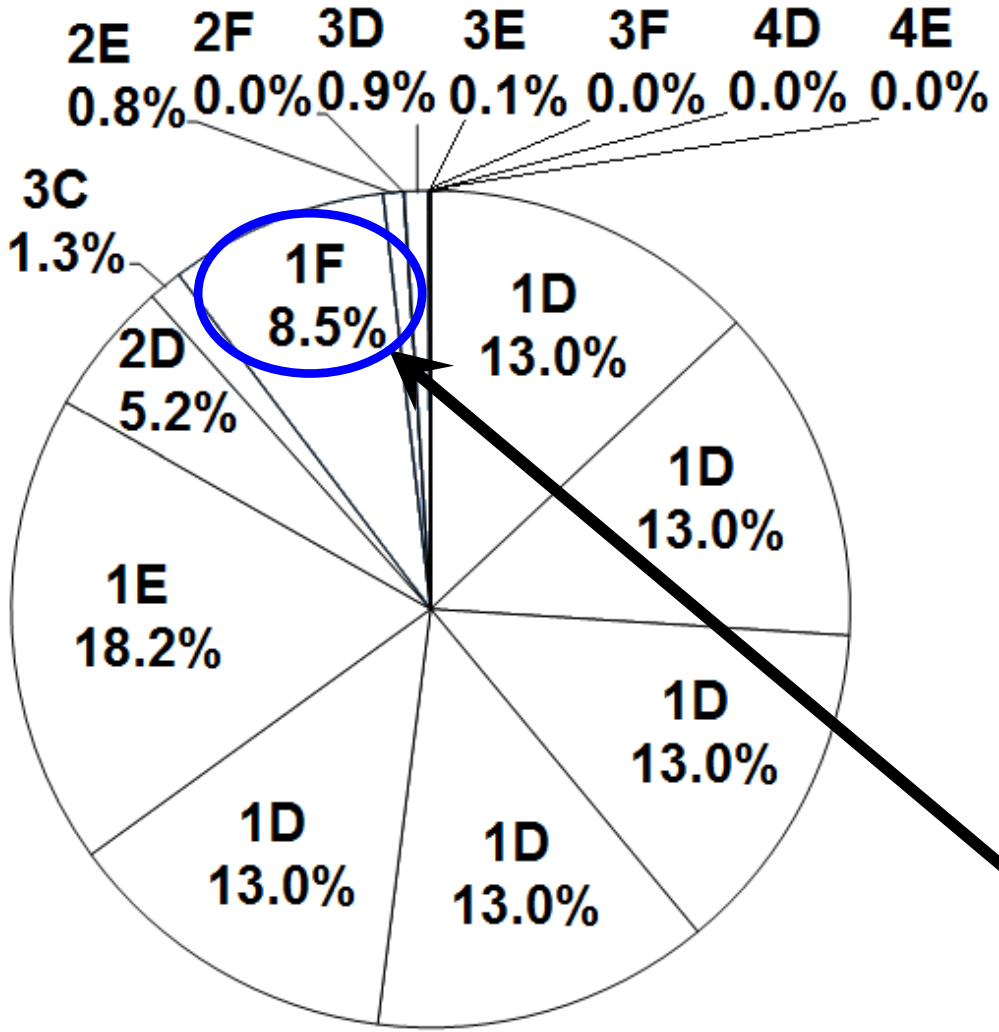
	A	B	C	D	E	F
1				5	14	65
2				4	6	2
3			1	7	5	4
4				2	1	

Risk Pie Chart by RAC



	A	B	C	D	E	F
1				5	14	65
2				4	6	2
3			1	7	5	4
4				2	1	

Risk Pie Chart by RAC



	A	B	C	D	E	F
1				5	14	65
2				4	6	2
3			1	7	5	4
4				2	1	

Topics for this Tutorial

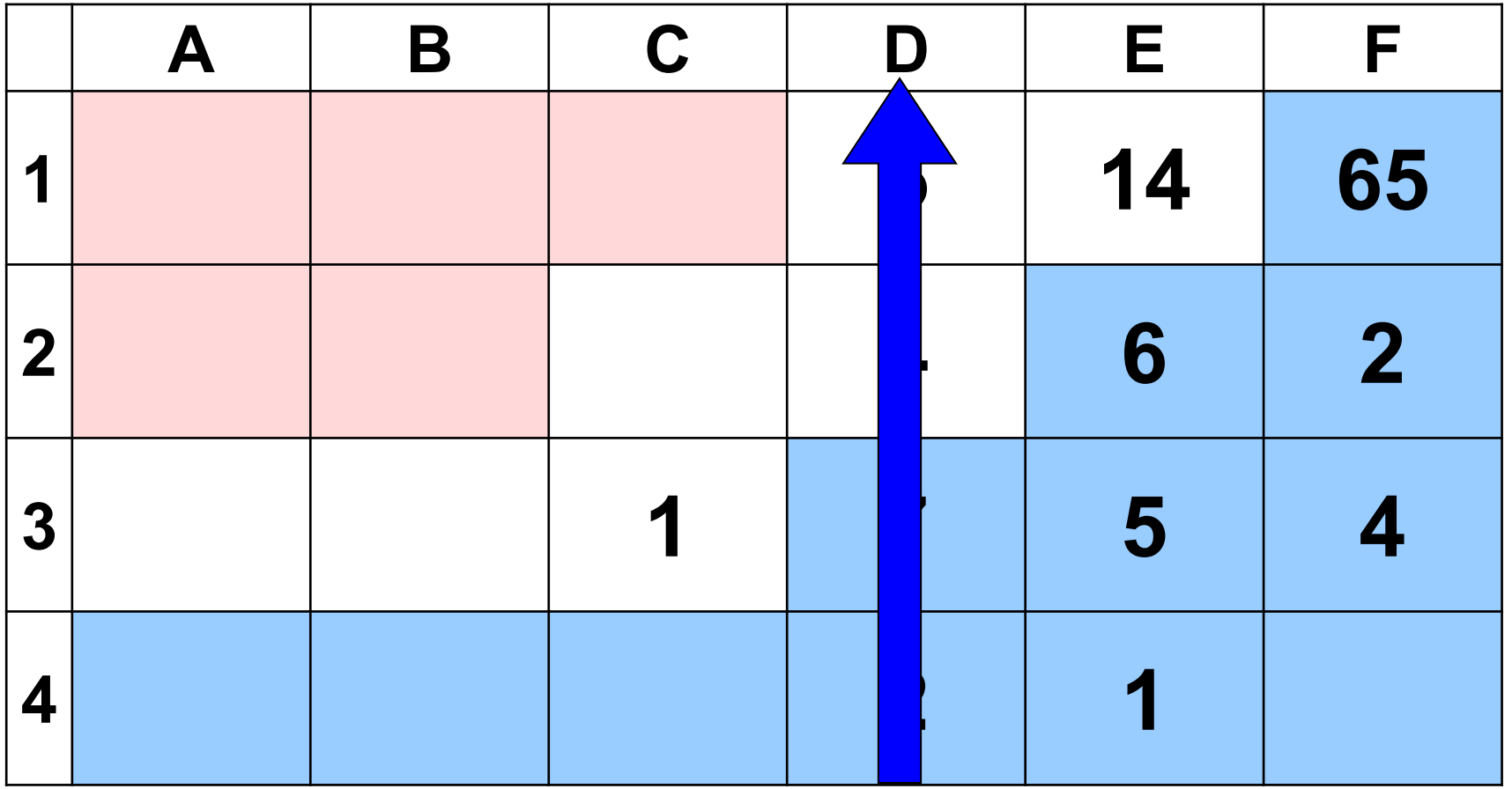
- Purpose of a Hazard Risk Matrix
- Understanding the Attributes of a well-designed risk assessment matrix
- How to Assign a Risk Assessment Code
- Understanding Probability
- Building an Expanded Matrix
- Plotting Accidents on a Matrix
- Using Relative Risk Values
- **Building Hazard Risk Profiles**
- Impact on Software Safety Matrices

Hazard Risk Profile

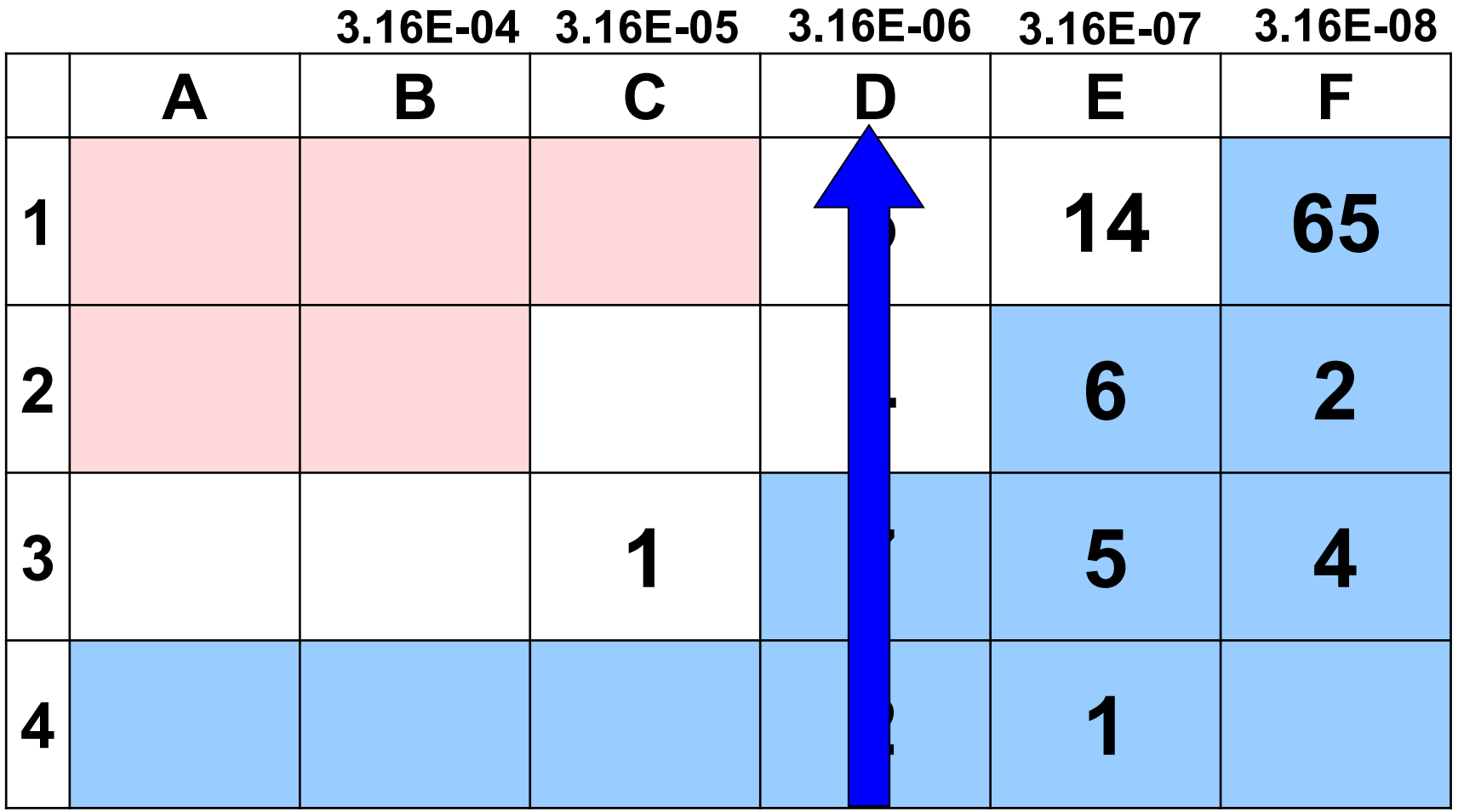
	A	B	C	D	E	F
1				5	14	65
2				4	6	2
3			1	7	5	4
4				2	1	

Hazard Risk Profile

3.16E-06



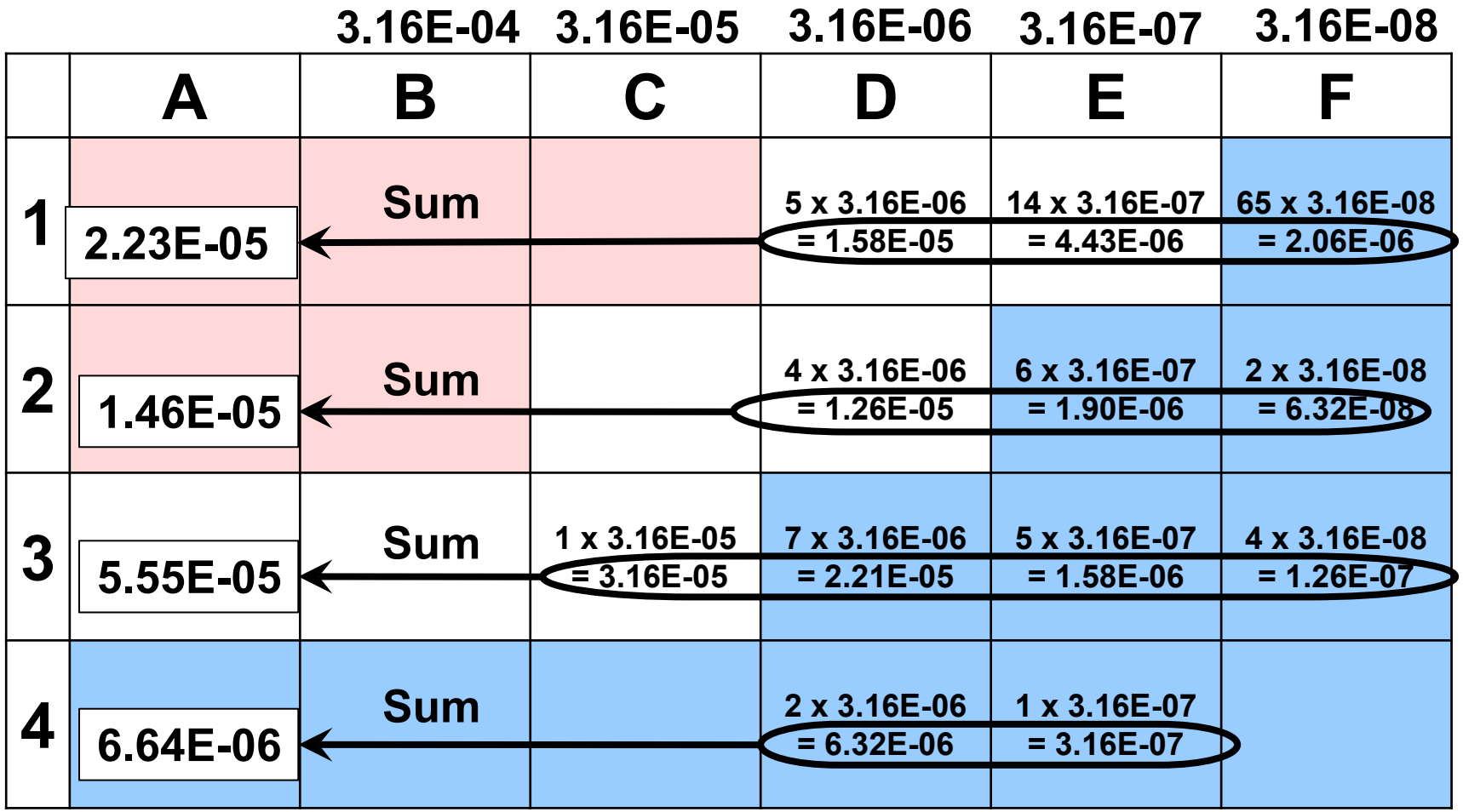
Hazard Risk Profile



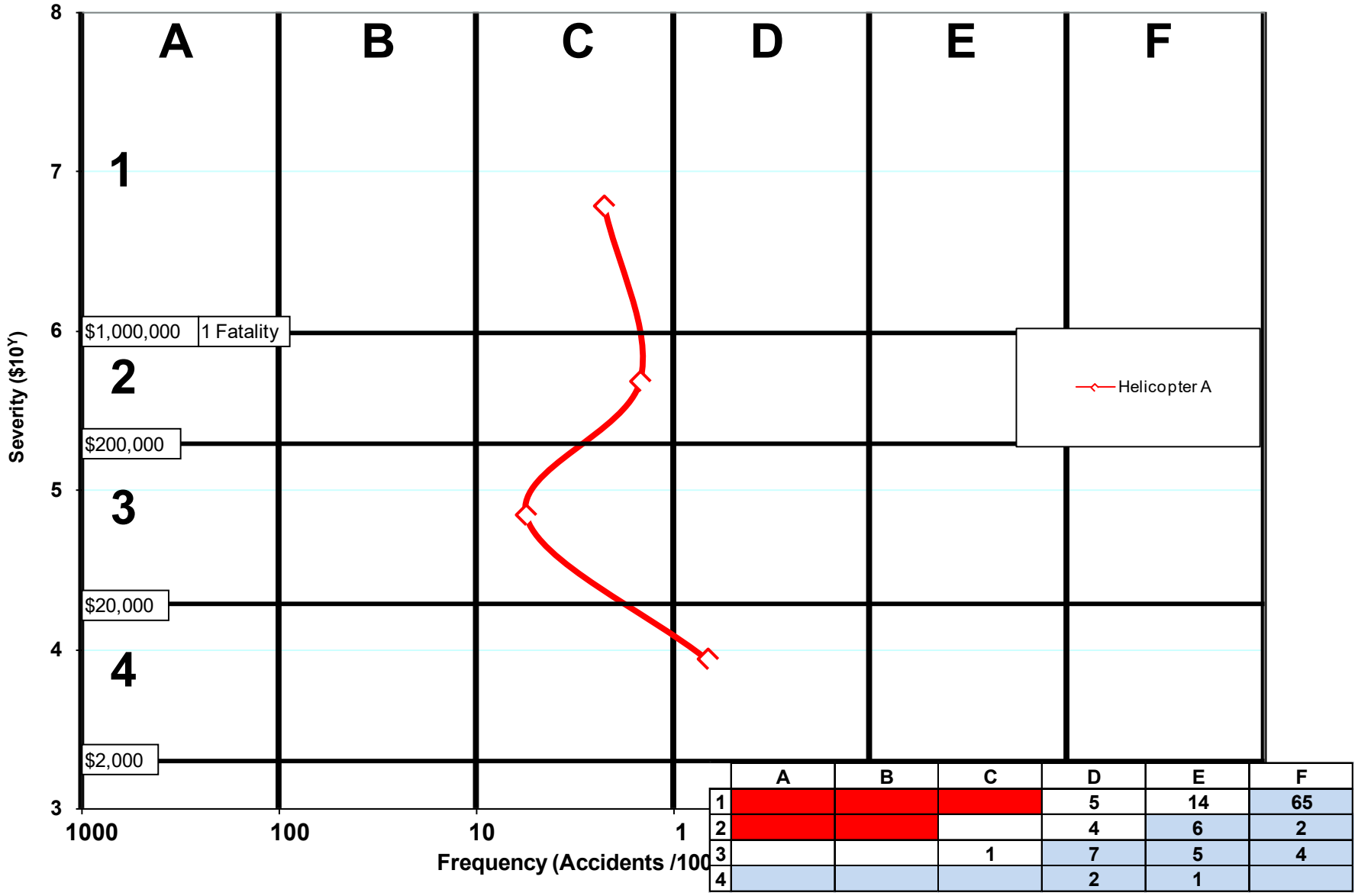
Hazard Risk Profile

		3.16E-04	3.16E-05	3.16E-06	3.16E-07	3.16E-08
	A	B	C	D	E	F
1				5 x 3.16E-06 = 1.58E-05	14 x 3.16E-07 = 4.43E-06	65 x 3.16E-08 = 2.06E-06
2				4 x 3.16E-06 = 1.26E-05	6 x 3.16E-07 = 1.90E-06	2 x 3.16E-08 = 6.32E-08
3			1 x 3.16E-05 = 3.16E-05	7 x 3.16E-06 = 2.21E-05	5 x 3.16E-07 = 1.58E-06	4 x 3.16E-08 = 1.26E-07
4				2 x 3.16E-06 = 6.32E-06	1 x 3.16E-07 = 3.16E-07	

Hazard Risk Profile

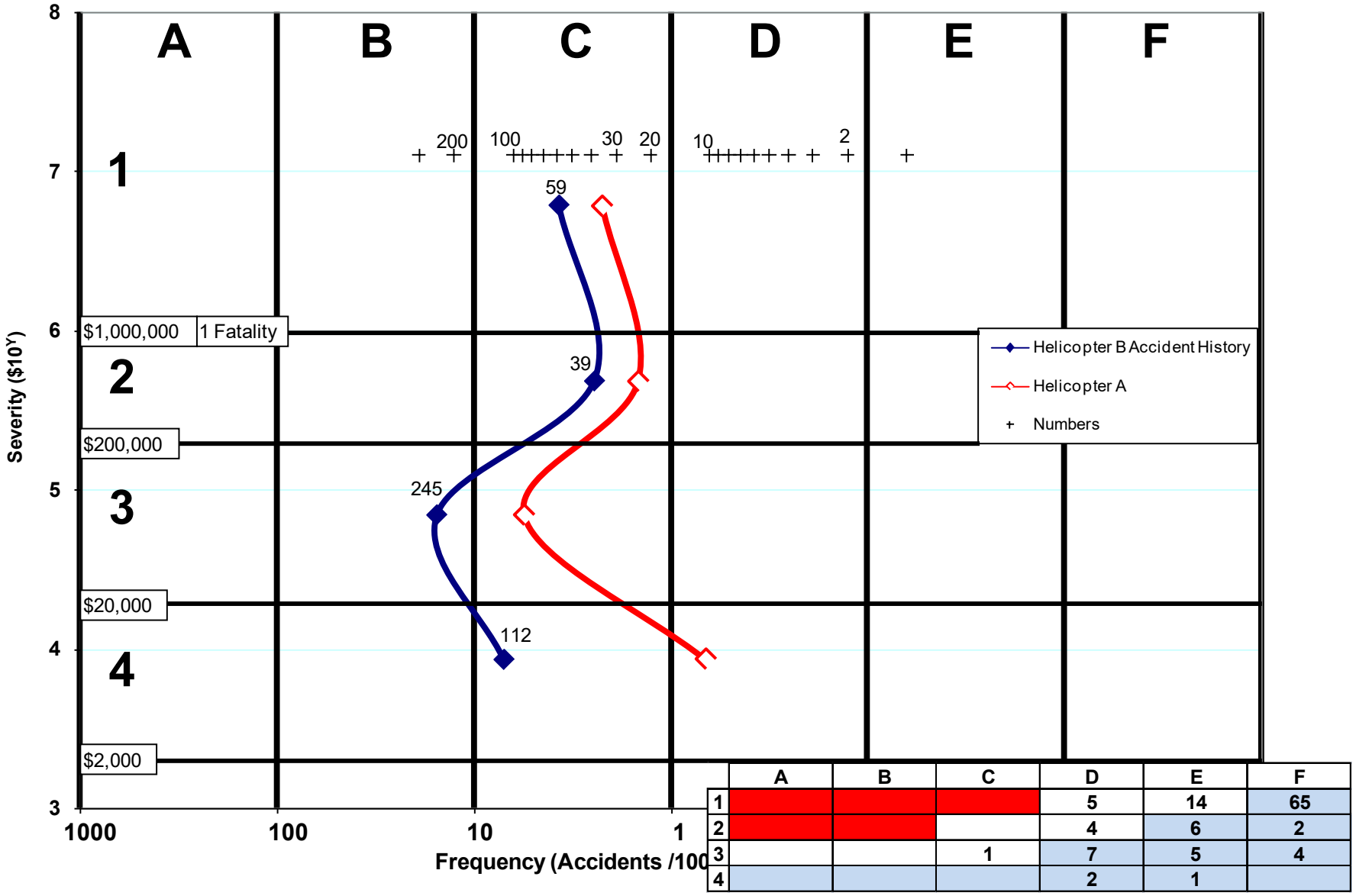


Hazard Risk Profile



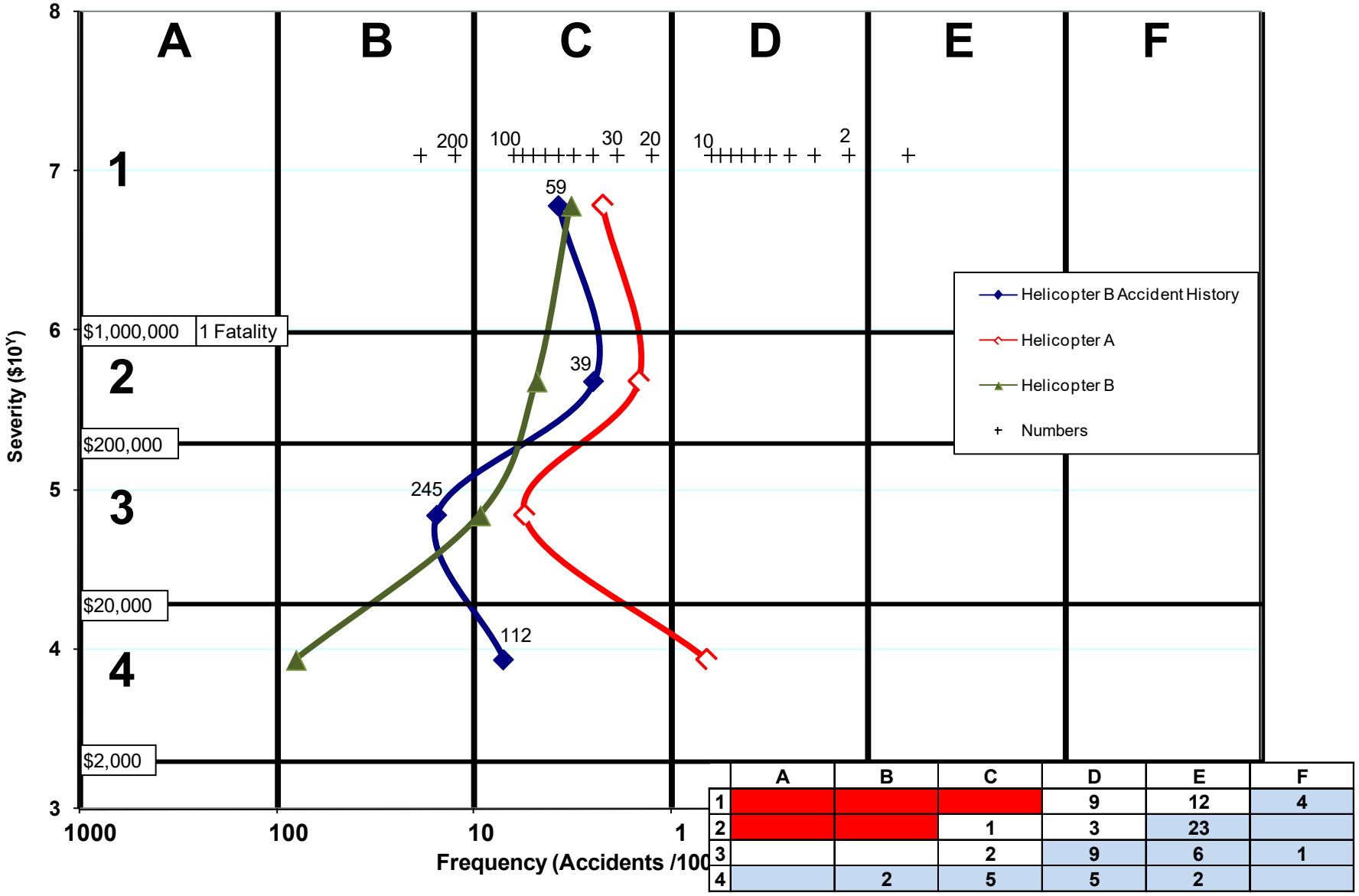
	A	B	C	D	E	F
1				5	14	65
2				4	6	2
3			1	7	5	4
4				2	1	

Comparing Hazard Profile to Accident History



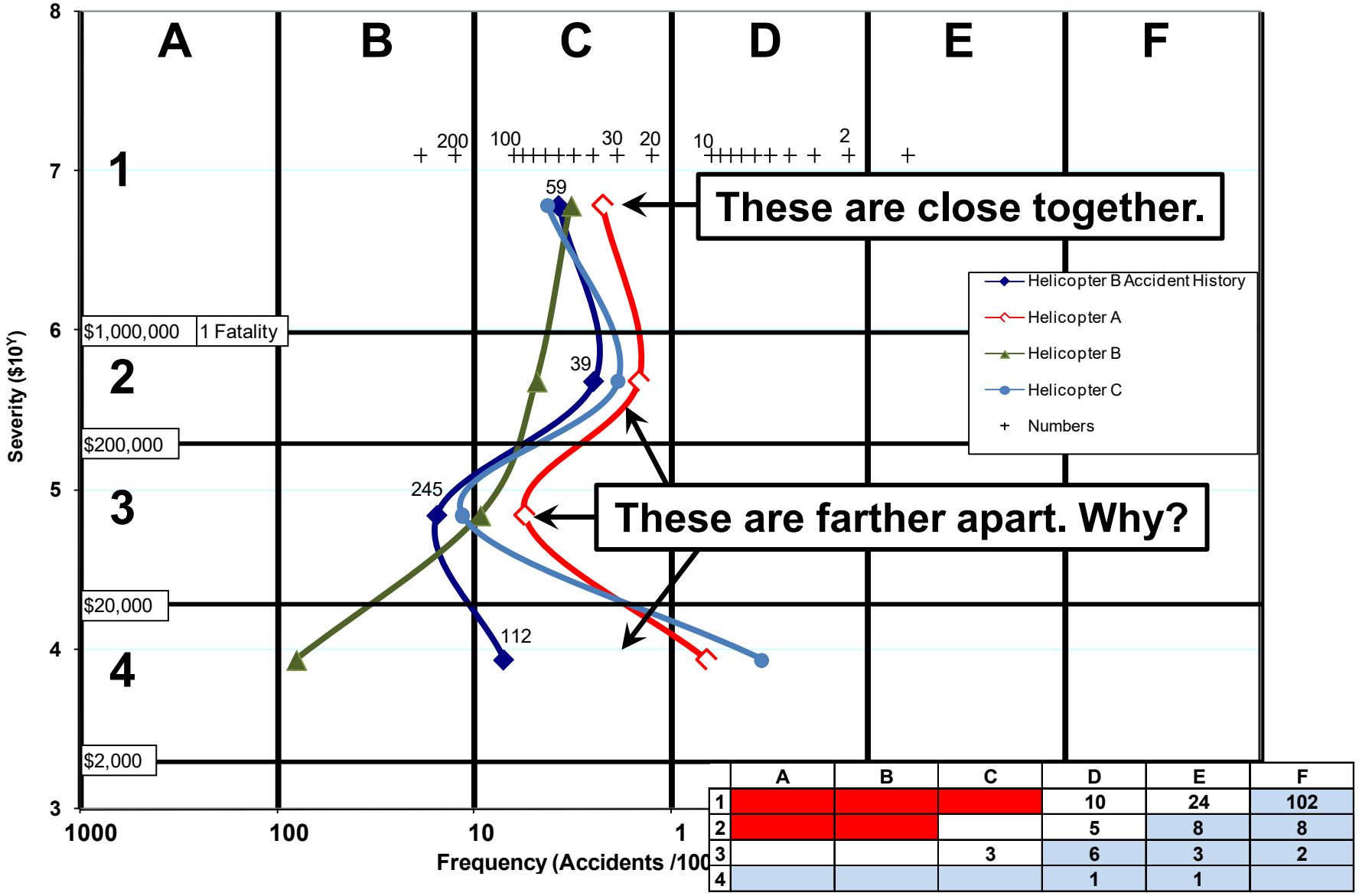
	A	B	C	D	E	F
1				5	14	65
2				4	6	2
3			1	7	5	4
4				2	1	

Comparing Hazard Profile to Accident History



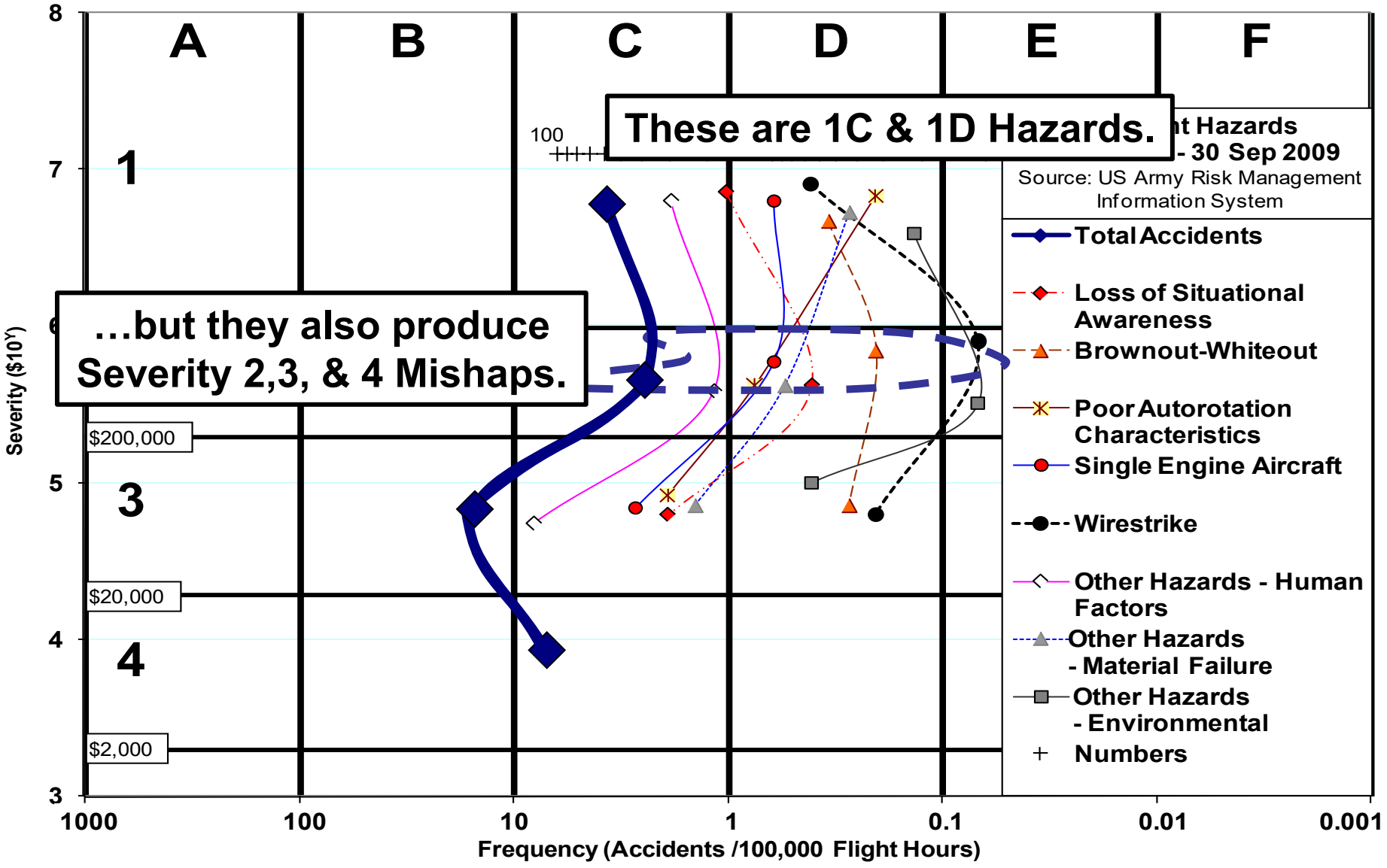
	A	B	C	D	E	F
1				9	12	4
2			1	3	23	
3			2	9	6	1
4		2	5	5	2	

Comparing Hazard Profile to Accident History



	A	B	C	D	E	F
1				10	24	102
2				5	8	8
3			3	6	3	2
4				1	1	

US Army Aviation Mishaps



Missile Hazard Risk Matrix

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY *	Catastrophic (1) 1 Fatal $10M	Critical (2) $1M	Marginal (3) $100K	Negligible (4)
Frequent (A) 10^{-1}	High	High	Serious	Medium
Probable (B) 10^{-2}	High	High	Serious	Medium
Occasional (C) 10^{-3}	High	Serious	Medium	Low
Remote (D) 10^{-6}	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Missile Hazard Risk Matrix

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY *	Catastrophic (1) — 1 Fatal / $10M	Critical (2) — $1M	Marginal (3) — $100K	Negligible (4)
Frequent (A) — 1/10	High	High	Serious	Medium
Probable (B) — 1/100	High	High	Serious	Medium
Occasional (C) — 1/1,000	High	Serious	Medium	Low
Remote (D) — 1/1,000,000	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Back of the Envelope Calculation

40,000 Shishkebab Missiles

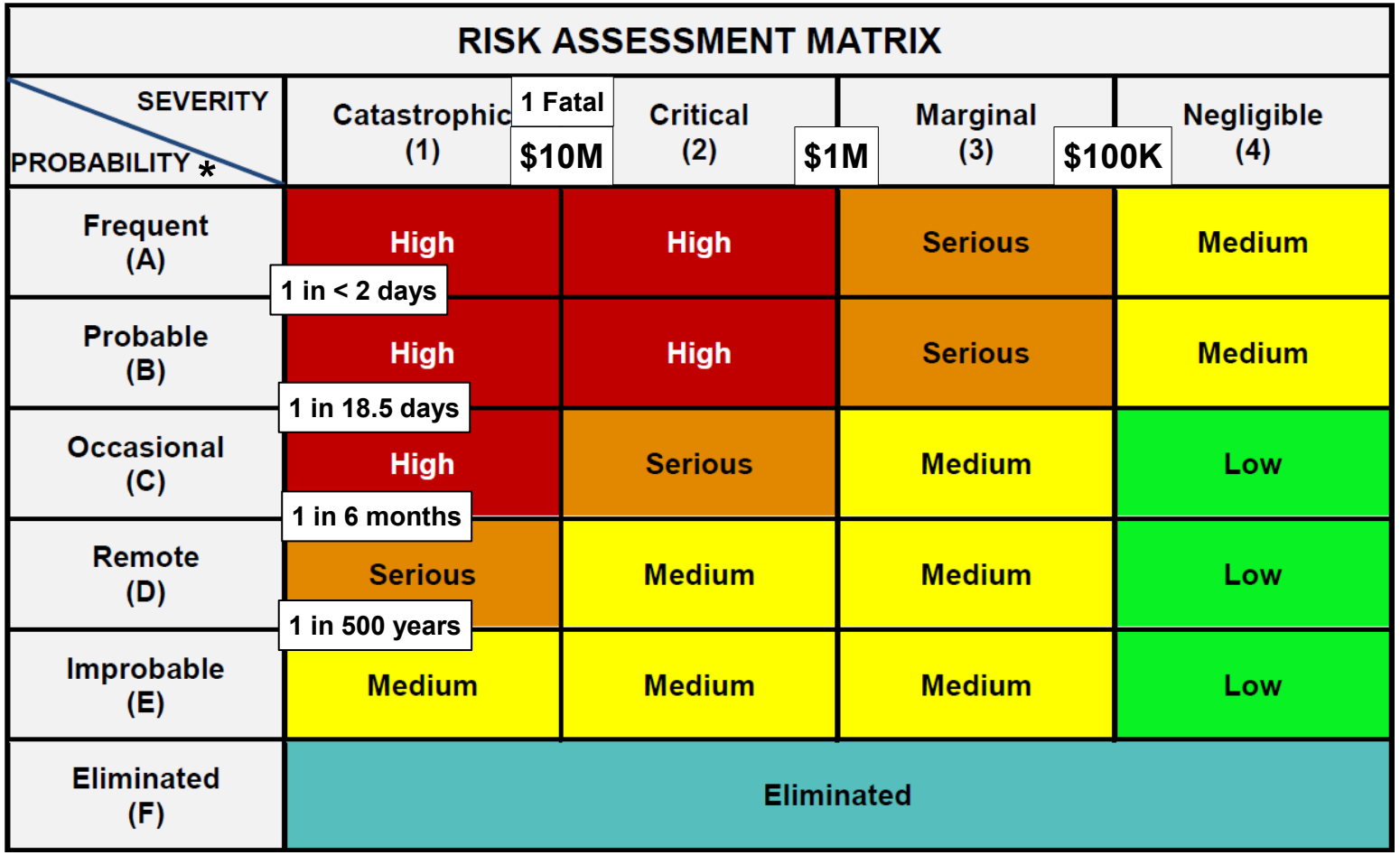
Delivered over 20 years

Assume all fired

1 accident in 1,000,000 firings

$$\frac{\text{1 accident}}{\text{1,000,000 ~~firings~~}} \times \frac{\text{40,000 ~~firings~~}}{\text{20 years}} = \frac{\text{1 accident}}{\text{500 years}}$$

Missile Hazard Risk Matrix



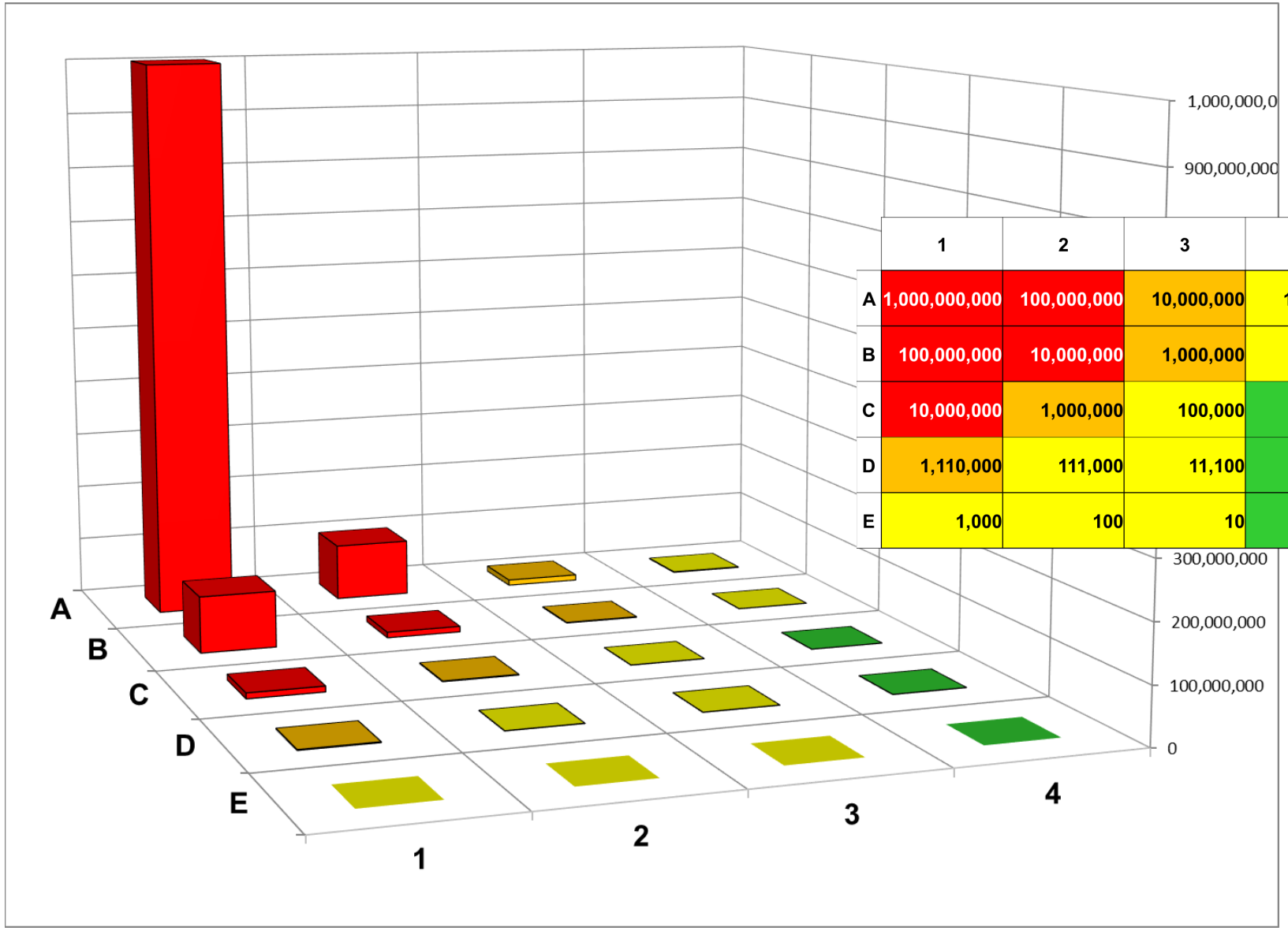
Matrix Relative Risk Values

	1	2	3	4
A	1,000,000,000	100,000,000	10,000,000	1,000,000
	10^{-1}			
B	100,000,000	10,000,000	1,000,000	100,000
	10^{-2}			
C	10,000,000	1,000,000	100,000	10,000
	10^{-3}			
D	1,000,000	100,000	10,000	1,000
	10^{-4}			
	100,000	10,000	1,000	100
	10^{-5}			
	10,000	1,000	100	10
	10^{-6}			
E	1,000	100	10	1

Matrix Relative Risk Values

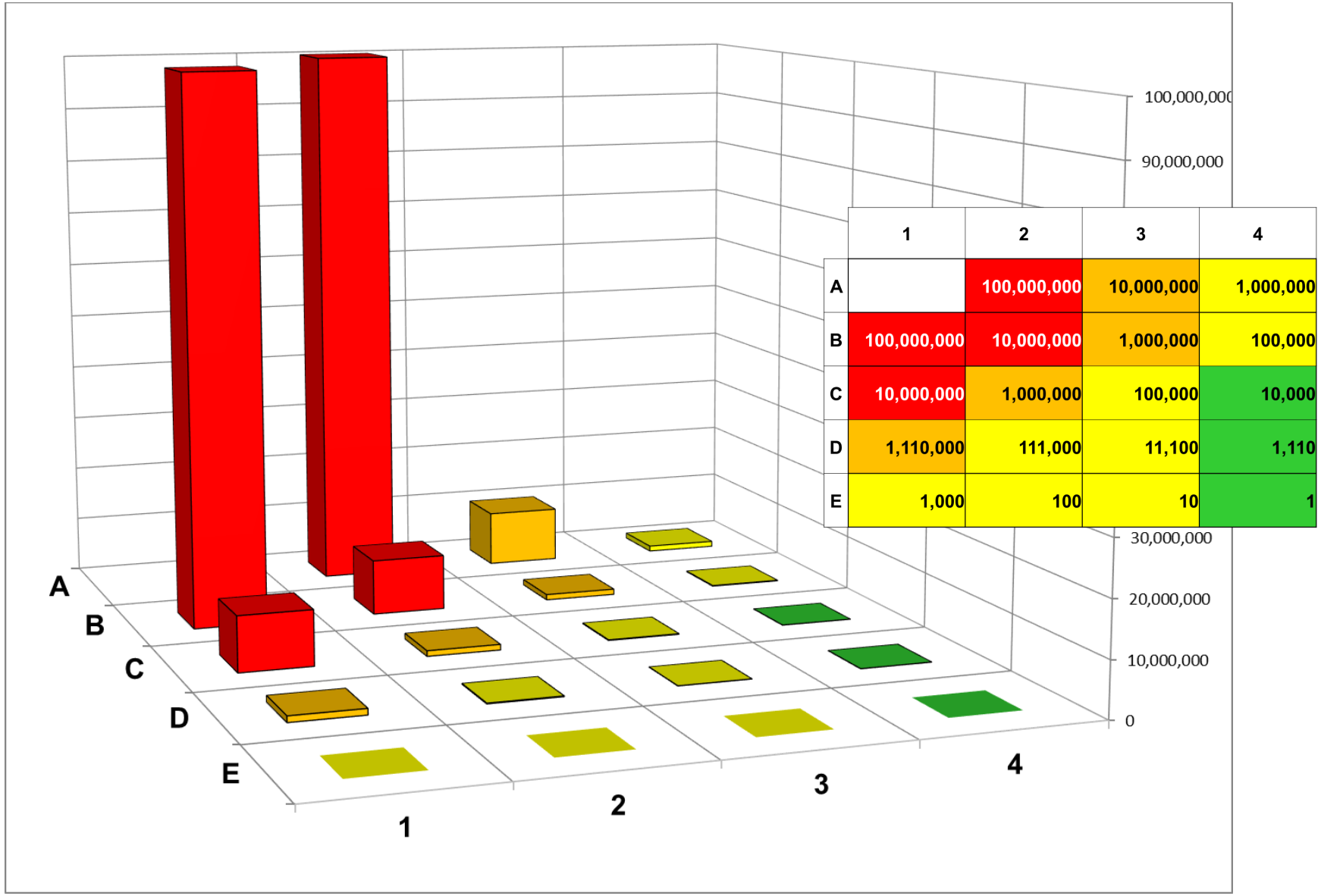
	1	2	3	4
A	1,000,000,000	100,000,000	10,000,000	1,000,000
	10^{-1}			
B	100,000,000	10,000,000	1,000,000	100,000
	10^{-2}			
C	10,000,000	1,000,000	100,000	10,000
	10^{-3}			
D	1,110,000	111,000	11,100	1,110
	10^{-6}			
E	1,000	100	10	1

Matrix Relative Risk Values



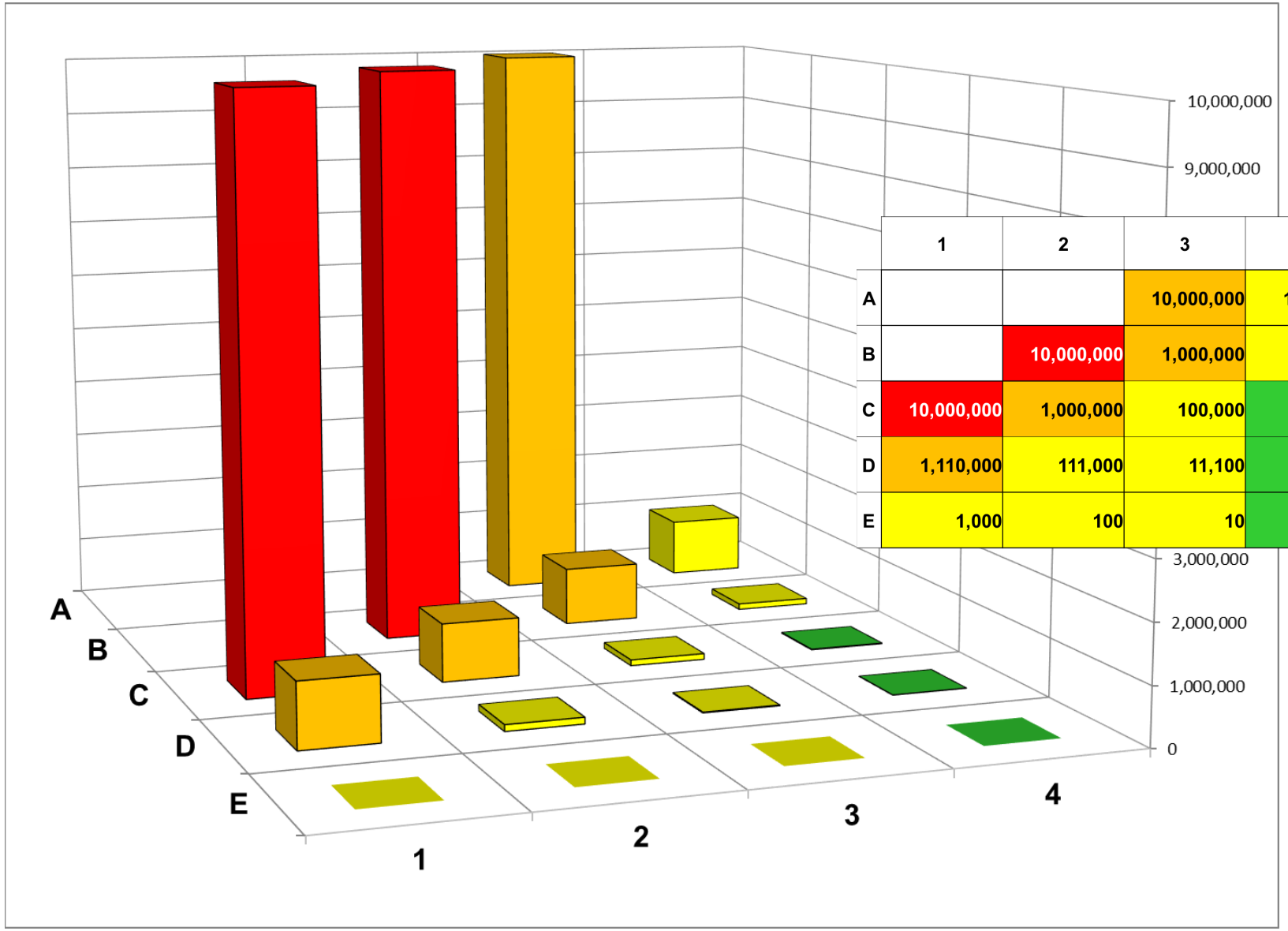
	1	2	3	4
A	1,000,000,000	100,000,000	10,000,000	1,000,000
B	100,000,000	10,000,000	1,000,000	100,000
C	10,000,000	1,000,000	100,000	10,000
D	1,110,000	111,000	11,100	1,110
E	1,000	100	10	1

Matrix Relative Risk Values



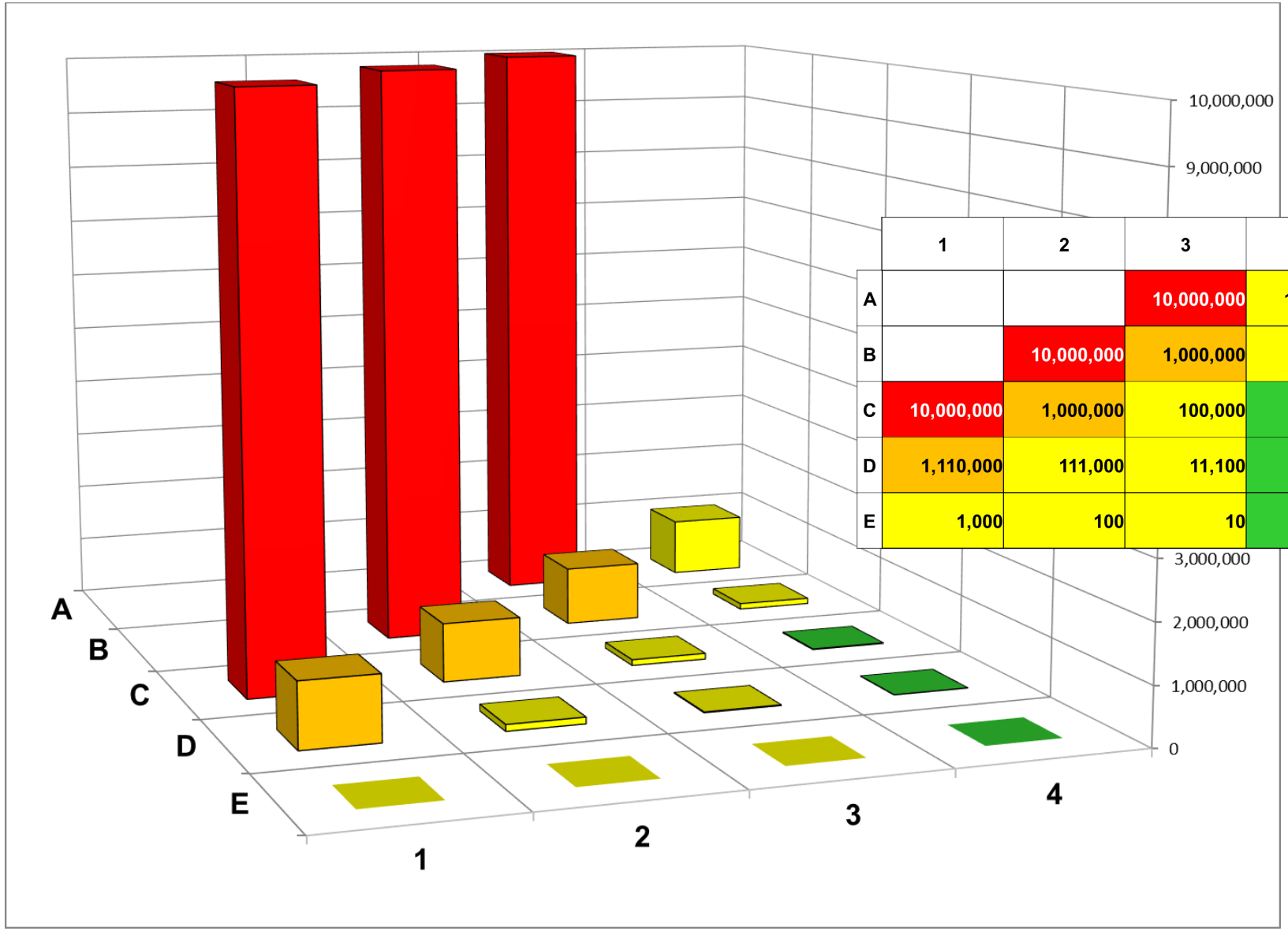
	1	2	3	4
A		100,000,000	10,000,000	1,000,000
B	100,000,000	10,000,000	1,000,000	100,000
C	10,000,000	1,000,000	100,000	10,000
D	1,110,000	111,000	11,100	1,110
E	1,000	100	10	1

Matrix Relative Risk Values



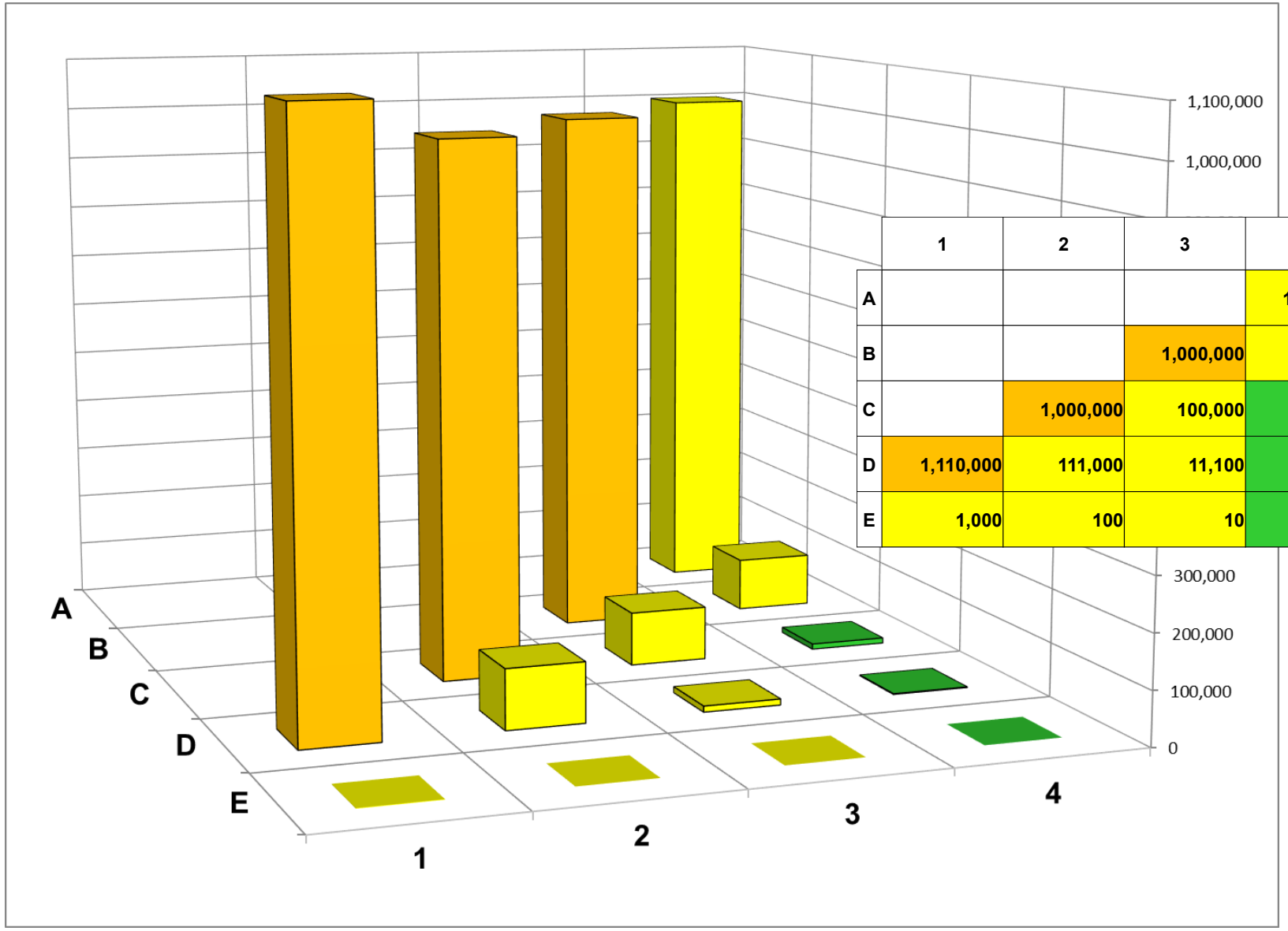
	1	2	3	4
A			10,000,000	1,000,000
B		10,000,000	1,000,000	100,000
C	10,000,000	1,000,000	100,000	10,000
D	1,110,000	111,000	11,100	1,110
E	1,000	100	10	1

Matrix Relative Risk Values



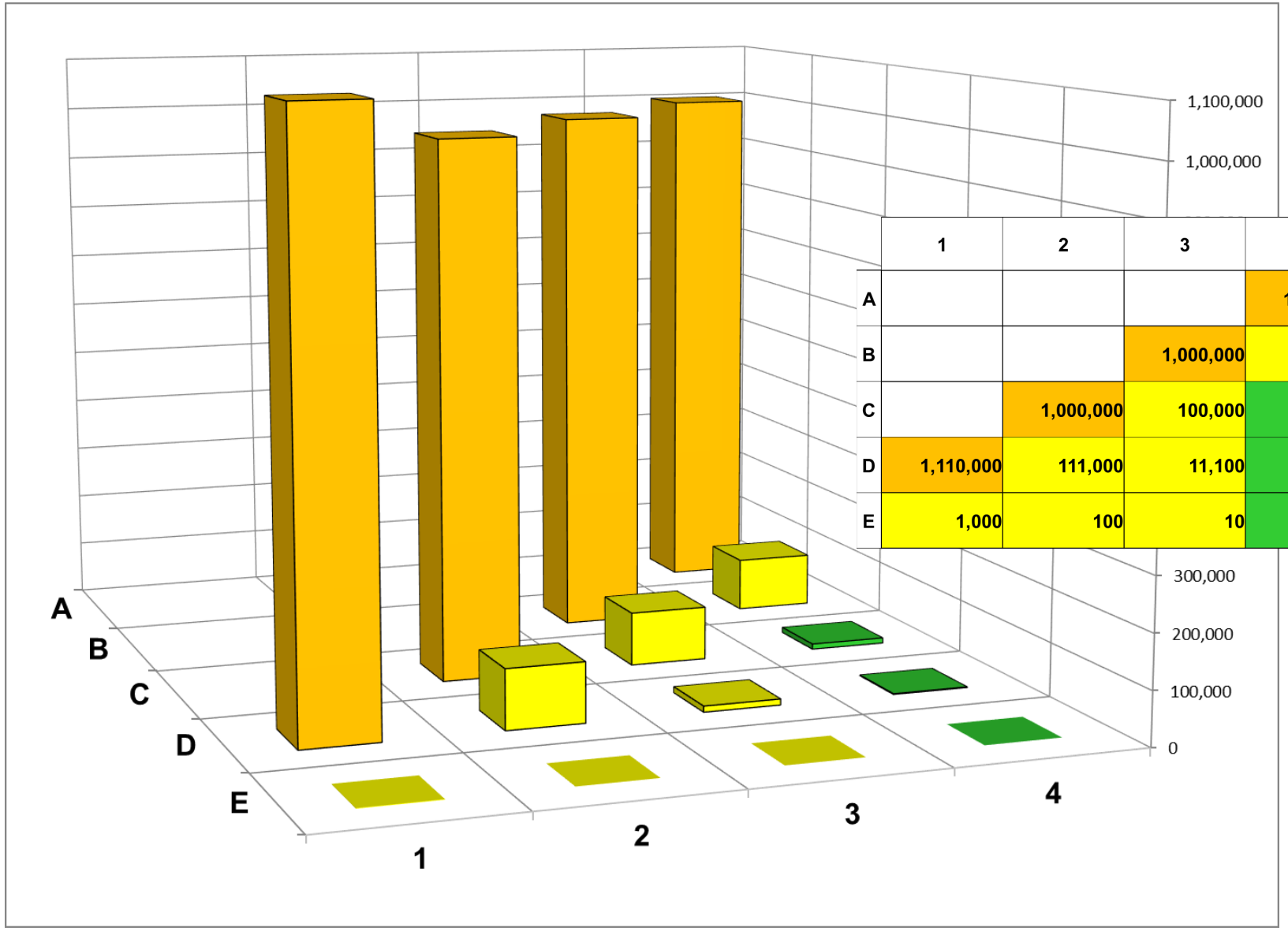
	1	2	3	4
A			10,000,000	1,000,000
B		10,000,000	1,000,000	100,000
C	10,000,000	1,000,000	100,000	10,000
D	1,110,000	111,000	11,100	1,110
E	1,000	100	10	1

Matrix Relative Risk Values



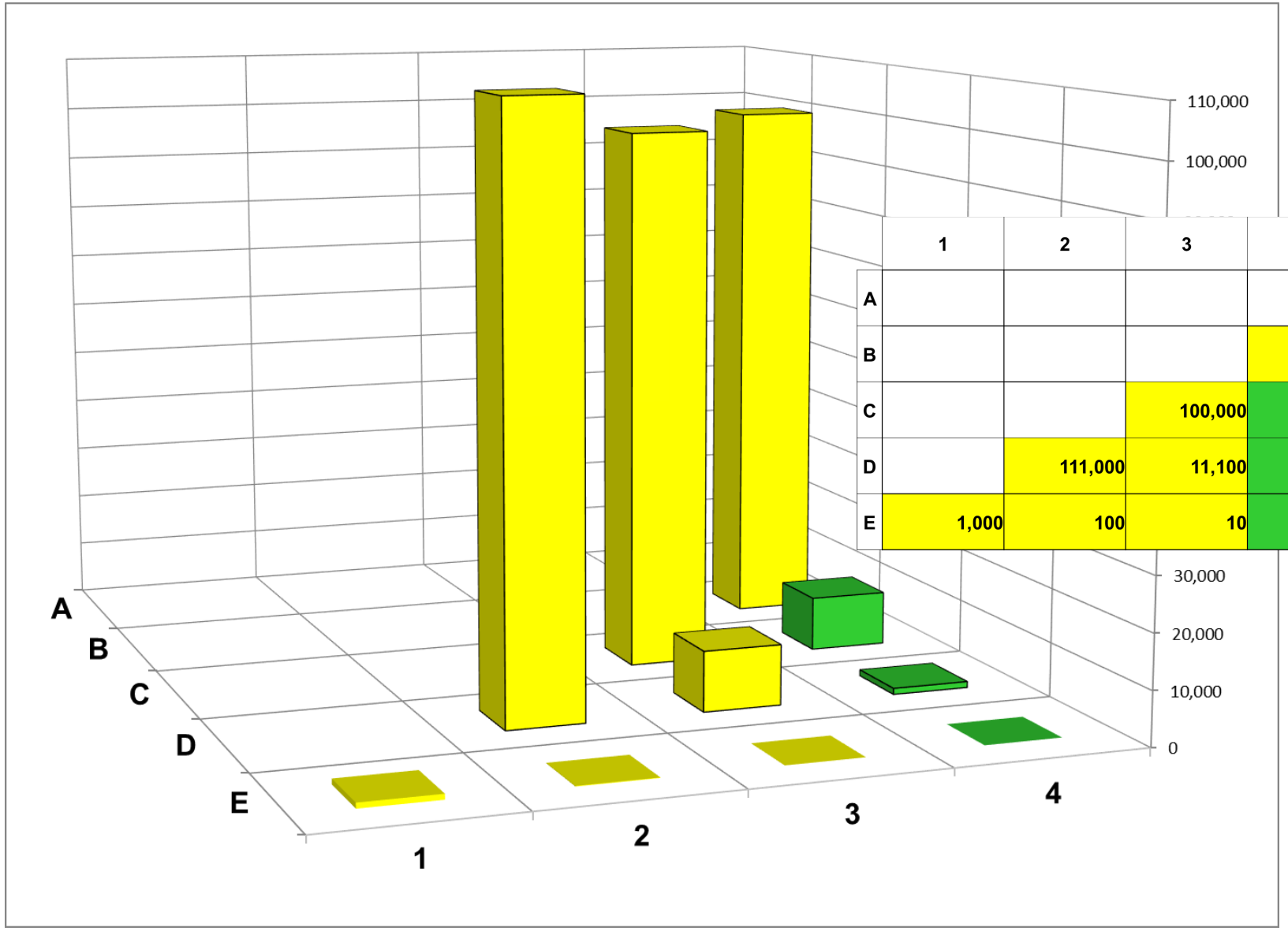
	1	2	3	4
A				1,000,000
B			1,000,000	100,000
C		1,000,000	100,000	10,000
D	1,110,000	111,000	11,100	1,110
E	1,000	100	10	1

Matrix Relative Risk Values



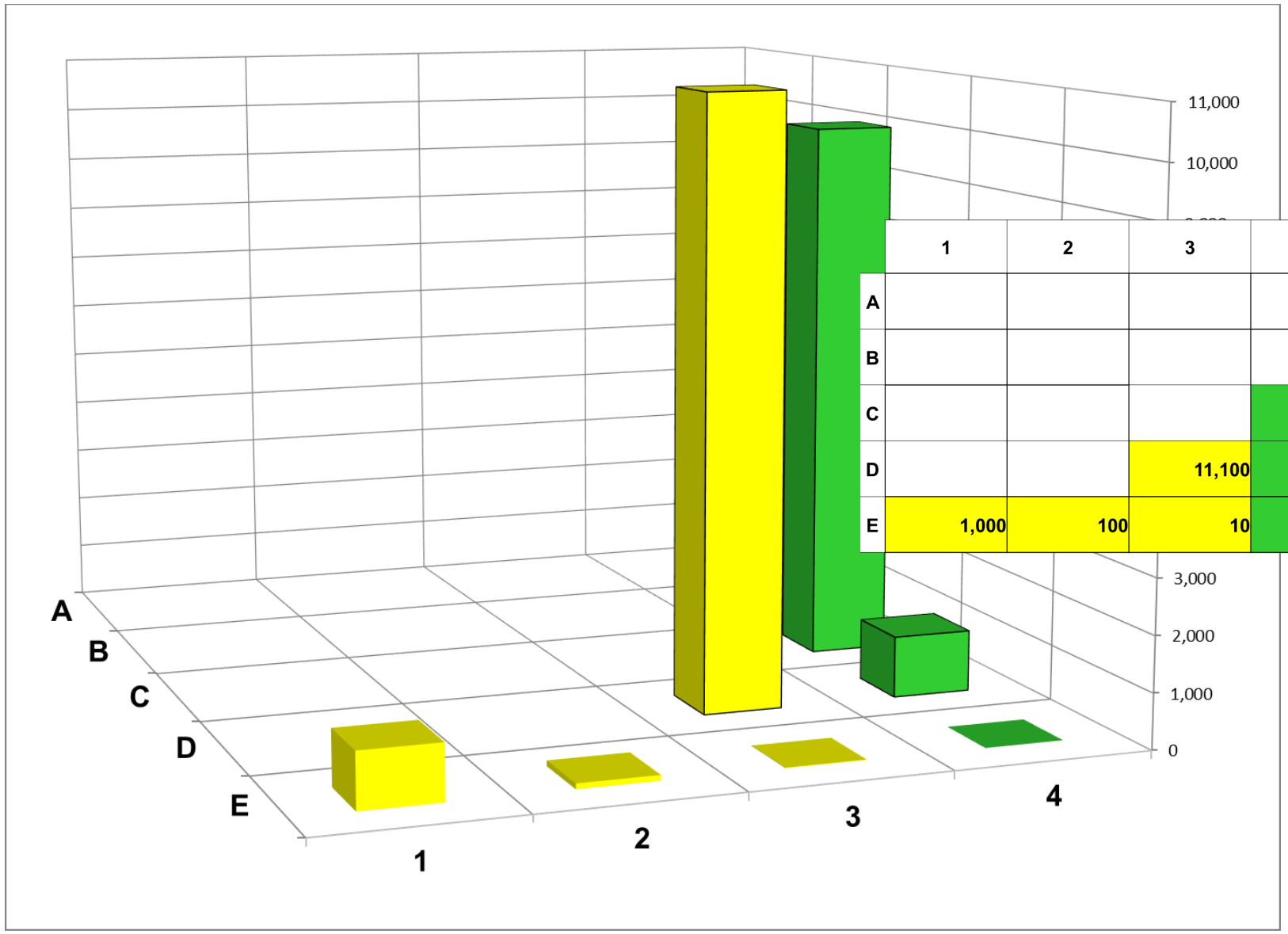
	1	2	3	4
A				1,000,000
B			1,000,000	100,000
C		1,000,000	100,000	10,000
D	1,110,000	111,000	11,100	1,110
E	1,000	100	10	1

Matrix Relative Risk Values



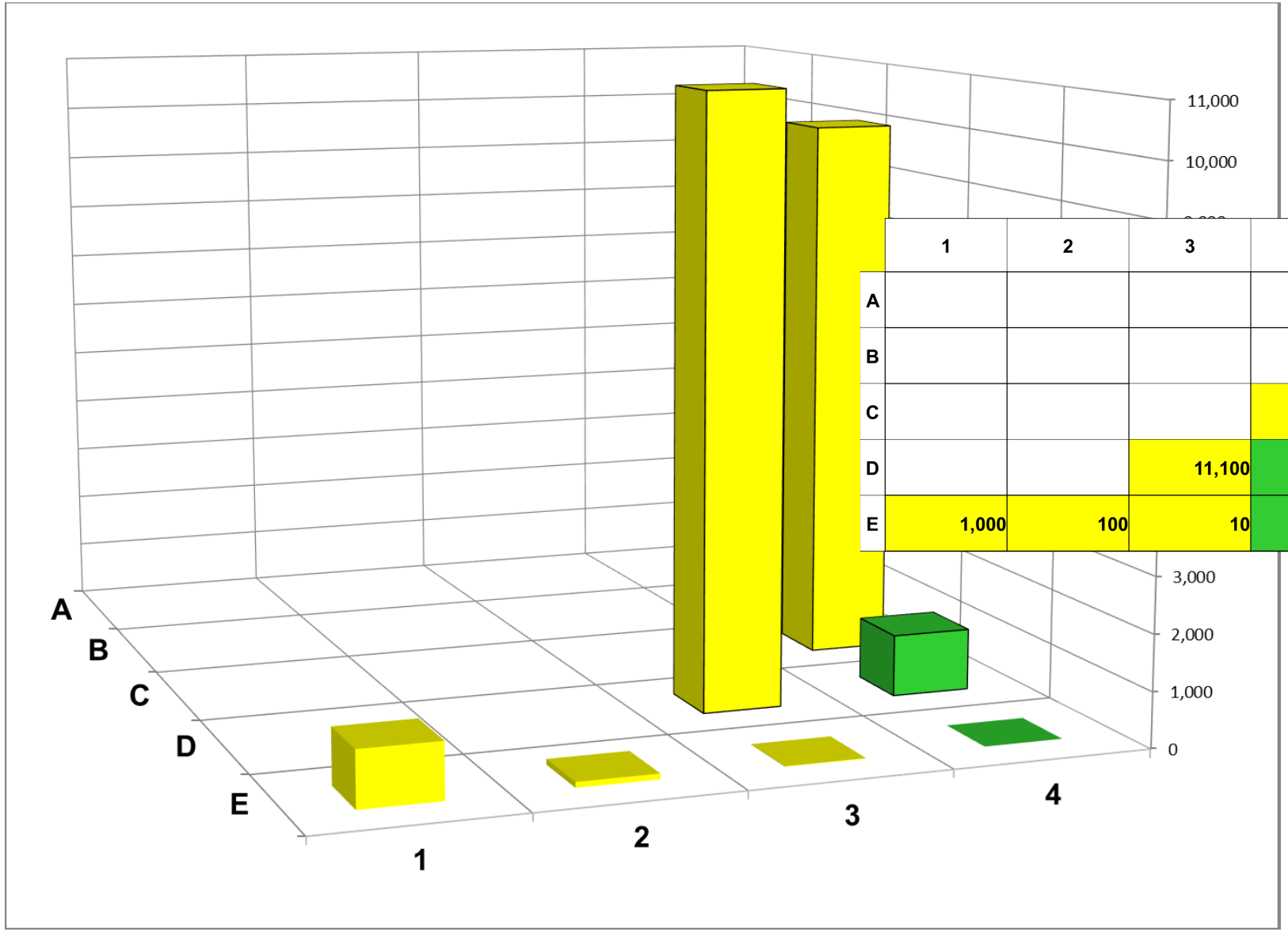
	1	2	3	4
A				
B				100,000
C			100,000	10,000
D		111,000	11,100	1,110
E	1,000	100	10	1

Matrix Relative Risk Values



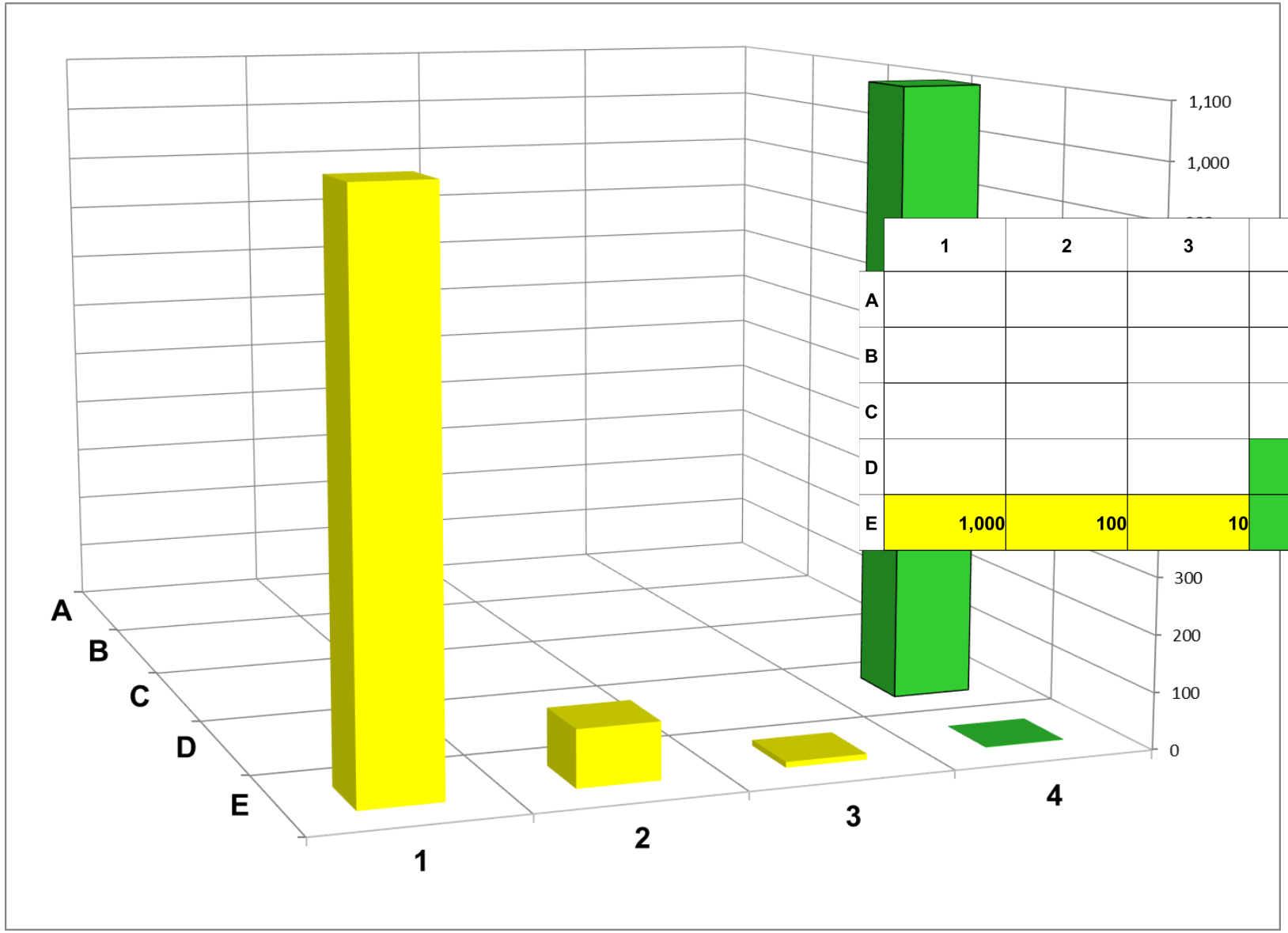
	1	2	3	4
A				
B				
C				10,000
D			11,100	1,110
E	1,000	100	10	1

Matrix Relative Risk Values



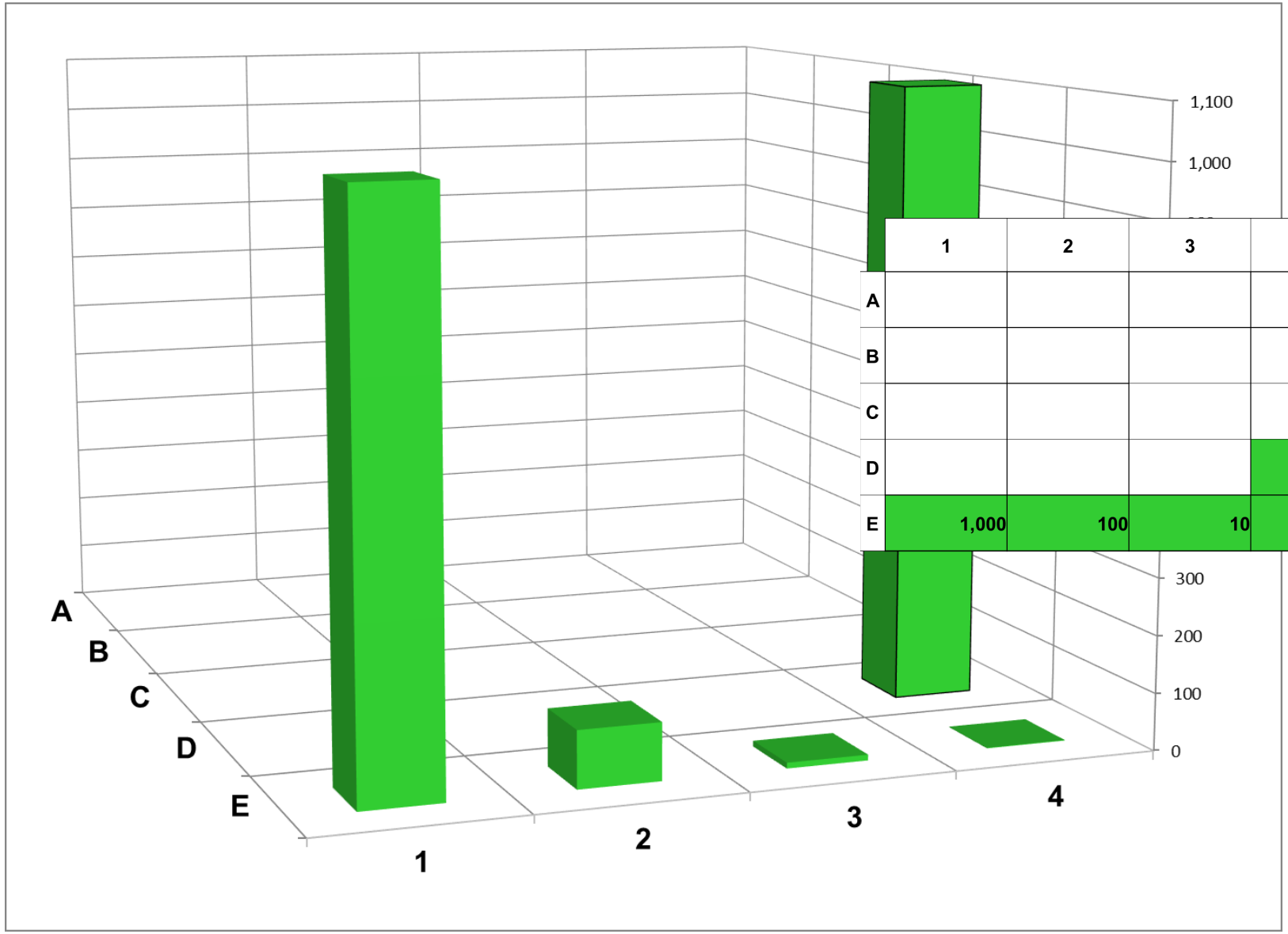
	1	2	3	4
A				
B				
C				10,000
D			11,100	1,110
E	1,000	100	10	1

Matrix Relative Risk Values



	1	2	3	4
A				
B				
C				
D				1,110
E	1,000	100	10	1

Matrix Relative Risk Values

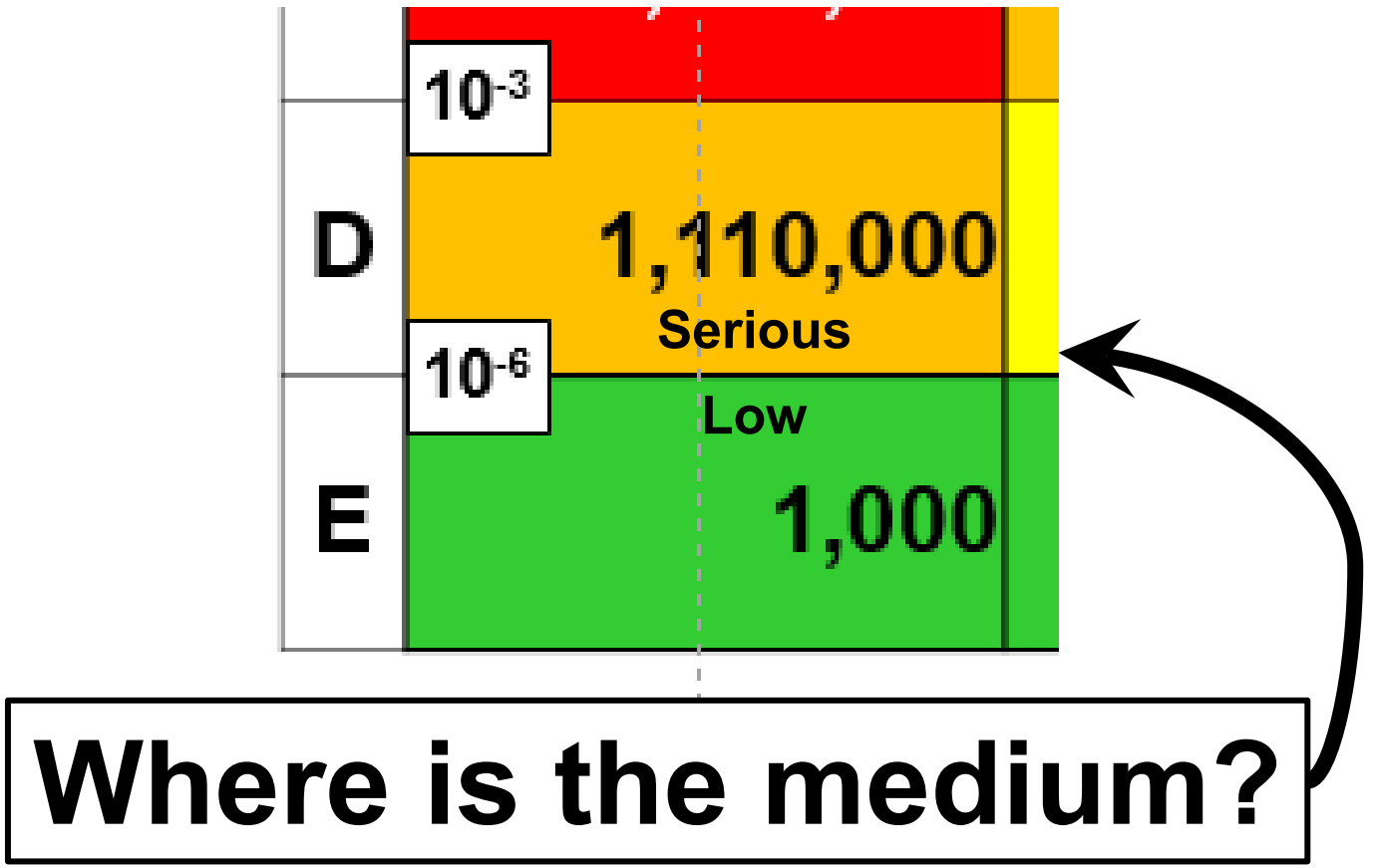


	1	2	3	4
A				
B				
C				
D				1,110
E	1,000	100	10	1

Matrix Relative Risk Values

	1	2	3	4
A	1,000,000,000	100,000,000	10,000,000	1,000,000
	10^{-1}			
B	100,000,000	10,000,000	1,000,000	100,000
	10^{-2}			
C	10,000,000	1,000,000	100,000	10,000
	10^{-3}			
D	1,110,000	111,000	11,100	1,110
	10^{-6}			
E	1,000	100	10	1

Matrix Relative Risk Values



Matrix Relative Risk Values

	1	2	3	4
A	1,000,000,000	100,000,000	10,000,000	1,000,000
B	100,000,000	10,000,000	1,000,000	100,000
C	10,000,000	1,000,000	100,000	10,000
D	1,000,000	100,000	10,000	1,000
	100,000	10,000	1,000	100
	10,000	1,000	100	10
E	1,000	100	10	1

10^{-1}

10^{-2}

10^{-3}

10^{-4}

10^{-5}

10^{-6}

Matrix Relative Risk Values

	1	2	3	4
A	1,000,000,000 1 in <2 days	100,000,000	10,000,000	1,000,000
B	100,000,000 1 in 18.5 days	10,000,000	1,000,000	100,000
C	10,000,000 1 in 6 months	1,000,000	100,000	10,000
D	1,000,000 1 in 5 years	100,000	10,000	1,000
E	100,000 1 in 50 years	10,000	1,000	100
F	10,000 1 in 500 years	1,000	100	10
G	1,000	100	10	1

Matrix Relative Risk Values

	1	2	3	4
A	10,000,000	1,000,000	100,000	10,000
B	1,000,000	100,000	10,000	1,000
C	100,000	10,000	1,000	100
D	10,000	1,000	100	10
E	1,000	100	10	1

10^{-3}

10^{-4}

10^{-5}

10^{-6}

Matrix Relative Risk Values

	1	2	3	4
A	10,000,000 1 in 6 months	1,000,000	100,000	10,000
B	1,000,000 1 in 5 years	100,000	10,000	1,000
C	100,000 1 in 50 years	10,000	1,000	100
D	10,000 1 in 500 years	1,000	100	10
E	1,000	100	10	1

Matrix Relative Risk Values

	1	2	3	4
A	10,000 1 in 6 months	100,000	1,000,000	10,000,000
B	1,000 1 in 5 years	10,000	100,000	1,000,000
C	100 1 in 50 years	1,000	10,000	100,000
D	10 1 in 500 years	100	1,000	10,000
E	1	10	100	1,000

Topics for this Tutorial

- Purpose of a Hazard Risk Matrix
- Understanding the Attributes of a well-designed risk assessment matrix
- How to Assign a Risk Assessment Code
- Understanding Probability
- Building an Expanded Matrix
- Plotting Accidents on a Matrix
- Using Relative Risk Values
- Building Hazard Risk Profiles
- **Impact on Software Safety Matrices**

Software Safety Criticality Matrix

Worst

SOFTWARE SAFETY CRITICALITY MATRIX				
	SEVERITY CATEGORY			
SOFTWARE CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

Software Safety Criticality Matrix

SOFTWARE SAFETY CRITICALITY MATRIX				
	SEVERITY CATEGORY			
SOFTWARE CONTROL CATEGORY	4	3	2	1
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

Software Control Categories

Worst

SOFTWARE CONTROL CATEGORIES		
Level	**Name**	**Description**
1	**Autonomous (AT)**	• Software functionality that exercises autonomous control authority over potentially safety-significant hardware systems, subsystems, or components without the possibility of predetermined safe detection and intervention by a control entity to preclude the occurrence of a mishap or hazard. *(This definition includes complex system/software functionality with multiple subsystems, interacting parallel processors, multiple interfaces, and safety-critical functions that are time critical.)*
2	**Semi-Autonomous (SAT)**	• Software functionality that exercises control authority over potentially safety-significant hardware systems, subsystems, or components, allowing time for predetermined safe detection and intervention by independent safety mechanisms to mitigate or control the mishap or hazard. *(This definition includes the control of moderately complex system/software functionality, no parallel processing, or few interfaces, but other safety systems/mechanisms can partially mitigate. System and software fault detection and annunciation notifies the control entity of the need for required safety actions.)* • Software item that displays safety-significant information requiring immediate operator entity to execute a predetermined action for mitigation or control over a mishap or hazard. Software exception, failure, fault, or delay will allow, or fail to prevent, mishap occurrence. *(This definition assumes that the safety-critical display information may be time-critical, but the time available does not exceed the time required for adequate control entity response and hazard control.)*
3	**Redundant Fault Tolerant (RFT)**	• Software functionality that issues commands over safety-significant hardware systems, subsystems, or components requiring a control entity to complete the command function. The system detection and functional reaction includes redundant, independent fault tolerant mechanisms for each defined hazardous condition. *(This definition assumes that there is adequate fault detection, annunciation, tolerance, and system recovery to prevent the hazard occurrence if software fails, malfunctions, or degrades. There are redundant sources of safety-significant information, and mitigating functionality can respond within any time-critical period.)* • Software that generates information of a safety-critical nature used to make critical decisions. The system includes several redundant, independent fault tolerant mechanisms for each hazardous condition, detection and display.
4	**Influential**	• Software generates information of a safety-related nature used to make decisions by the operator, but does not require operator action to avoid a mishap.
5	**No Safety Impact (NSI)**	• Software functionality that does not possess command or control authority over safety-significant hardware systems, subsystems, or components and does not provide safety-significant information. Software does not provide safety-significant or time sensitive data or information that requires control entity interaction. Software does not transport or resolve communication of safety-significant or time sensitive data.

Software Safety Criticality Index (SwCI)

Worst

SwCI	Level of Rigor Tasks
SwCI 1	Program shall perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.
SwCI 2	Program shall perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SwCI 3	Program shall perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SwCI 4	Program shall conduct safety-specific testing.
SwCI 5	Once assessed by safety engineering as Not Safety, then no safety specific analysis or verification is required.

Functional Control Categories (FCC) and Safety Function Criticality Index*

Function control categories (FCC)

FCC	Name	Description
4	Autonomous (AT)	Function exercises control authority over safety-significant hardware systems, subsystems or components without the possibility of predetermined safe detection and intervention by an independent safety control entity to preclude the occurrence of a mishap. -OR- Function that displays safety-significant information that does not allow time for the operator (time is critical) to execute any action (e.g., independently validate display data) that would prevent or eliminate the occurrence of a mishap. -OR- In the case of function failure, there is no functioning interlock that would prevent or eliminate the occurrence of a mishap.
3	Semi-Autonomous (SAT)	Function exercises control authority over safety-significant hardware systems, subsystems or components, allowing time for predetermined safe detection and intervention by an independent safety control entity to preclude the occurrence of a mishap. -OR- Function that displays safety-significant information, allowing the operator (with sufficient time) to execute an action for mitigation or control over a mishap. The operator must be trained to perform this action. -OR- In the case of function failure, there is at least one functioning interlock that would prevent or eliminate the occurrence of a mishap.
2	Redundant Fault Tolerant (RFT)	Function that issues commands over safety-significant hardware systems, subsystems, or components but requires a safety control entity to complete the command function. The system must provide the safety control entity sufficient notification of a failure or potential unsafe state. The system must additionally include one or more interlocks that would preclude the occurrence of a mishap. -OR- Function that generates information or display of a safety-significant nature used by a safety control entity to make safety significant decisions. The system includes two or more interlocks that would preclude the occurrence of a mishap. -OR- In the case of function failure, the system includes two or more independent interlocks that preclude the occurrence of a mishap.
1	Influential	Function generates information of a safety-related nature used to make decisions by the operator but does not require operator action to avoid a mishap. -OR- In the case of function failure, the system includes three or more independent interlocks that preclude the occurrence of a mishap.
0	No Safety Impact (NSI)	Function does not possess command or control authority over safety-significant hardware systems, subsystems, or components and does not provide safety-significant information. Function does not provide safety-significant data or information that requires control entity interaction. Function does not transport or resolve communication of safety-significant data.

Safety Function Criticality Index Matrix

	Severity					
Function Control Category (FCC)	**1**	**2**	**3**	**4**	**5**	**6 and Up**
4	SFCI 1	SFCI 2	SFCI 4	SFCI 4	SFCI 4	SFCI 4
3	SFCI 1	SFCI 2	SFCI 3	SFCI 4	SFCI 4	SFCI 4
2	SFCI 1	SFCI 1	SFCI 2	SFCI 3	SFCI 4	SFCI 4
1	SFCI 1	SFCI 1	SFCI 1	SFCI 2	SFCI 3	SFCI 4
0	SFCI 0 - No Safety Impact					

Safety Function Criticality Index Level or Rigor Tasks

SFCI	**Level of Rigor Tasks**
SFCI 4	Perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.
SFCI 3	Perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SFCI 2	Perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SFCI 1	Identify and track safety-critical requirements. Follow normal development processes. Conduct safety-specific testing.
SFCI 0	No safety specific analysis or verification required.

***See: DoD White Paper: Guidance to Perform Functional Hazard Analysis for Weapon Systems with Artificial Intelligence Capabilities**

Summary

Summary
Attributes of a well-designed risk assessment matrix

- ✔ Severity scale covers full range of possible outcomes
- ✔ Probability calibrated with reference to an exposure interval
- ✔ Equally proportioned, logarithmic scales (1, 10, 100, 1000…)
- ✔ Cartesian Orientation – Increase up and to the right
- ✔ Risk levels assigned to cells consistent with contours of equal risk

Severity		1	2	3	4	5	6	7	8
		≥$2k	≥$20k	≥$200k	≥$2M	≥$20M	≥$200M	≥$2B	≥$20B
Frequency		Injury, no lost work day	Lost Work Day	Permanent partial disability	≥1 Fatality	≥10 Fatalities	≥100 Fatalities	≥1,000 Fatalities	≥10,000 Fatalities
A	>100								
B	>10								
C	>1						Prohibitive SECDEF		
D	>0.1					High - CAE			
E	>0.01				Serious - PEO				
F	>0.001			Medium - PM					
G	>0.0001	Low – SSWG/Principal for Safety							
H	>0.00001								
I	> 0.000001								
J	≤ 0.000001								

Summary
Attributes of a well-designed risk assessment matrix

- ✔ Sufficient probability categories so highest severity level reach the PM level
- ✔ Frequency category letters increase with decreasing frequency
- ✔ A RAC for hazards whose risk has been eliminated
- ✔ Easily tailored & consistent with other systems within its family of systems
- ✔ Severity Category numbers increase with increasing Severity

Severity		1	2	3	4	5	6	7	8
		≥$2k	≥$20k	≥$200k	≥$2M	≥$20M	≥$200M	≥$2B	≥$20B
Frequency		Injury, no lost work day	Lost Work Day	Permanent partial disability	≥1 Fatality	≥10 Fatalities	≥100 Fatalities	≥1,000 Fatalities	≥10,000 Fatalities
A	>100								
B	>10								
C	>1								
D	>0.1								
E	>0.01								
F	>0.001								
G	>0.0001								
H	>0.00001								
I	> 0.000001								
J	≤ 0.000001								

Prohibitive SECDEF
High - CAE
Serious - PEO
Medium - PM
Low – SSWG/Principal for Safety

How to Determine the Risk Assessment Code (RAC)

To determine the appropriate RAC for a given hazard:

(1) Identify the full range of potential outcomes for the hazard (death, injury, system loss, environmental impact, and monetary loss). The range of outcomes will often span more than one severity category.

(2) For each severity category associated with this range of severity, determine the associated probability category.

(3) Determine which severity-probability pair has the greatest risk. This pair is the RAC assigned to the hazard.

(4) If two or more severity-probability pairs are equal as the greatest risk, select the one with the greatest severity.

Summary Understanding Probability

Math Definition:

- **Repeat a random experiment "n" number of times.**
- **If a specific outcome has occurred "f" times in these n trials, the number "f" is the frequency of the outcome.**
- **The ratio f/n is the relative frequency of the outcome.**
- **A relative frequency is usually very unstable for small values of "n," but it tends to stabilize about some number "p" as "n" increases.**
- **The number "p" is the probability of the outcome.**

$$p = f / n$$

for very large values of n

Simple example:

Probability of rolling a "3" with one die.

Roll #1 - "5", f/n = 0

Roll #2 - "2", f/n = 0

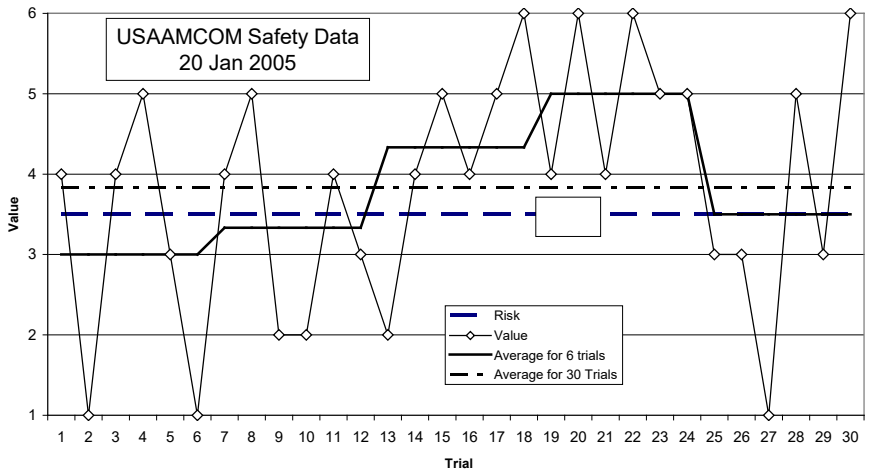
Roll #3 - "3", f/n = 1/3 = .333…

Roll #4 - "4", f/n = 1/4 = .25

Roll #1,000: 163 "3"s, f/n = 163/1000 = .163

Rolls approach infinity f/n = .166666….

Roll a single die 30 times. The expe
What you actually get is somewhat



Hazard: AH-64 strikes wire results in Class A mishap

Probability: 4.406E-06 occurrences per flight hour

1 Flight Hr, no mishap, rate = 0

1,000 Flight Hrs, no mishap, rate = 0

176,182 Flight Hrs, 1 mishap, rate = 5.676E-06 /flt hr

274,539 Flight Hrs, 2 mishaps, rate = 7.285E-06 /flt hr

700,462 Flt Hrs, 3 mishaps, rate = 4.283E-06 /flt hr

10,000,000 Flt Hrs, 46 mishaps, rate = 4.600E-06 /flt hr

1,000,000,000 Hrs, 4407 mishaps, rate = 4.407E-06 /flt hr

Flight hours approach infinity, rate = 4.406E-06 /flt hr

Summary Expanded Matrix

Applying Probability Classifications to a military helicopter

Fleet Size = 368 aircraft

Utilization = 240 hours/year

Life = 20 years/aircraft

Aircraft Life = 240 x 20
= 4,800 hours

Fleet Exposure Hours = 368 x 240 x 20
= 1,776,400 hours

Fleet Hours per Year = 368 x 240
= 88,320 hours

US Army PEO Aviation Expanded Matrix

	Events per Flight Hour	Flight Hours per Event	Events per 100,000 Flt Hrs	Events per Year	Years per Event	Event per Fleet Life	Fleet Life per Event
Frequent A	10^{-3}	1,000	100	88.32	0.0113	1,060	0.000944
Probable B	10^{-4}	10,000	10	8.832	0.113	105.98	0.00944
Occasional C	10^{-5}	100,000	1	0.8832	1.13	10.598	0.0944
Remote D	10^{-6}	1,000,000	0.1	0.0883	11.3	1.0598	0.944
Improbable E	10^{-7}	10,000,000	0.01	0.00883	113	0.106	9.44
Very Improbable F	0		0	0		0	
Zero Risk 0R							

Numbers greater than 1 are easier to comprehend

29

16

Input

Calculated

Assumptions	
Fleet Size:	368 aircraft
Utilization:	240.0 hours/yr
Aircraft Life:	12 years
Calculations	
Aircraft Exposure Hours:	2,880 hours
Fleet Exposure Hours:	1,059,840 hours
Fleet Hours per Year:	88,320 hours

	Events per Flight Hour	Flight Hours per Event	Events per 100,000 Flt Hrs	1 Catastrophic ($10M)	2 Critical ($1M)	3 Marginal ($100K)	4 Negligible	Fleet-wide: Events per Year	Years per Event	Event per Fleet Life	Fleet Life per Event
Frequent A	10^{-3}	1,000	100	1A (High AAE)	2A	3A	4A	88.32	0.0113	1,060	0.000944
Probable B	10^{-4}	10,000	10	1B (High AAE)	2B	3B	4B	8.832	0.113	105.98	0.00944
Occasional C	10^{-5}	100,000	1	1C (High AAE)	2C (Serious PEO)	3C	4C	0.8832	1.13	10.598	0.0944
Remote D	10^{-6}	1,000,000	0.1	1D	2D	3D	4D	0.0883	11.3	1.0598	0.944
Improbable E	10^{-7}	10,000,000	0.01	1E	2E (Medium PM)	3E	4E	0.00883	113	0.106	9.44
Very Improbable F	0		0	1F	2F (Low PM)	3F	4F	0		0	
Zero Risk 0R											

Summary

Accidents on a Matrix

Based on this relationship between mishap risk and mishap loss, we can plot mishap histories on a risk matrix as follows:

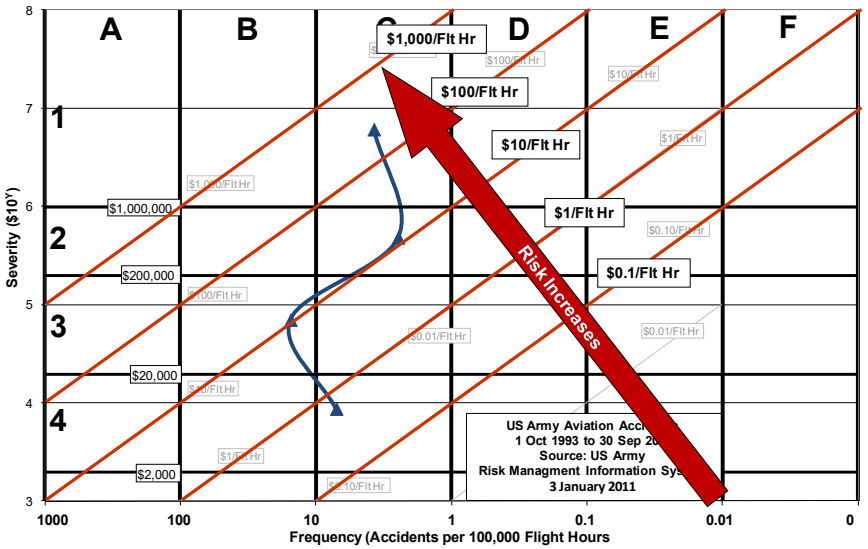
$$\text{Severity} = \frac{\text{Total Cost from Class A mishaps}}{\text{Total Number of Class A mishaps}}$$

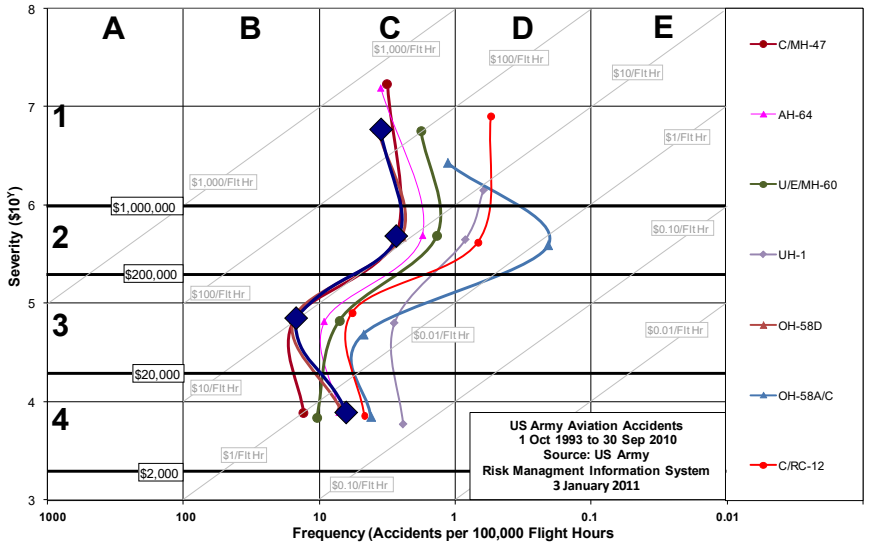
$$= \frac{\$1{,}305{,}079{,}886}{83} = \$\ 15{,}723{,}854$$

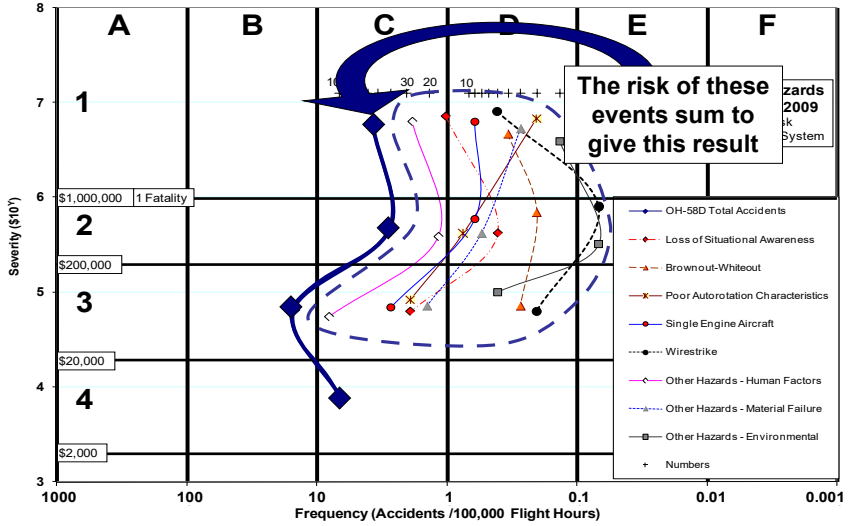
$$\text{Probability} = \frac{\text{Total Number of Class A mishaps}}{\text{Total Hours Flown}}$$

$$= \frac{83}{2{,}351{,}860} = 3.529 \text{ mishaps / 100,000 Flt Hrs}$$

21







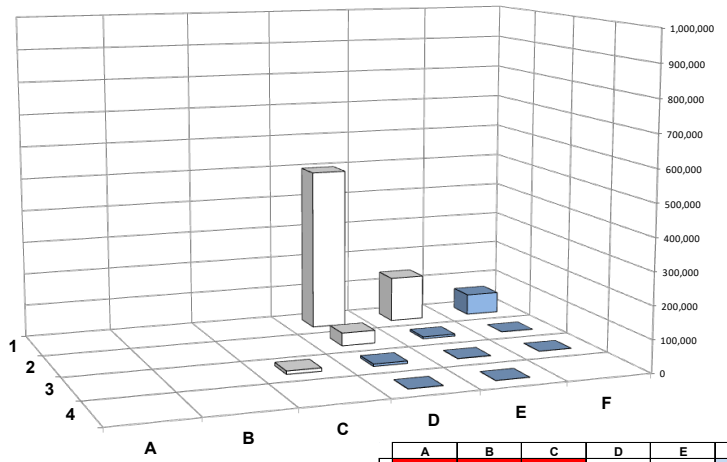
Summary

	A	B	C	D	E	F
1	100,000,000	10,000,000	1,000,000	100,000	10,000	1,000
2	10,000,000	1,000,000	100,000	10,000	1,000	100
3	1,000,000	100,000	10,000	1,000	100	10
4	100,000	10,000	1,000	100	10	1

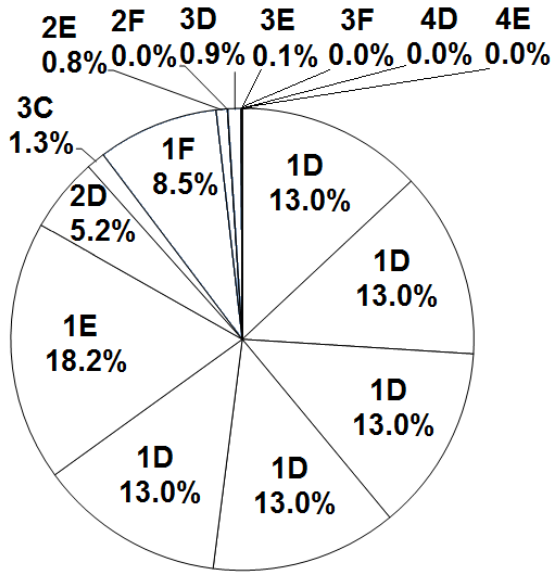
Relative Risk Values (Clemens)

	A	B	C	D	E	F
1				500,000	140,000	65,000
2				40,000	6,000	200
3			10,000	7,000	500	40
4				200	10	

Helicopter A



	A	B	C	D	E	F
1				5	14	65
2				4	6	2
3			1	7	5	4
4				2	1	



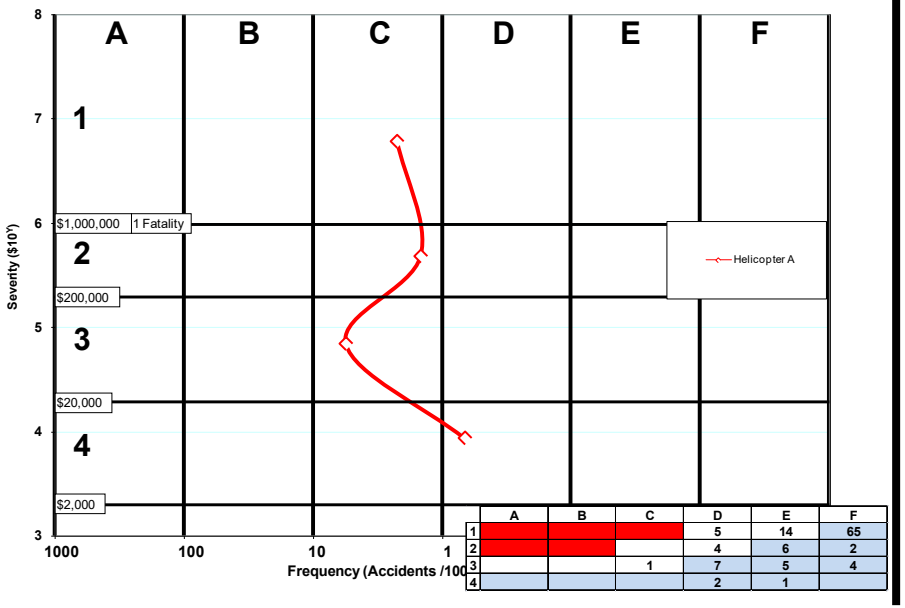
	A	B	C	D	E	F
1				5	14	65
2				4	6	2
3			1	7	5	4
4				2	1	

Summary

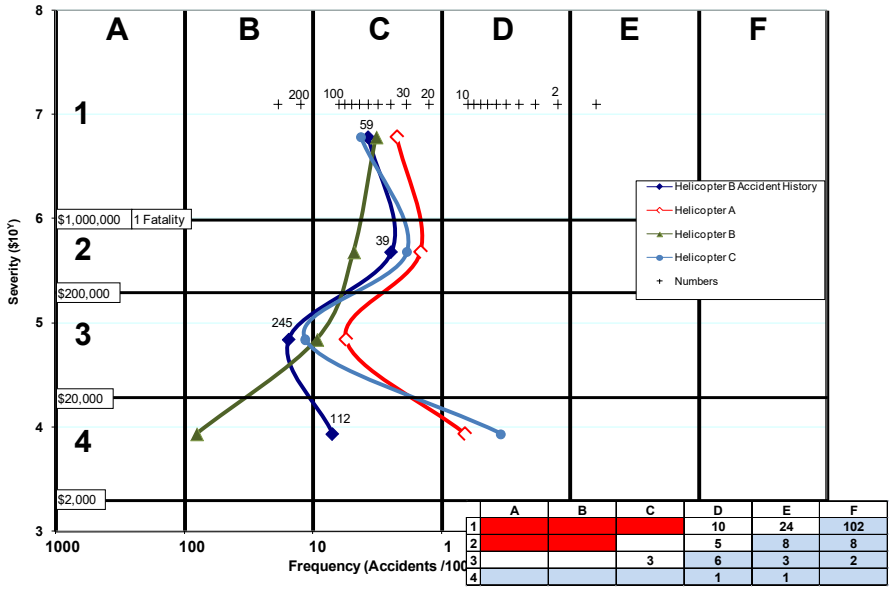
Hazard Risk Profile

	3.16E-04 A	3.16E-05 B	3.16E-06 C	D	3.16E-07 E	3.16E-08 F
1					14	65
2					6	2
3			1		5	4
4					1	

	A	B	C	D	E	F
1	2.23E-05	Sum		5 x 3.16E-06 = 1.58E-05	14 x 3.16E-07 = 4.43E-06	65 x 3.16E-08 = 2.06E-06
2	1.46E-05	Sum		4 x 3.16E-06 = 1.26E-05	6 x 3.16E-07 = 1.90E-06	2 x 3.16E-08 = 6.32E-08
3	5.55E-05	Sum	1 x 3.16E-05 = 3.16E-05	7 x 3.16E-06 = 2.21E-05	5 x 3.16E-07 = 1.58E-06	4 x 3.16E-08 = 1.26E-07
4	6.64E-06	Sum		2 x 3.16E-06 = 6.32E-06	1 x 3.16E-07 = 3.16E-07	



	A	B	C	D	E	F
1				5	14	65
2				4	6	2
3			1	7	5	4
4				2	1	



	A	B	C	D	E	F
1				10	24	102
2				5	8	8
3			3	6	3	2
4				1	1	

Summary

Missile Risk Matrix

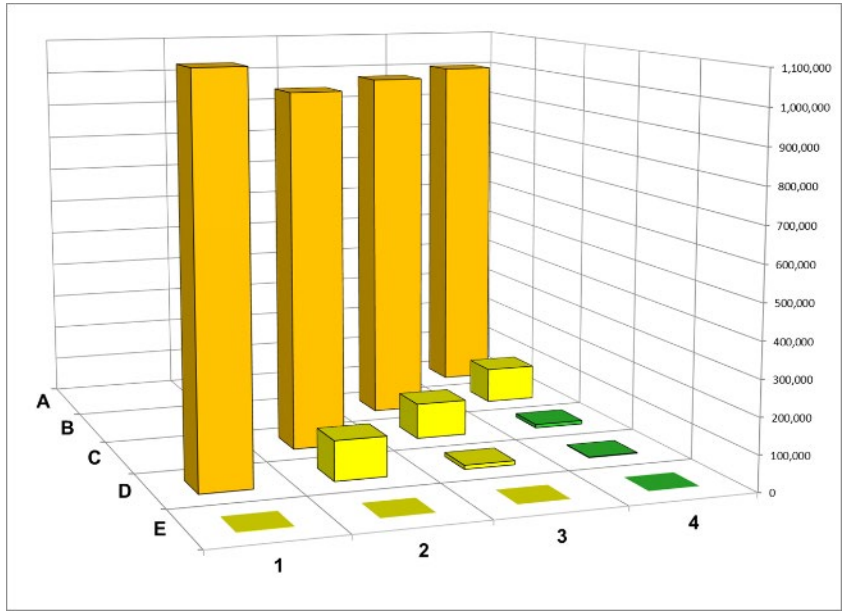
RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY *	Catastrophic (1) 1 Fatal $10M	Critical (2) $1M	Marginal (3) $100K	Negligible (4)
Frequent (A) 10^{-1}	High	High	Serious	Medium
Probable (B) 10^{-2}	High	High	Serious	Medium
Occasional (C) 10^{-3}	High	Serious	Medium	Low
Remote (D) 10^{-6}	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Back of the Envelope Calculation

40,000 Shishkebab Missiles
Delivered over 20 years
Assume all fired
1 accident in 1,000,000 firings

$$\frac{\text{1 accident}}{\text{1,000,000 ~~firings~~}} \times \frac{\text{40,000 ~~firings~~}}{\text{20 years}} = \frac{\text{1 accident}}{\text{500 years}}$$

	1	2	3	4
A	1,000,000,000	100,000,000	10,000,000	1,000,000
B 10^{-1}	100,000,000	10,000,000	1,000,000	100,000
C 10^{-2}	10,000,000	1,000,000	100,000	10,000
D 10^{-3}	1,000,000	100,000	10,000	1,000
10^{-4}	100,000	10,000	1,000	100
10^{-5}	10,000	1,000	100	10
10^{-6}				
E	1,000	100	10	1



Summary

Software Risk Matrix

Function control categories (FCC)

FCC	Name	Description
4	Autonomous (AT)	Function exercises control authority over safety-significant hardware systems, subsystems or components without the possibility of predetermined safe detection and intervention by an independent safety control entity to preclude the occurrence of a mishap. -OR- Function that displays safety-significant information that does not allow time for the operator (time is critical) to execute any action (e.g., independently validate display data) that would prevent or eliminate the occurrence of a mishap. -OR- In the case of function failure, there is no functioning interlock that would prevent or eliminate the occurrence of a mishap.
3	Semi-Autonomous (SAT)	Function exercises control authority over safety-significant hardware systems, subsystems or components, allowing time for predetermined safe detection and intervention by an independent safety control entity to preclude the occurrence of a mishap. -OR- Function that displays safety-significant information, allowing the operator (with sufficient time) to execute an action for mitigation or control over a mishap. The operator must be trained to perform this action. -OR- In the case of function failure, there is at least one functioning interlock that would prevent or eliminate the occurrence of a mishap.
2	Redundant Fault Tolerant (RFT)	Function that issues commands over safety-significant hardware systems, subsystems, or components but requires a safety control entity to complete the command function. The system must provide the safety control entity sufficient notification of a failure or potential unsafe state. The system must additionally include one or more interlocks that would preclude the occurrence of a mishap. -OR- Function that generates information or display of a safety-significant nature used by a safety control entity to make safety significant decisions. The system includes two or more interlocks that would preclude the occurrence of a mishap. -OR- In the case of function failure, the system includes two or more independent interlocks that preclude the occurrence of a mishap.
1	Influential	Function generates information of a safety-related nature used to make decisions by the operator but does not require operator action to avoid a mishap. -OR- In the case of function failure, the system includes three or more independent interlocks that preclude the occurrence of a mishap.
0	No Safety Impact (NSI)	Function does not possess command or control authority over safety-significant hardware systems, subsystems, or components and does not provide safety-significant information. Function does not provide safety-significant data or information that requires control entity interaction. Function does not transport or resolve communication of safety-significant data.

Safety Function Criticality Index Matrix

	Severity					
Function Control Category (FCC)	**1**	**2**	**3**	**4**	**5**	**6 and Up**
4	SFCI 1	SFCI 2	SFCI 4	SFCI 4	SFCI 4	SFCI 4
3	SFCI 1	SFCI 2	SFCI 3	SFCI 4	SFCI 4	SFCI 4
2	SFCI 1	SFCI 1	SFCI 2	SFCI 3	SFCI 4	SFCI 4
1	SFCI 1	SFCI 1	SFCI 1	SFCI 2	SFCI 3	SFCI 4
0	SFCI 0 - No Safety Impact					

Safety Function Criticality Index Level or Rigor Tasks

SFCI	**Level of Rigor Tasks**
SFCI 4	Perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.
SFCI 3	Perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SFCI 2	Perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SFCI 1	Identify and track safety-critical requirements. Follow normal development processes. Conduct safety-specific testing.
SFCI 0	No safety specific analysis or verification required.

Take-aways

- High degree of precision? – No
- Gets hazards to the correct cell of the matrix
- Confidence that overall assessment ≈ reality
- Helps communicate risk to the risk acceptor
- Very useful for programs with:
  - Reasonably good accident data for analysis
  - A well-designed matrix
- Just one of many tools for managing system safety risk

For Further Reading

Clemens, P. L. (2000). Comments on the MIL-STD-882D Example Risk Assessment Matrix. Journal of System Safety, 20-24.

Clemens, P. L., Pfitzer, T., Simmons, R. J., Dwyer, S., Frost, J., & Olson, E. (2005). The RAC Matrix: A Universal Tool or a Toolkit? Journal of System Safety, Vol. 41, No. 2, 14-19.

Swallom, D. W. (2003). Developing a Common Risk Assessment Matrix for U.S. Army Aviation. Proceedings of the 21st International System Safety Conference. Ottawa, Ontario, Canada.

Swallom, D. W. (2005). A Common Mishap Risk Assessment Matrix for United States Department of Defense Aircraft Systems. Proceedings of the 23rd International System Safety Conference. San Diego, California.

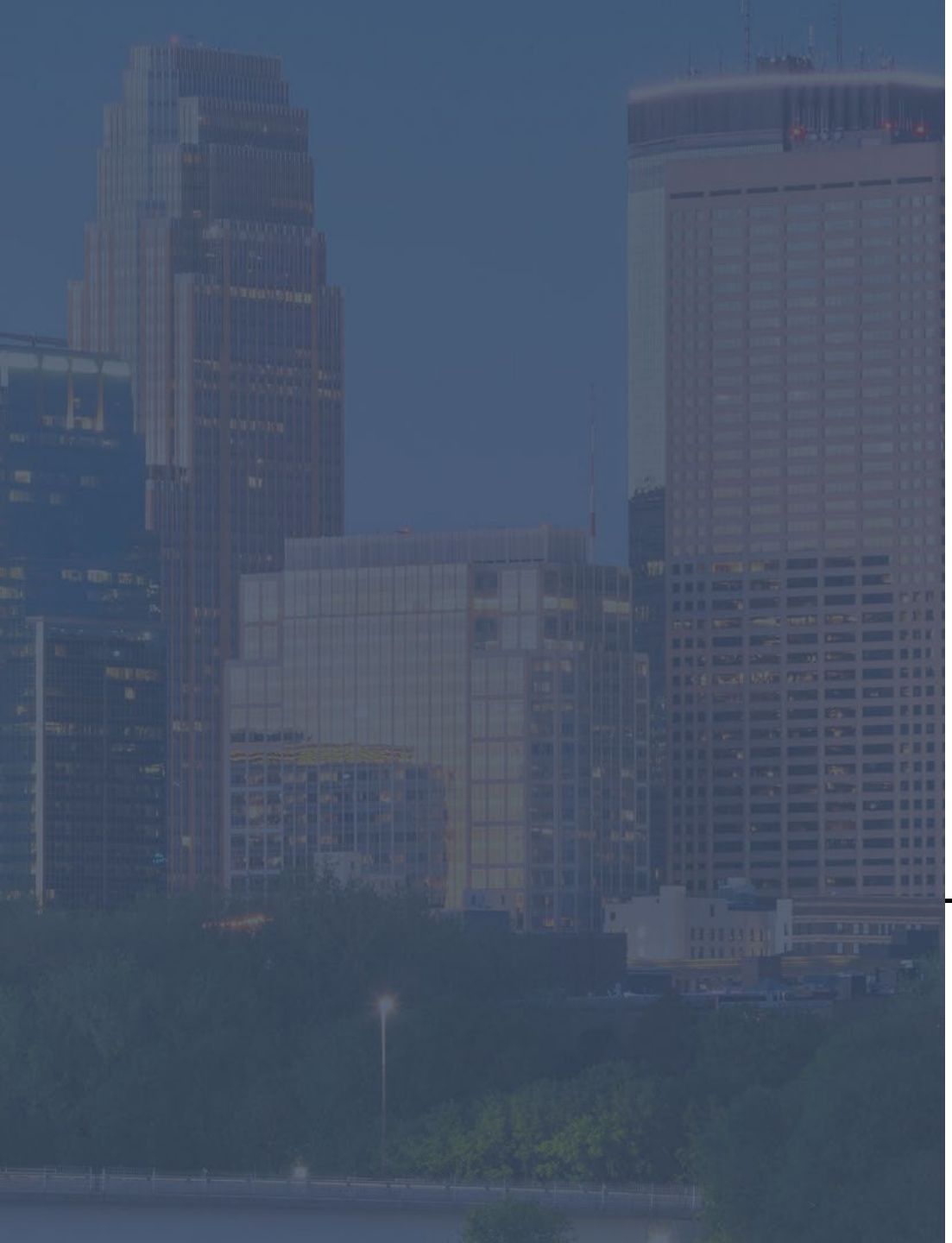
Swallom, D. W. (2006). An Improved Accident Severity Classification Scheme for United States Department of Defense Systems. Proceedings of the 24th International System Safety Conference. Albuquerque, New Mexico.

Swallom, D. W. (2008). Constructs for System Safety: Consequence, Likelihood, and Loss. Proceedings of the International System Safety Regional Conference. Singapore.

Swallom, D. W. (2011). Mathematical Techniques to Improve the Utility of a Hazard Risk Matrix. ” Proceedings of the 29th International System Safety Conference. Las Vegas, Nevada.

Swallom, D. W. (2012). Business Case for Using a Numbered Logarithmic Risk Severity Scale. Proceedings of the 30th International System Safety Conference. Atlanta, Georgia.

DoD Joint Weapon Safety Working Group (JWSWG) (2022). White Paper: Guidance to Perform Functional Hazard Analysis for Weapon Systems with Artificial Intelligence Capabilities.



Questions?

https://www.isss-tvc.org/SwallomD_Tutorial_Math_2024.pdf

Don Swallom
A-P-T Research, Inc. | An Employee-Owned Company
mobile: 256.583.4314
email: dswallom@apt-research.com
address: 4950 Research Drive, Huntsville, AL 35805
web: www.apt-research.com