#### Applications of System Safety Engineering in Improving Safety & Health

#### HKOSHA Safety Conference 26 July 2008

#### Vincent Ho

Chairman, HKARMS www.hkarms.org Immediate Past Chairman, IOSH (HK) Past Chairman, HKIE-SSC

# System Safety is....

- The application of engineering and management principles, criteria, and techniques to optimise Safety within the constraints of operational effectiveness, time, and cost throughout <u>all phases</u> of the System life cycle
- Primarily a <u>management tool</u> that applies special technical and managerial skills to the systematic, forward-looking identification and control of hazards <u>throughout the life</u> <u>cycle</u> of a project, program, or activity
- Addressing safety at a system level. (A system is a composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software)

#### System Safety *≠* Systems Safety



# **Objective of System Safety**

- To assure that a system does what it is supposed to do and does not do what it is not supposed to do
- To achieve acceptable mishap risk through a systematic approach of hazard analysis, risk assessment, and risk management *MIL-STD-882D, Department of Defense, USA*

#### Three Key Applications of System Safety Engineering in Improving Safety & Health

- Proof of safety
- Hazard identification and evaluation
- Prioritization of risks/resources

# **Proof of Safety: Risk Management Programme**



Contrac System: Subsyst	et No: : em:		Hazard Analysis Work Sheet							P R A	Prepared by: Reviewed by: Authorised by:			Date: Date: Date:		
Ref No.	Hazard Scenario Description/	Op. Mode	Existing Safeguard/ Control Measure	xisting feguard/ Ind Massures		et	Proposed Mitigation Measures/Control	Residu Impa		dual act		Comment/ Resolution	Status	Responsibility	Days Remained	
	Consequence		Control Measure	L		ĸ	G		L		к	G				Open

People often mistakenly think that it is THE" only way to do hazard or risk analysis... NOT

# **Example of Risk Matrices**

	Consequence Class							
		R – Service- Related	Cl – Trivial	C2 – Minor	C3 – Serious	C4 – Critical	C5 – Disastrous	
	F1 – Frequent (>10/yr)	R	В	A	A	A	А	
8	F2 - Common (1/yr to 10/yr)	R	В	В	A	A	А	
Clas	F3 - Likely (0.1/yr to 1/yr)	R	С	В	A	A	А	
ency	F4 - Rare (0.01/yr to 0.1/yr)	R	С	С	В	A	A	
requ	F5 – Unlikely (10 <sup>-3</sup> /yr to 0.01/yr)	R	D	С	с	В	А	
Ŧ	F6 – Improbable (10 <sup>-4</sup> /yr to 10 <sup>-3</sup> /yr)	R	D	D	С	С	В	
	F7 – Incredible (<10 <sup>-4</sup> /yr)	R	D	D	D	С	с	

Risk Class	Description
A	<b>High Risk</b> – Risk control measures should be implemented to mitigate the risk to a level that is ALARP with a top priority.
В	<b>Medium Risk</b> – Cost-effective risk control measures should be implemented to mitigate the risk to a level that is ALARP within a reasonable time.
С	Low Risk – Cost-effective risk control measures should be implemented to mitigate the risk to a level that is ALARP with a low priority.
D	<b>Negligible Risk</b> – Risk is considered acceptable; no additional risk control action is normally required. Cost-effective risk control measures may be implemented to further mitigate the risk with the lowest priority.

# **Risk Acceptance Concept - ALARP**



Limit

# **Risk Matrix Should Actually be Designed by Quantitative Input**

	- /								
Tolera			0	0.001	0.01	0.1	1	10	20
e/db/e			S1	S2	S3	S4	S5	S6	S7
		G. Mean	0.000	0.003	0.03	0.32	3.16	14.14	44.72
	F1	31.62	1.00E-02	0.10	1.00	10.12	99.93	447.15	1414.21
661e	F2	3.16	1.00E-03	1.00E-02	0.10	1.01	9.99	44.71	141.42
	F3	0.32	1.00E-04	1.00E-03	1.00E-02	0.10	1.00	4.47	14.14
	F4	3.16E-02	1.00E-05	1.00E-04	1.00E-03	1.01E-02	0.10	0.45	1.41
	F5	3.16E-03	1.00E-06	1.00E-05	1.00E-04	1.01E-03	9.99E-03	0.04	0.14
	F6	3.16E-04	1.00E-07	1.00E-06	1.00E-05	1.01E-04	9.99E-04	4.47E-03	0.014
	F7	0.00	1.00E-08	1.00E-07	1.00E-06	1.01E-05	9.99E-05	4.47E-04	1.41E-03
	Tolerable acjustole	Fl Fl   F2 F3   F4 F5   F6 F7	Fl G. Mean   F1 31.62   F2 3.16   F3 0.32   F4 3.16E-02   F5 3.16E-03   F6 3.16E-04   F7 0.00	Colerable 0   S1 G. Mean 0.000   F1 31.62 1.00E-02   F2 3.16 1.00E-03   F3 0.32 1.00E-04   F4 3.16E-02 1.00E-05   F5 3.16E-03 1.00E-06   F6 3.16E-04 1.00E-07   F7 0.00 1.00E-08	Olerable 0 0.001   S1 S2   G. Mean 0.000   F1 31.62   F2 3.16   F3 0.32   F4 3.16E-02   F3 1.00E-03   F4 3.16E-02   F5 3.16E-03   F6 3.16E-04   F7 0.00   F7 0.00	Olerable 0 0.001 0.01   S1 S2 S3   G. Mean 6.000 0.003 0.03   F1 31.62 1.00E-02 6.40 1.00   F2 3.16 1.00E-03 1.00E-02 6.40   F3 0.32 1.00E-04 1.00E-03 1.00E-02   F4 3.16E-02 1.00E-04 1.00E-03 1.00E-03   F5 3.16E-03 1.00E-06 1.00E-05 1.00E-04   F6 3.16E-04 1.00E-07 1.00E-06 1.00E-05   F7 0.00 1.00E-08 1.00E-07 1.00E-06	O 0.001 0.01 0.1   S1 S2 S3 S4   G. Mean 0.000 0.003 0.03 0.32   F1 31.62 1.00E-02 0.40 1.00 10.12   F2 3.16 1.00E-02 0.40 1.00 10.12   F3 0.32 1.00E-03 1.00E-02 0.40 1.01   F3 0.32 1.00E-04 1.00E-03 1.00E-02 0.40   F4 3.16E-02 1.00E-04 1.00E-03 1.00E-02 0.40   F4 3.16E-02 1.00E-04 1.00E-03 1.00E-03 1.01E-02   F5 3.16E-03 1.00E-06 1.00E-04 1.00E-03 1.01E-03   F6 3.16E-04 1.00E-07 1.00E-06 1.01E-04   F7 0.00 1.00E-08 1.00E-07 1.00E-06 1.01E-05	Colorable 0 0.001 0.01 0.1 1   S1 S2 S3 S4 S5   G. Mean 0.900 0.003 0.03 0.32 3.16   F1 31.62 1.00E-02 0.40 1.00 10.12 99.93   F2 3.16 1.00E-03 1.00E-02 0.40 1.01 9.99   F3 0.32 1.00E-04 1.00E-03 1.00E-02 0.40 1.01 9.99   F3 0.32 1.00E-04 1.00E-03 1.00E-02 0.40 1.00 1.01 9.99   F4 3.16E-02 1.00E-04 1.00E-03 1.01E-02 0.40 1.00   F4 3.16E-02 1.00E-06 1.00E-04 1.01E-03 9.99E-03   F6 3.16E-04 1.00E-07 1.00E-06 1.00E-06 1.01E-04 9.99E-04   F7 0.00 1.00E-08 1.00E-07 1.00E-06 1.01E-05 9.99E-05	Clereble 0 0.001 0.01 0.1 1 10   S1 S2 S3 S4 S5 S6   G. Mean 0.900 0.003 0.03 0.32 3.16 14.14   F4 31.62 1.00E-02 0.40 1.00 10.12 99.93 447.15   F2 3.16 1.00E-02 0.40 1.00 10.12 99.93 447.15   F2 3.16 1.00E-03 1.00E-02 0.40 1.01 9.99 44.71   F3 0.32 1.00E-04 1.00E-03 1.00E-02 0.40 1.00 4.47   F4 3.16E-02 1.00E-04 1.00E-03 1.01E-02 0.40 0.45   F5 3.16E-03 1.00E-06 1.00E-04 1.01E-03 9.99E-03 0.04   F6 3.16E-04 1.00E-07 1.00E-06 1.01E-04 9.99E-04 4.47E-03   F7 0.00 1.00E-08 1.00E-06 1.01E-05 9.99E-05 4.47E-0

#### Prioritization of Risks/Resources: Cost/Risk-Benefit Ratio



#### where:

i

- = *i*<sup>th</sup> decision alternative
- $\begin{array}{ll} B/C_i &= Benefit-to-cost\ ratio\ of\ decision\ alternative\ i \\ Risk_{i,baseline} &= Baseline\ risk\ for\ decision\ alternative\ i \\ Risk_{i,improved} &= Residual\ risk\ following\ implementation\ of \\ decision\ alternative\ i \\ Cost_i &= cost\ of\ decision\ alternative\ i \end{array}$

### www.hkarms.org





