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….

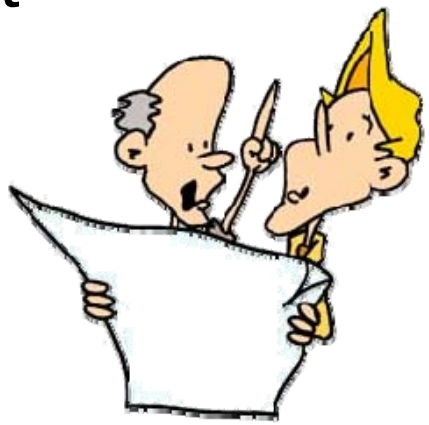
- The application of engineering and management principles, criteria, and techniques to optimise Safety within the constraints of operational effectiveness, time, and cost throughout all phases of the System life cycle
- Primarily a management tool that applies special technical and managerial skills to the systematic, forward-looking identification and control of hazards throughout the life cycle 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

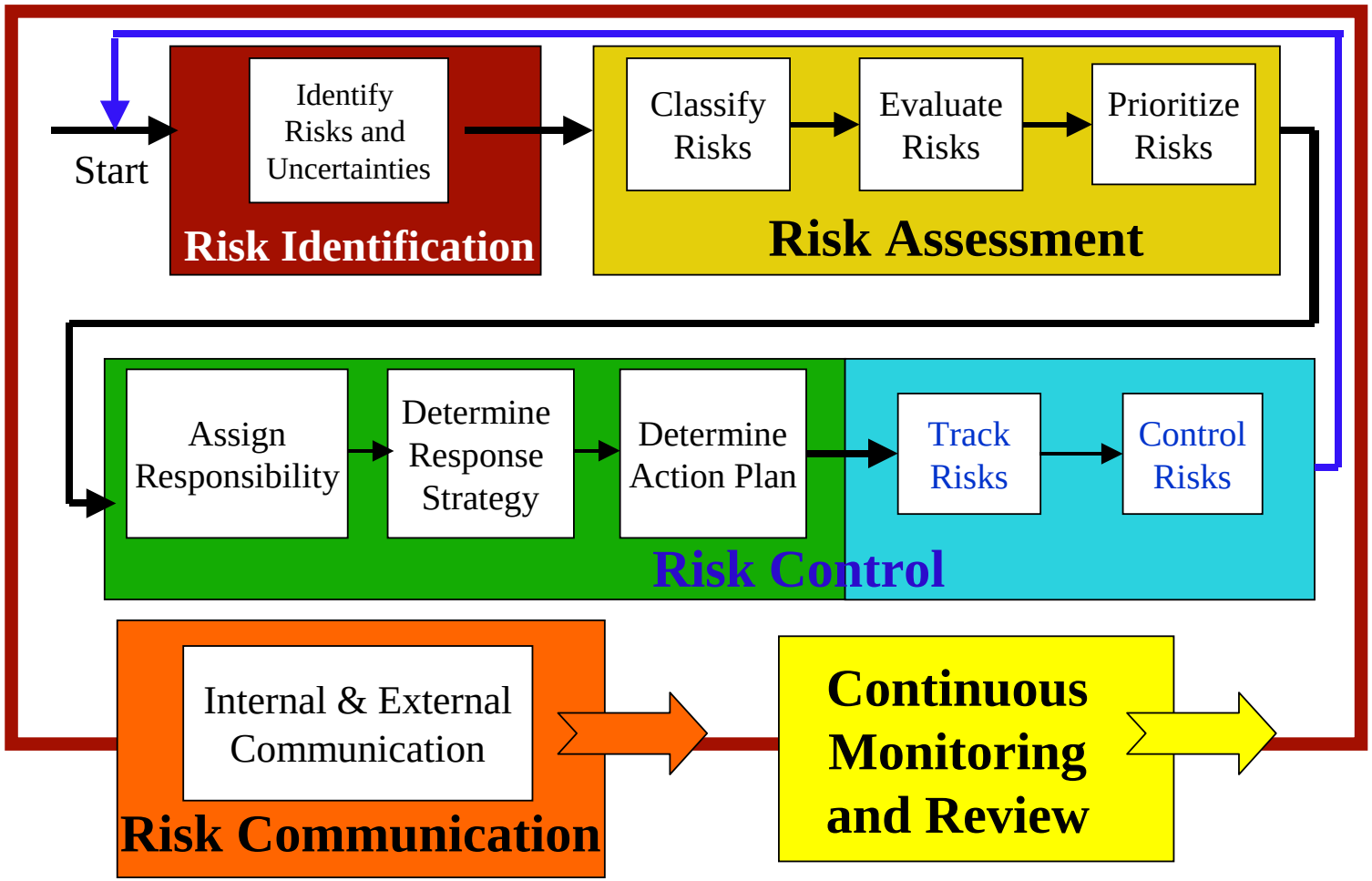
  MIL-STD-882D, Department of Defense, USA



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



Contract No: System: Subsystem:			Hazard Analysis Work Sheet						Prepared by: Reviewed by: Authorised by:				Date: Date: Date:			
Ref No.	Hazard Scenario Description/ Consequence	Op. Mode	Existing Safeguard/ Control Measure	Risk Impact				Proposed Mitigation Measures/Control	Residual Impact				Comment/ Resolution	Status	Responsibility	Days Remained Open
				L	C	R	G		L	C	R	G				

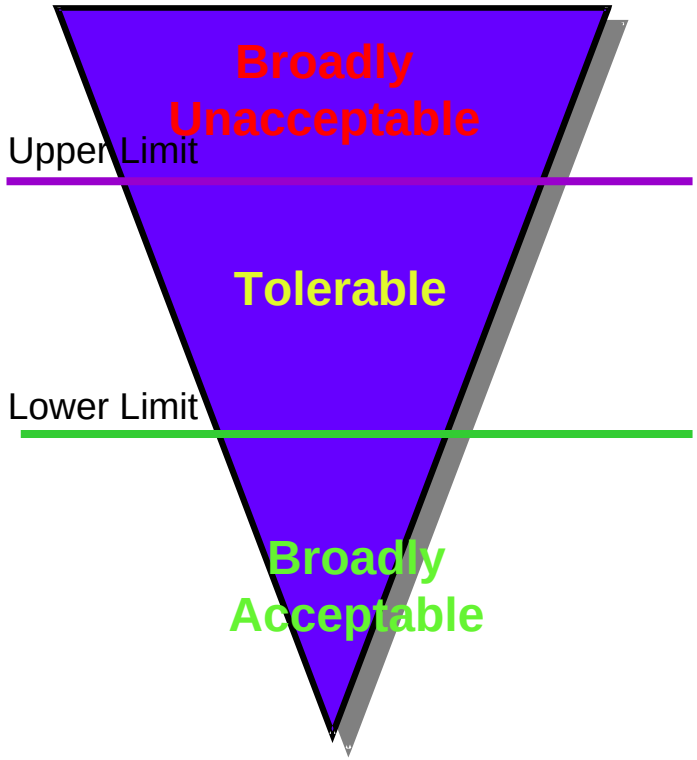
People often mistakenly think that it is THE" only way to do hazard or risk analysis… NOT

Example of Risk Matrices

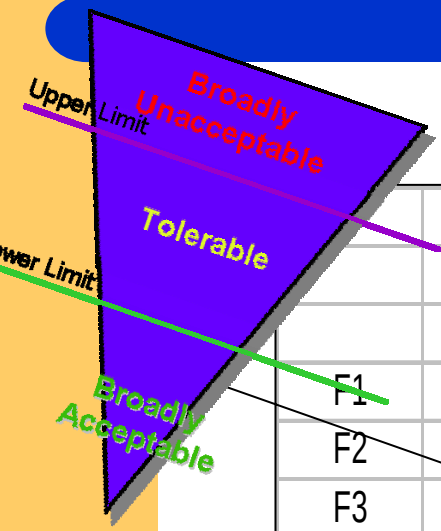
Frequency Class	Consequence Class: R – Service-Related	C1 – Trivial	C2 – Minor	C3 – Serious	C4 – Critical	C5 – Disastrous
F1 – Frequent (>10/yr)	R	B	A	A	A	A
F2 – Common (1/yr to 10/yr)	R	B	B	A	A	A
F3 – Likely (0.1/yr to 1/yr)	R	C	B	A	A	A
F4 – Rare (0.01/yr to 0.1/yr)	R	C	C	B	A	A
F5 – Unlikely (10^{-3}/yr to 0.01/yr)	R	D	C	C	B	A
F6 – Improbable (10^{-4}/yr to 10^{-3}/yr)	R	D	D	C	C	B
F7 – Incredible (<10^{-4}/yr)	R	D	D	D	C	C

Risk Class	Description
A	**High Risk** – Risk control measures should be implemented to mitigate the risk to a level that is ALARP with a top priority.
B	**Medium Risk** – Cost-effective risk control measures should be implemented to mitigate the risk to a level that is ALARP within a reasonable time.
C	**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	**Negligible Risk** – 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



Risk Matrix Should Actually be Designed by Quantitative Input



		0	0.001	0.01	0.1	1	10	20
		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
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

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

$$B/C_i = \frac{Risk_{i,baseline} - Risk_{i,improved}}{cost_i}$$

where:

i	= i^{th} *decision alternative*
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*

www.hkarms.org

落實風險管理
共創安全明天

END

HKARMS