System Safety Assurance

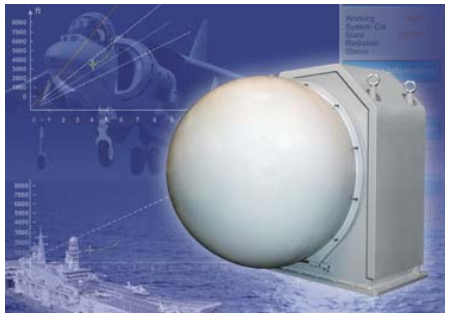
How Much Assurance is Enough ?

Steve Drabble

Systems & Software
Technology Conference 2009

QinetiQ

Presentation Contents



QinetiQ

01 Introduction

Safety Engineering Effort/Costs Difficult To Predict

Estimates Range from 1-15%

Some Domains maybe higher – Nuclear

Anecdotal evidence suggests a Norm of 12%

Complex systems cost more to develop ?

Safety Effort *'Silent'* – Successful Outcome – No Accidents

Leading to downward pressure on Safety Budget

Business *Risks* Over/Under Allocation of Resources

Significant investment in Safety Resources – How do we know that makes good business sense ?

02 Whats The ***True*** Cost Of Safety Engineering ?

- US DoD Estimated Safety Losses $10 - $20 Billion Per Year (2008)
- Piper Alpha Losses Estimated Over £2 Billion
- BP Texas City Oil Refinery Explosion - $1.6 Billion Victim Compensation
- Buncefield Oil Depot Explosion – Estimated £1 Billion

03 Key Lessons From Major Accidents

BP Grangemouth Report

- Weakness in adopting right measures
- Share experiences – Web Site Communities
- Key Lesson(s) *'Ensure Safety Performance is monitored and Reported'*

BP Buncefield

- Implementation process safety indicators

BP Texas City – Baker Report

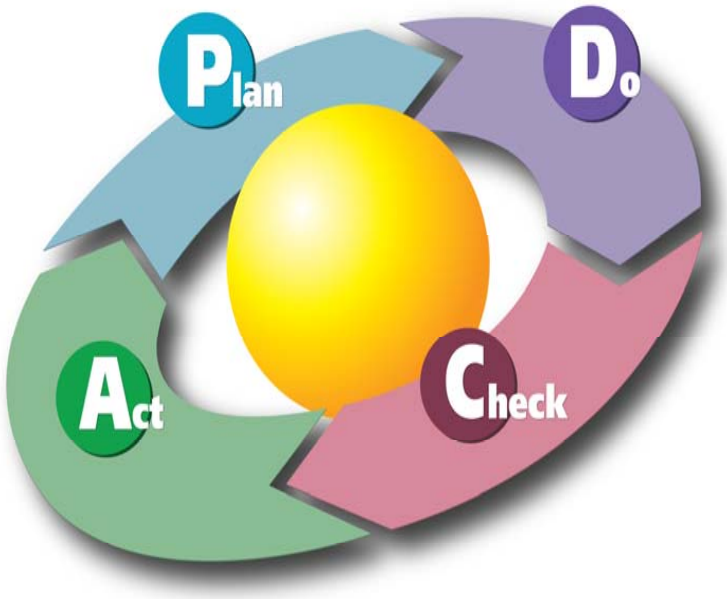
- Occupational Safety vs Process Safety
- Poor Safety Culture

03 Key Lessons From Major Accidents

Safety Measurement Can Be Used To

- Set safety performance targets/objectives
- Assess safety performance
- Set goals for improvements
- Anticipate potential deviation
- Apply corrective action

= Plan Do Check Act Management Process



Caution

- Don't set targets because we ***can***
- Don't set objectives that ***can't be measured***
- We need to ensure we measure the ***right things***

04 Who Is At Risk ?

System/Plant Developer – ROI

- Accurate estimates of safety engineering effort
- Cost effective use of resources
- Reduced exposure to business risks

Acquisition organisation –

- Inaccurate estimates will increase the risk of a late, over budget, limited capability system – *'Fit for Purpose ?'*

Operator & Maintainer

- Site/Plant Visitors
- Local Community
- Emergency Services
- Wider Community

05 Why Measure ?

- Helps prevent accidents – Learning From Experience
- Reduced exposure to business risks during development
- Reduced acquisition risks

Measurement Provides Business Information – Aids Decision Making

Good Business Sense – Identification/Management (Safety) Risks.

‘*You cannot control what you cannot measure.’ Tom Demarco*

05 Why Measure ?

Over Allocation Of Safety Resources

- Over engineered System
- Increased Bid Costs ?
- Assumed Sufficient Safety Resources to Meet Project Commitments
- *Pressures on Profit Margins/System Schedule*

05 Why Measure ?

Under Allocation Of Safety Resources

- Completion All Safety Activities – Challenging
- Late Safety Evidence – Inability to Influence System Design
- Lack of Safety Evidence – Implications for Certification
- Schedule Delays
- Contractual Penalties
- Company Reputation ?

06 What Are The Measurement Challenges ?

Safety Effort = Project Costs (£/$) V Benefits ?

- Safety Effort *'Silent'* – Successful Outcome – No Accidents
- How Do You Measure The Absence of Something ?
- If You Don't Measure Safety Effort:-
  - How Do You Defend Safety Budget Cuts ?
  - How Do You Identify Resources, Costs, Schedule To Meet Project Commitments ?

06 What Are The Measurement Challenges ?

Influence of Domain Safety Standards

- Safety Critical Systems – Certification Requirements
- Operator Provides Evidence – *'System is Safe'*
- Domain Safety Standards Influence Safety Engineering Activities
- Domain Safety Standards Are Either:-
  - Prescriptive – Mandate Method & Technique
  - Evidence/Goal Based – *'What'* not *'How'*
- *Domain Safety Standards Do Not Mandate Safety Process Measurement*

06 What Are The Measurement Challenges ?

Influence of Domain Safety Standards

- **Prescriptive** Domain Safety Standards :-
  - Majority Safety Standards Prescriptive
  - ***Mandate Method & Technique (M&T)***
  - Some allow alternative Methods & Techniques
  - Use of alternatives M&T to Show Compliance Unclear
  - Use of alternative M&T – Certification Risk ?
  - Little evidence of use of alternative (M&T)

06 What Are The Measurement Challenges ?

Influence of Domain Safety Standards

- Evidence/Goal Based Domain Safety Standards
  - *'What'* not *'How'*
  - Freedom to select M&T
  - However - Developers using 'Tried & Tested' M&T
  - *Why ?*
    - *How to* Satisfy certification requirements
    - Lack of guidance and interpretation of standard
    - Can use prescriptive M&T
    - Departing from the '*accepted norm is risky*'
    - Safety practitioners skilled & experienced in use of existing M&T

06 What Are The Measurement Challenges ?

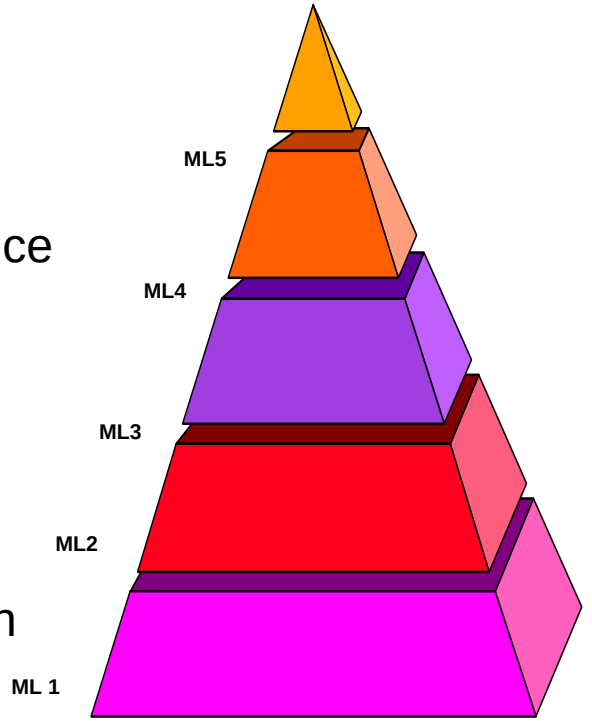
Additional '*Measurement*' Resources

- Extra Resources = More Cost £/$ - *Whats the ROI ?*
- Project Budget Implications ?
- Measurement Framework – '*What, When, Who, How*'
- Data Collection and Analysis – *Who*
- Any New Risks Introduced ?

06 What Are The Measurement Challenges ?

Lack Of Measurement Models

- Why Measurement Models ?
  - Background – Poor Track Record
  - 1984 SEI Established To Address Poor Performance
  - 1991 SEI Produced CMM – Used To Benchmark
  - CMM Objective
    - Common Framework & Vocabulary
    - Measure Performance against ‘Best Practice’
    - Identify Process Weaknesses - Corrective Action Plans
    - *Focus on Process Areas Critical To Business Success – Improve Performance and Effectiveness*



06 What Are The Measurement Challenges ?

Lack Of Measurement Models

- *+SAFE*
  - CMMI Generic Framework - Does Not Address Safety
  - Australian DMO Produced +SAFE – Extension CMMI
    - Two +SAFE Process Areas that Address Safety
      - Safety Management & Safety Engineering

06 What Are The Measurement Challenges ?

Lack Of Measurement Models

- *Practical Software & Systems Measurement (PSM)*
  - Safety Measurement White Paper – Jan 2006
  - Applies PSM ISO/IEC 15939 Measurement Framework
  - Measurement Process Model Based on *Information Needs* and *Measurable* Entities/Attributes
  - Draft Guidelines for PSM Safety Measurement
  - Proposals Not Yet Validated Through Field Trials

07 What To Measure ?

Competencies

'the ability to perform activities to the standards required in employment using an appropriate mix of knowledge, skill and attitude' IET

Not just Qualifications

- *Domain Knowledge, Awareness Of Legislation, Effective Application Of Safety Technique/Method, Good Communication Skills, Appropriate Behaviour & Attitude*

Suitably Qualified and Experienced Personnel (SQEP) HSE

07 What To Measure ?

Safety Culture (ACSNI)

'The safety culture of an organisation is the product of individual and group values, attitudes, perceptions, competencies, and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organisation's health and safety management.

Organisations with a positive safety culture are characterised by communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of preventive measures.'

Safety Culture (CBI)

'The way we do things around here'

07 What To Measure ?

Safety Culture

- Safety Culture Questionnaire
- Staff Interviews
- Safety Culture Maturity Model
- Offshore Technology, Aviation and Railway sectors

07 What To Measure ?

Safety

Culture ?

07 What To Measure ?

Safety Engineering

- Wide Range of Available Safety Techniques/Methods
- Small Number Techniques/Methods *In Use*
- Any Empirical Effort/Costs Information Available ?
  - Best Practice
  - Bench Marking
  - Safety Technique/Method Selection
  - Automated Safety Analysis
  - Learn From Experience – Process Improvement

07 What To Measure ?

Safety Engineering

- Lack Of Empirical Effort/Costs Information
  - Empirical Data Not Collected
  - Empirical Data Available – Not Analysed/Used
  - Commercially Sensitive Information
- *Observations:-*
  - *No Widespread Measurement of Safety Effort/Costs*
  - *No Compelling Case For Safety Measurement – No Information Need*
  - *No Motivation To Share Experiences*

08 Conclusions – Part 1

Why Measure ? – Makes Good Business Sense

Why Measure ? – Identify/Manage (Safety) Risks

Why Measure ? – Cost Effective Utilisation of Resources

Why Measure ? – Information Supports Business Decisions

Measurement Challenges ? - ROI for Measurement Framework

Measurement Challenges ? - No Common Measurement Model

Measurement Challenges ? - Influence Of Domain Safety Standard

What To Measure ? – Competencies, Culture, Safety Engineering

Collection & Sharing of Empirical Data Will Help With Benchmarking

08 Conclusions – Part 2

Cost of Getting it Wrong- £/$ Billions, Harm, Environmental Damage

Influence of Safety Standards – Impede Cost Effective Safety Analysis

Who Is Measuring Safety Performance – Limited Evidence

Cost of High Assurance – No Empirical Evidence

How Do We Measure Safety Engineering Effort – Historical

Who is Measuring Safety Engineering Effort – No Empirical Evidence

Why Bother Measuring Safety Engineering – Reduced Business Risk by Identifying & Mitigating System Risks

Questions ?

QinetiQ

System Safety Assurance

How Much Assurance is Enough ?

QinetiQ

The Global Defence and Security Experts