

A learning model for organisational improvement based on incident investigation and analysis - PARCEL

Luke Emmet & Prof. Peter Bishop

Adelard

loe@adelard.com, pgb@adelard.com

<http://www.adelard.com>

Overview of talk

- ◆ Acknowledgements, background and motivation
- ◆ Summary of industry consultation
- ◆ Overview of scheme design and scheme components
- ◆ Customisation and application issues

Adelard – who we are

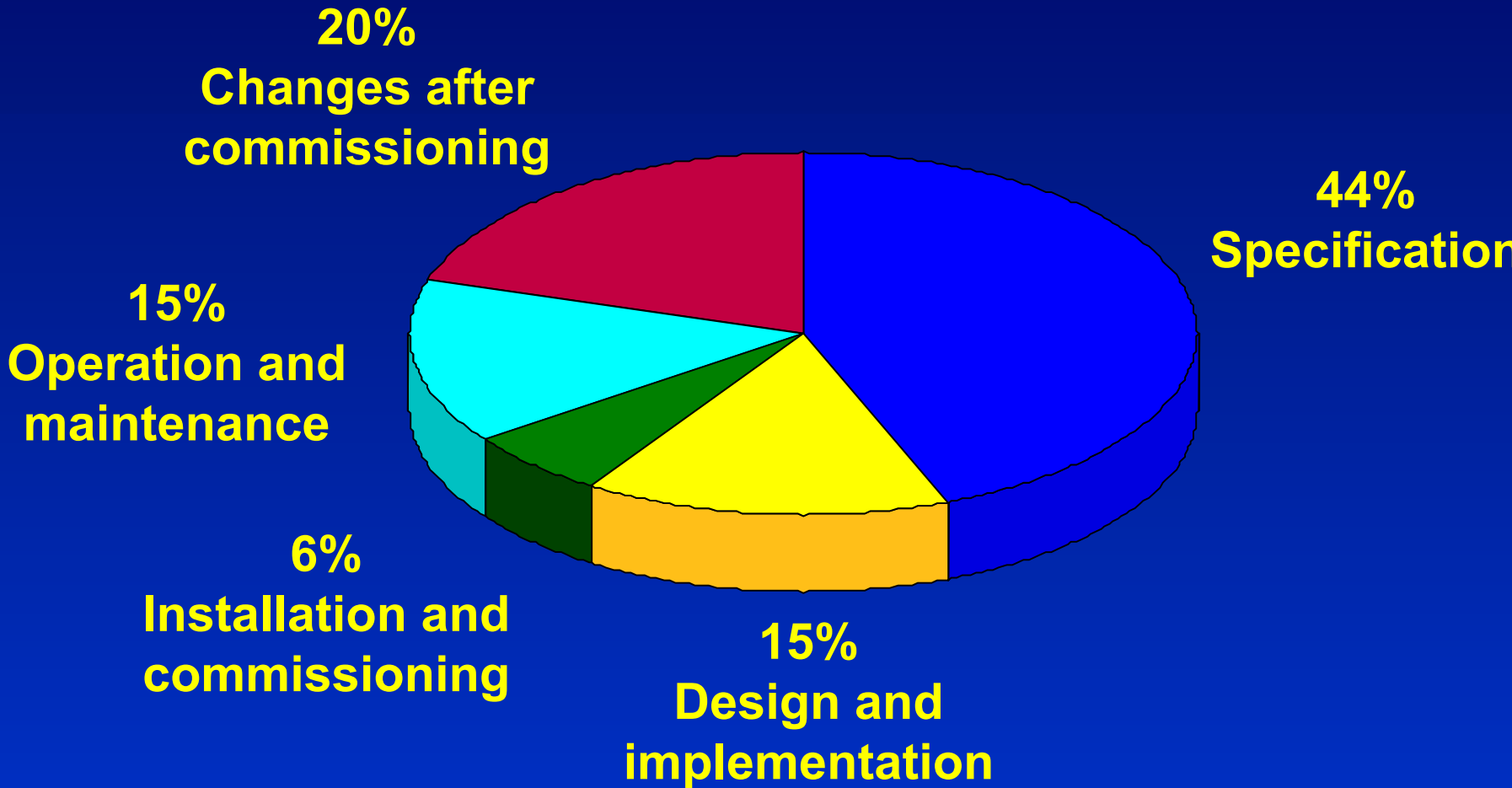
- ◆ Small specialist consultancy based in UK
- ◆ Particular strengths in safety related computer systems
- ◆ Work on a wide range of strategic safety policy and research projects
 - Standards policy formulation, including standards writing and interpretation
 - Safety Analysis and Independent Assessment
 - Safety Case production and assessment
 - The Adelard Safety Case Editor – including GSN, WBA, C-A-E
 - Software analysis - including static analysis
 - Software development
 - Human Factors and organisational aspects of safety management

Background publication: “Out of control”

- ◆ Published by UK Health and Safety Executive (HSE) in 1995
- ◆ 34 incidents involving control systems
- ◆ Chemical/petroleum plant and machinery
- ◆ Incidents characterized by originating **lifecycle phase**
- ◆ *Widely seen as a useful publication*

Out of control: Why control systems go wrong and how to prevent failure, HSE Books, ISBN 0-7176-0847-6

Out of control



The project

- ◆ Research best practice in learning from incidents
- ◆ Develop examples schemes to aid adoption
- ◆ Focus on IEC61508 aspects (i.e. E/E/PES related)
- ◆ Support HSE in the development of guidance to industry

- ◆ Way forward for HSE:
 - Publish HSE guidance: “How to learn from your incidents”
 - Create data in line with classification scheme as incidents occur
 - HSE may add value by publishing anonymised incident data and analysis results in an updated “Out of Control”

The project team

◆ Consortium led by Adelard

- Also including:

- GAAG Chris Johnson

- Blacksafe Bill Black

- Contributions from:

- TU Delft Floor Koornneef

- Viv Hamilton Associates

Project overview – core tasks

- ◆ Survey of existing methods
- ◆ Industry consultation
- ◆ Scheme development
- ◆ Scheme concepts and learning model
- ◆ Scheme customisation and application
- ◆ Reports on some experience on use and application of the draft scheme

Core motivation for the project

- ◆ IEC 61508 on the functional safety of E/E/PES requires:
 - 6.2.1. procedures which ensure that hazardous incidents (or incidents with potential to create hazards) are analysed, and that recommendations are made to minimise the probability of a repeat occurrence".
- ◆ And:
 - 7.8.2.2 Manufacturers or system suppliers which claim compliance with all or part of this standard shall maintain a system to initiate changes as a result of defects being detected in hardware or software and to inform users of the need for modification in the event of the defect affecting safety.

Management of Health and Safety at Work Regulations 1999 Approved Code of Practice

Monitoring includes:

(b) Adequately investigating the immediate and underlying causes of incidents and accidents to ensure that remedial action is taken, lessons are learnt and longer term objectives are introduced.

It may be appropriate to record and analyse the results of monitoring activity, to identify any underlying themes or trends which may not be apparent from looking at events in isolation.

Management of Health and Safety at Work Regulations 1999

(1) Every employer shall make and give effect to such arrangements as are appropriate, having regard to the nature of his activities and the size of his undertaking, for the effective planning, organisation, control, monitoring and review of the preventative and protective measures.

Regulation 5

Control of Major Accident Hazards Regulations 1999

Procedures should cover the operator's system for reporting major accidents or near misses, particularly those involving failure of protective measures, and their investigation and follow-up on the basis of lessons learnt.

Schedule 2 (4) (f)

Industry Consultation

◆ Main sectors for HSE

- Process, Offshore, Machinery, Nuclear, Rail

◆ Other sectors for comparison

- Marine, Medical, Aviation

◆ E/E/PES Supply chain

- systems designers/suppliers
- product suppliers

◆ Roles

- Procurers, System Suppliers, Users, Maintainers, Assessors/ licensors/ regulators, Standards/ guidance developers , Incident investigation consultant/academics

Analysis of Interviews (and experience)

- ◆ Sector and role
- ◆ Incident reporting
- ◆ Incident investigation
- ◆ Handling of E/E/PES
- ◆ Learning
- ◆ Dissemination

Actual Scheme (medical end user)

- ◆ Incident reporting
 - Simple capture form (reporter name, date, free text)
- ◆ Incident analysis
 - No further analysis if incident is known and frequency acceptable
 - Local incident review group (who know the context)
 - Incident analysis could include further data gathering from the reporter
 - Analysis using Event Causal Factor (ECF) chart
- ◆ Lessons learned
 - Modify process: up stream prevention, local-downstream mitigation
 - Modify/replace equipment (higher management decision)
- ◆ Dissemination
 - Regular staff briefing
 - Protocol changes

Actual Scheme (System Designer)

◆ Incident reporting

- End user phones or emails company
- Incident recorded on standard customer feedback form (but with a hazard classification) mainly *free text description*
- Resolution of incident tracked as part of standard QA system
- Reporting to Director for serious incidents

◆ Incident Analysis

- Performed by Chartered Engineer (no specific analysis method)
- Fast response for safety related incidents (next day)
- Follow-up of incident (maybe with site visit)
- Identification of cause (system design, component problem, inadequate user information, personnel competence)

Actual Scheme (System Designer - cont)

◆ Problem resolution

- Site modification / replacement
- User hazard notification (if user was negligent)
- Component failure covered by issuing a non-compliance notification NCN to supplier (tracked in the QA system)

◆ Feedback of lessons

- Changes to portfolio of standard designs
- Changes to equipment configuration guidelines
- Changes of supplier and/or component
- Changes to engineer training (maybe also disciplinary action)
- Changes checklists (testing, commissioning, documentation)
- Regular review of customer feedback, component supplier alerts, info

Actual Scheme (System Designer - cont)

◆ Dissemination

- Intranet holding incident reports, standard designs, configuration guides, bulletin boards, hints and tips
- email to alert engineers about problems
- Access to Product supplier via Internet (updates of documentation, software, configuration information)
- Email to notify supplier and users of problems

Actual Scheme (PES supplier)

◆ Reporting

- Notification via email, phone, mail
- Entered in customer feedback form

◆ Analysis

- Assessment of problem
- Assignment to relevant department (design, documentation, etc)

◆ Corrective Action

- Special procedures for IEC 61508
- Could result in engineering change request, doc./ guidance change
- Impact analysis (other products with common hardware/sw parts?)
- User alerts (all affected users, based on eqt serial numbers)

Actual Scheme (PES supplier - cont)

◆ Learning

- Reviews / trend analysis of problem report database
- Updates to development process and procedures

◆ Dissemination

- Intranet access to problem reports
- Email for reporting and alerting
- Internet and document material, product specs and manuals, application guides, etc.

Task 1. Conclusions - Methods

- ◆ A range of methods are available for incident reporting analysis reporting and dissemination
- ◆ Single method probably not appropriate for such a broad spectrum of industries
- ◆ Need to have appropriate guidance for selection of appropriate methods, e.g. depending on:
 - Maturity
 - Organisational complexity

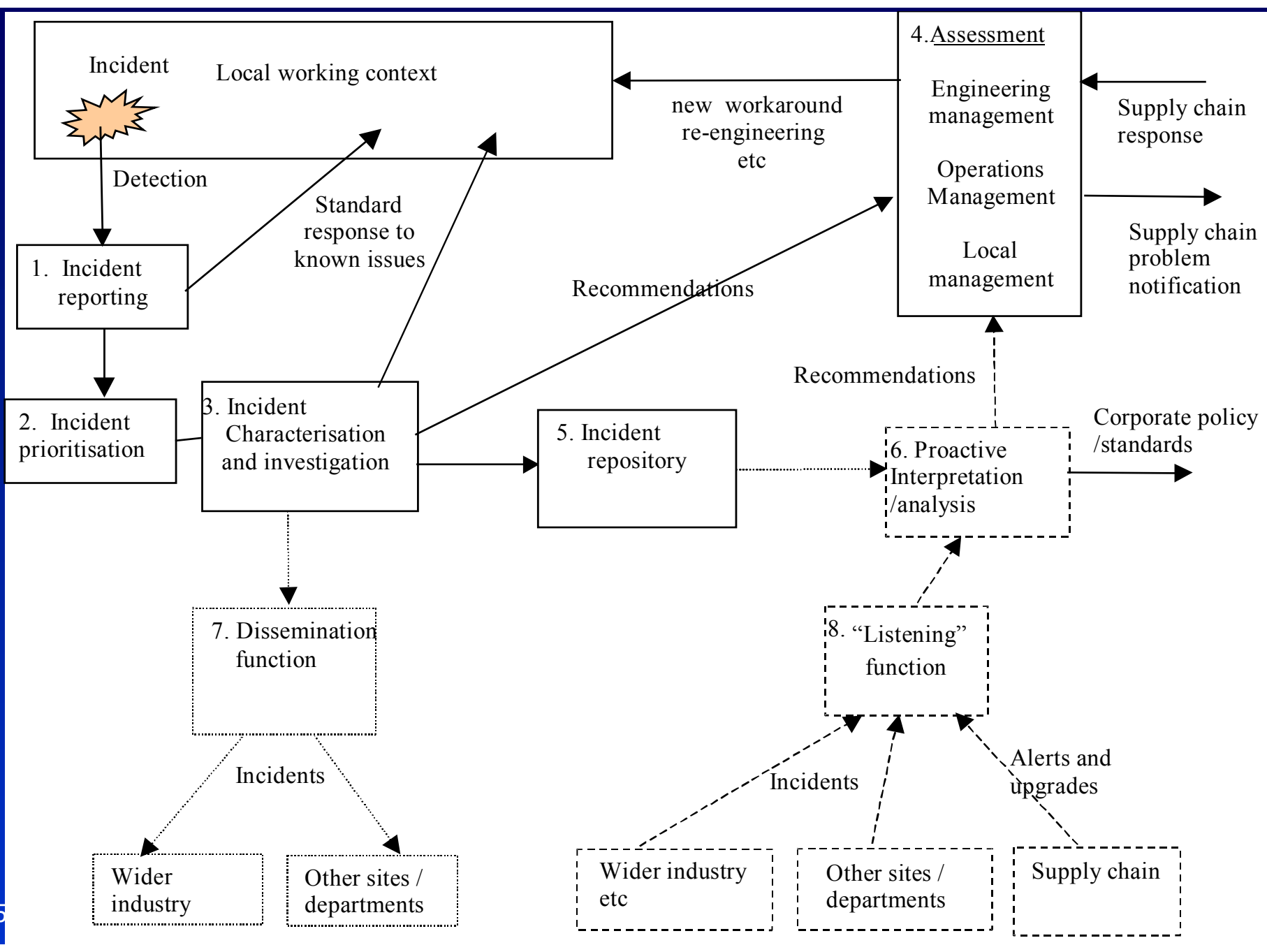
Task 1. Conclusions - Industry practice

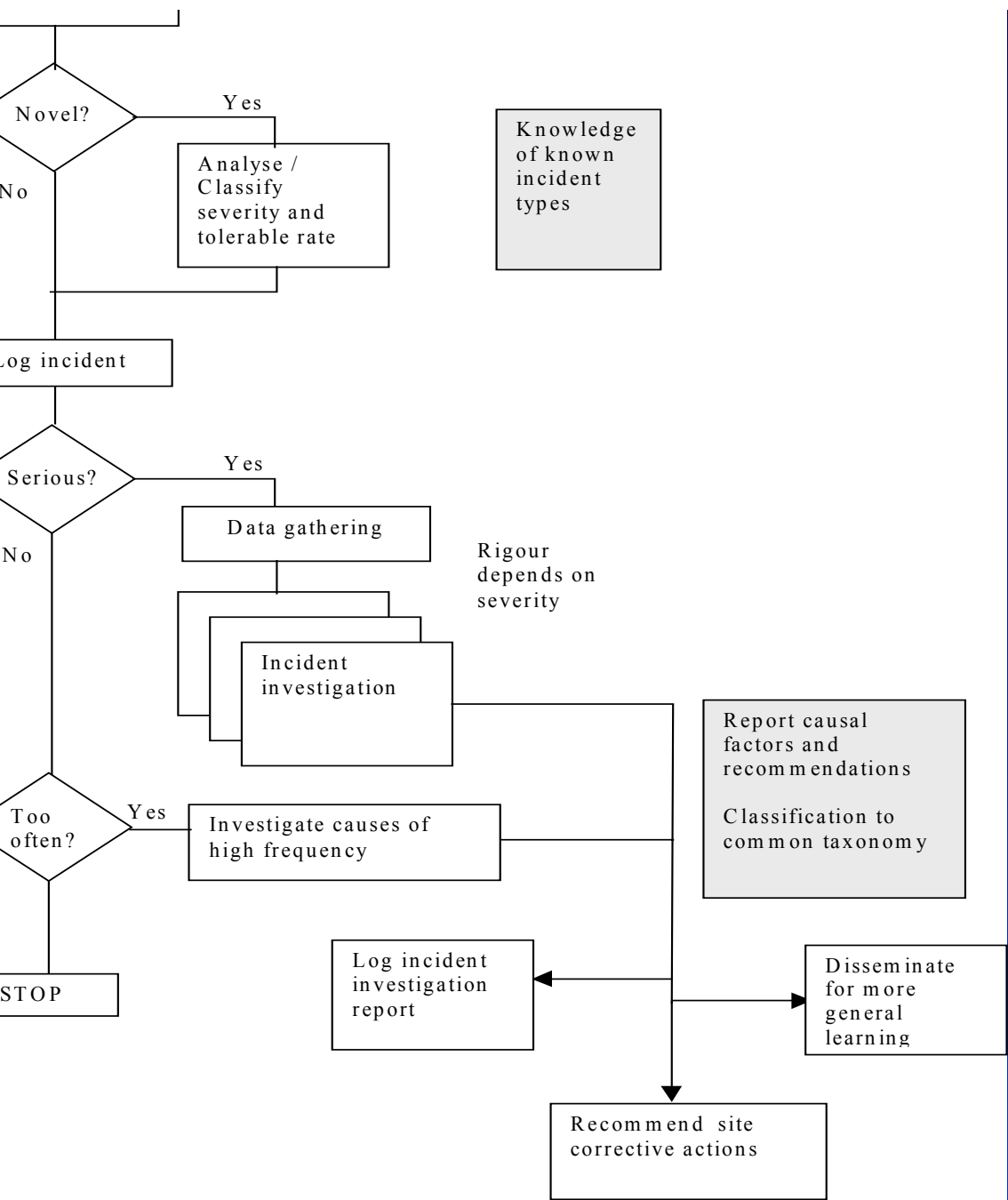
- ◆ The best companies have well established schemes
 - Not practical to change
 - Only modify where needed
- ◆ If no existing scheme, then:
 - important to allow gradual adoption
 - needs to be commensurate with complexity of the organisation
- ◆ Some user organisations think there are few E/E/PES problems (but could be unrecognised/unreported)
- ◆ Long-term learning can be aided by:
 - use of simple tools such email list, bulletin boards, "tips".
 - softer aspects (briefings, anecdotes)

Task 2. Scheme design

- ◆ Generic process model as basis for scheme
 - Organisations can line up in-house process against overall model
 - Look for missing components and interactions
- ◆ E/E/PES components seen pragmatically as a specialist Add-On
 - To ease adoption in organisations where aspects of the process already exist
 - To give detailed guidance on E/E/PES aspects
- ◆ Need flexibility in adapting to different scales and maturities
 - Roles can be mapped on to different people/organisations
 - Or one person can undertake several roles
 - Different levels of documentation and detail

PARCEL – PES Analysis of Root Cause and Experience based Learning



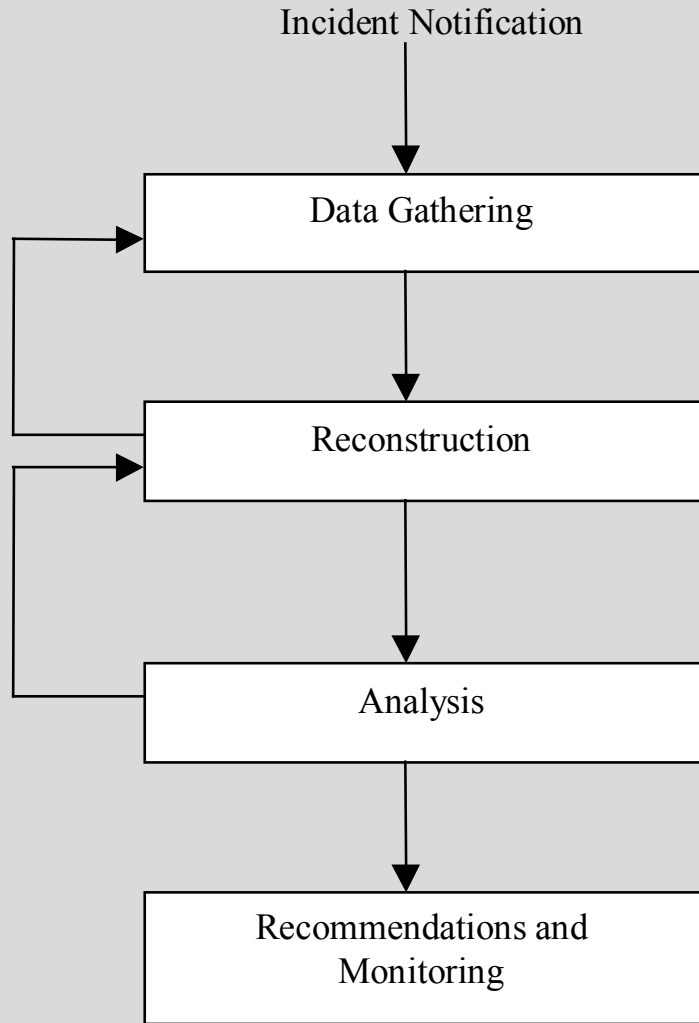


Incident handling decision process

Guidance provided on

- ◆ Incident reporting
- ◆ Factors affecting investigation policy - e.g. what determines high priority:
 - High impact – number of fatalities
 - High frequency of incident type
 - Incident is novel or unexpected
 - Number of installations in use
- ◆ Proactive “listening” functions
- ◆ Problem identification
- ◆ E/E/PES specialisations to general model
- ◆ Customisation and adaptation

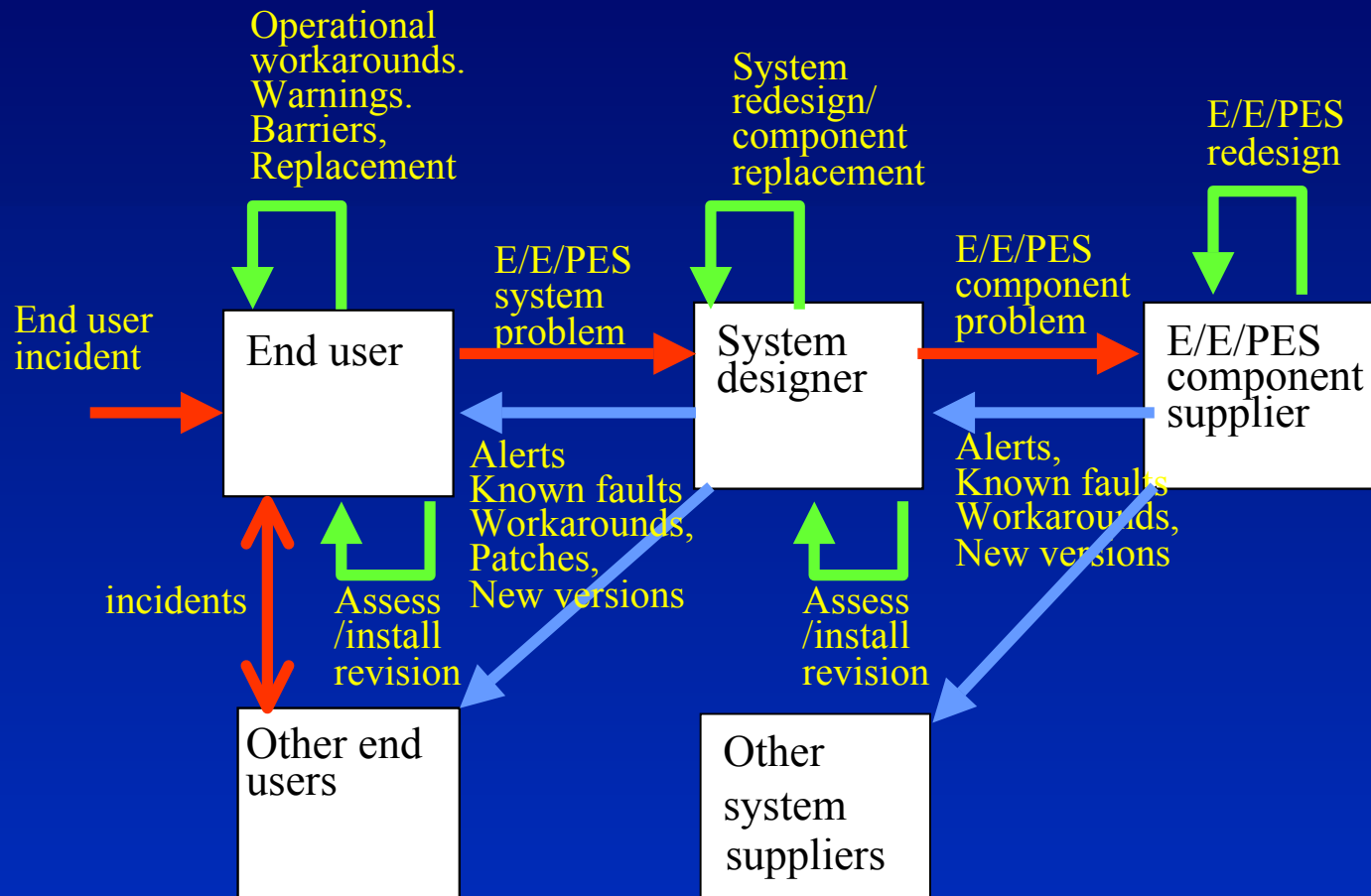
Incident investigation



Incident reconstruction

- ◆ Where incident considered suitably interesting to warrant detailed investigation, specialist reconstruction techniques can be applied:
 - Ranging from the simple:
 - Timeline reconstruction, standard narrative
 - Through to the more sophisticated:
 - WB Graphs, Events and Causal Factors charts (ECF), STAMP, SOL etc.
- ◆ PARC (PES Analysis of Root Cause) method developed as a simple method to determine the cause of a problem
 - Based on PRISMA method
 - Focused on IEC 61508 view of the world – Safety Lifecycle
 - Initially paper based – but implemented as a hypertext

Reporting through the supply chain



◆ Other feedbacks - standards, regulator, etc

Recommendations

- ◆ Incident causes can suggest recommendations:
 - Equipment
 - People
 - Environment
 - Interfaces between the above
- ◆ Also lifecycle stages: what could be done differently next time?
 - Process improvement within safety lifecycle
 - Common processes – Competency, Lifecycle, Verification, Safety management, Documentation, Safety assessment
- ◆ Tracking and implementation usually via Safety Management System or Quality Management System

Classification

- ◆ What is the purpose of classification?
- ◆ User level
 - To recognise failure condition and implement corrective action
 - To exchange relevant experience with other users
 - To support analysis (identify trends, set policy, priorities)
 - To assess effectiveness of process changes
- ◆ Systems designer
 - To classify *causes* of failure
 - To support analysis (trends, principal causes) for policy, priorities
 - To assess effectiveness of process/training/design changes
- ◆ Regulator level
 - To facilitate data aggregation and analyse industry trends

Purposes of Taxonomy as such

- ◆ Provide a common representation for Incident representation and characterisation
- ◆ A tool to aid mechanical retrieval
- ◆ A tool to support common characterisation
- ◆ Enable retrieval from corporate memory
 - Have we had incidents “like” this one
- ◆ Provide a characterisation of the analysis of root causes
 - Have we had incidents caused in a “similar way”
 - Where are the organisational responsibilities
 - technical design, procedures, training, management etc

Dangers of classification

- ◆ can impose a particular world view
- ◆ lack of domain-awareness
 - has to be tailored
- ◆ sometimes hard for end user to relate to (especially in incident reporting)
- ◆ data collection should be purposeful
 - users need to see what is the learning opportunity
- ◆ taxonomists always disagree!

Classification implemented

- ◆ Classify in relation to stages in the IEC 61508 lifecycle to aid process improvement
- ◆ Example classifications
 - Initial problem prevention checklist – end user organisation response
 - overall concept, procurement, selection of suppliers,...
 - Equipment supplier
 - has more of design phases

Scheme Implementation

General Structure

- ◆ Roles within scheme
- ◆ Activities for each role
- ◆ Information required for each role
- ◆ Information generated by each role

Tailoring

- ◆ Mapping roles on to existing personnel
- ◆ Mapping information into current recording structure
- ◆ Identification of relevant feedback mechanisms within organisation and to external organisations

Application experience and industry feedback

Main results (1)

◆ LFI and supply chain processes

- broadly recognised and generally implemented by higher maturity organisations
 - some aspects merged, others even more complex (e.g. supply chain)
- wide variation in how enacted, but implemented on the whole by simple technologies and quality infrastructure
- any new E/E/PES aspects would generally have to fit in to existing processes

Main results (2)

- ◆ Flow chart method - PARC
 - broadly usable given basic competencies
 - could be done using a checklist
- ◆ Analysis categories and terminology
 - can be applied, but needs tailoring and customisation
 - good coverage of issues from 61508 perspective
- ◆ Recommendations by reviewers and evaluators
 - some additions, but mostly simplifications were suggested

Customisation and application

Customisation

- ◆ Three dimensions of customisation required
 - Maturity
 - Application domain
 - Organisational role (end user, system supplier etc)
- ◆ Two components to customise
 - Scheme
 - terms, classification categories and depth
 - methods (data collection, causal analysis etc)
 - data to be collected
 - Processes
 - components of the learning model vs maturity
 - roles and tasks
 - supporting technologies

Maturity levels

Several models (CMM, SPICE), but basically can map to learning model.

1. Undefined - reactive, ad hoc
2. Some basic information (RIDDOR, recording)
3. Defined processes (ISO 9000, IEC 61508)
4. Adaptive
5. Optimising

BUT, LFI requires adaptation/optimising via learning even at lower maturity levels (just more limited response - local workplace etc).

Reflected in 2000 version of ISO 9000

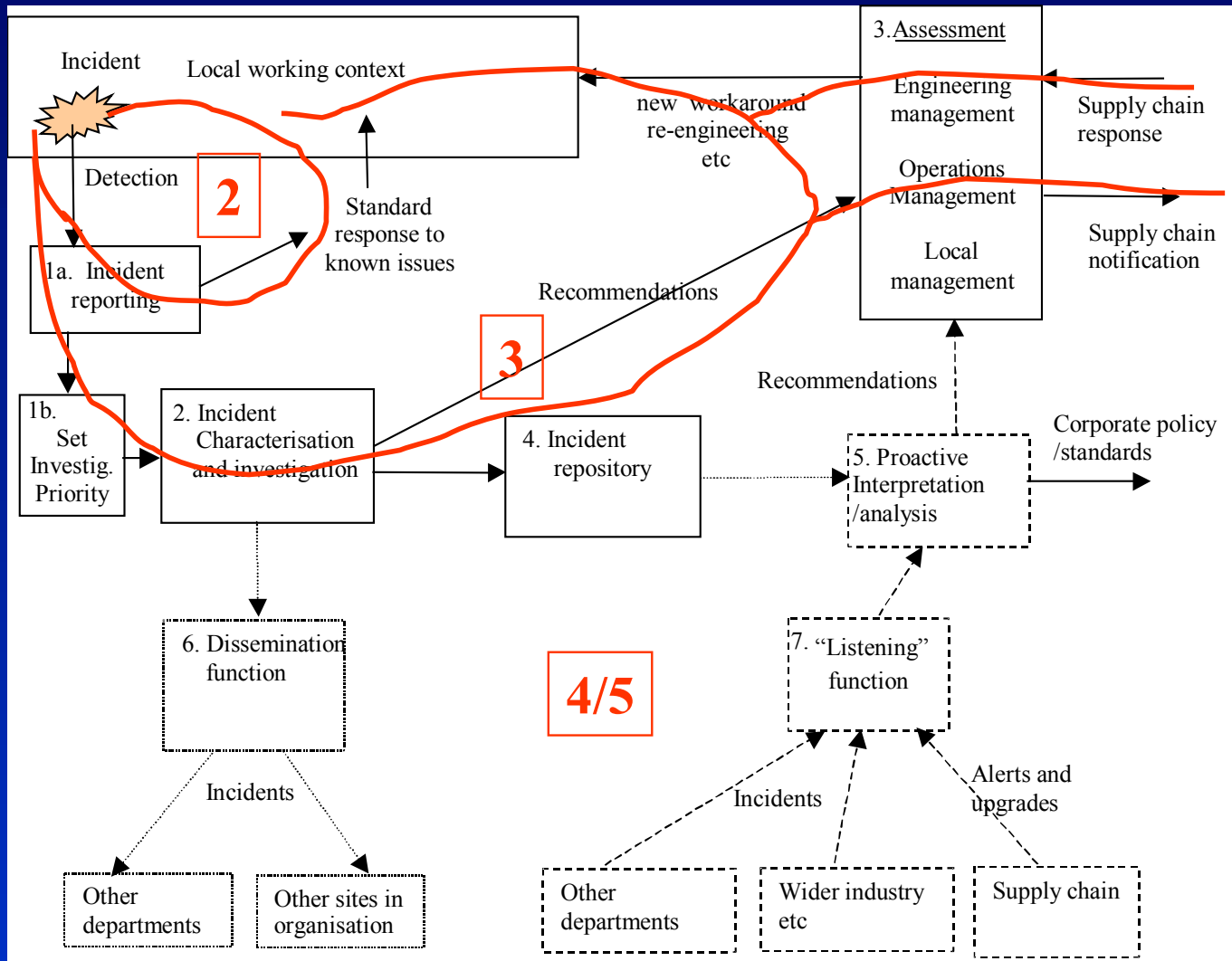
Need to maximise gain for pain

Operational capability	Learning capability		
	A. Low	B. Medium	C. High
<i>Quality infrastructure</i>			
What kind of quality system is in operation	<input type="checkbox"/> A basic management and review system only	<input type="checkbox"/> A company-specific or certified quality system in use (e.g. ISO 9000)	<input type="checkbox"/> An certified quality system in use (e.g. ISO 9000)
What is the mechanism for improving processes?	<input type="checkbox"/> Ad hoc – mostly personal experiences and anecdotes.	<input type="checkbox"/> Analysis of reported problems.	<input type="checkbox"/> Periodic review of incidents. Design and operation standards regularly reviewed
<i>Incident reporting</i>			
Is there an incident reporting system in operation?	<input type="checkbox"/> Only serious incidents are logged. RIDDOR-notifiable reports sent.	<input type="checkbox"/> Yes, although may be primarily focused on operation activities.	<input type="checkbox"/> Comprehensive incident reporting
Is incident reporting part of the operational infrastructure?	<input type="checkbox"/> No	<input type="checkbox"/> Staff assigned incident reporting and analysis responsibilities	<input type="checkbox"/> Reporting and analysis
Is incident reporting easy and accessible?	<input type="checkbox"/> n/a	<input type="checkbox"/> Paper forms to be filled in. Incident reports logged and filed.	<input type="checkbox"/> Yes – easily accessible via internal IT systems
<i>Incident investigation analysis</i>			
Are there stated criteria for incident investigation?	<input type="checkbox"/> Serious incidents may be examined at management request	<input type="checkbox"/> Criteria for some incident types	<input type="checkbox"/> Criteria for all incidents (and these criteria are effectively applied)
Does the organisation conduct specialist technical investigations as part of incident investigation?	<input type="checkbox"/> No	<input type="checkbox"/> Sometimes (when complex technical issues identified)	<input type="checkbox"/> Routinely when technical issues are identified
Does the organisation participate in wider learning with industry (forums, interest groups, seminars)?	<input type="checkbox"/> Not really	<input type="checkbox"/> Some	<input type="checkbox"/> Good participation in industry forums and experience sharing networks.

Current “learning capability” - self assessment

Learning lifecycle

1



Customisation: Getting started

- ◆ Capability assessment
- ◆ Worked examples at different maturity levels
- ◆ Sample processes and forms for lower maturity organisations
- ◆ Guidance on
 - Identifying purpose of reporting and analysis (what can be improved/changed?)
 - Fitting into existing processes
 - Exploiting existing quality infrastructure (ISO 9000, etc)
 - Exploiting existing technical infrastructure
 - Identifying stakeholders, roles and tasks
- ◆ Guidance on evolution (in line with maturity)

Customisation: Add on

- ◆ Identifying existing incident handling processes
- ◆ Modification of existing processes to cover E/E/PES problems
 - minimal modifications
 - additions to checklists only when PES identified
 - resources for special investigations
- ◆ Ensuring adequate information along the supply chain
 - incident and application context
- ◆ Listening and proactive functions

Accompanying Software

- ◆ We developed prototype web software over course of project which illustrated:
 - reporting forms
 - notification as status changed
 - audit trail
- ◆ But active package would need considerable expertise to install and customise
- ◆ So we delivered static “snapshot” (i.e. non -active example pages)
 - Exists standalone
 - Easily shared
 - Demonstrate ideas only
- ◆ Flow chart software of PARC method
 - Developed with Adelard notation tool ASCE

Conclusions

- ◆ Approach seems feasible, provided organisations adapt scheme to their needs
- ◆ Need to see clear benefits and purpose to ensure uptake and buy-in
- ◆ Need to minimise disruption and cost in adoption of scheme
 - evolutionary adoption process in line with maturity
 - E/E/PES aspect typically an add-on to existing process
- ◆ Need to benefit from learning activities in lower maturity processes

- ◆ Guidance should be made available shortly as HSE technical reports

Thank you