CRANFIELD UNIVERSITY

Rhydian Harries

SAFETY CASES AND SAFETY CULTURE

A SAFETY CASE ELICITATION TOOL FOR LIGHT UNMANNED AIR VEHICLES

DEPARTMENT OF APPLIED SCIENCE, SECURITY AND RESILIENCE

Faculty of Defence & Security

EngD THESIS

This page left intentionally blank.

CRANFIELD UNIVERSITY

DEFENCE COLLEGE OF MANAGEMENT AND TECHNOLOGY

Faculty of Defence & Security

EngD THESIS

Academic Period 2006-2010

Mr Rhydian Harries

SAFETY CASES AND SAFETY CULTURE

A SAFETY CASE ELICITATION TOOL FOR LIGHT UNMANNED AIR VEHICLES

Thesis Committee: Prof. P. John, Prof. R. Ormondroyd, Dr M. Williams (Management)

Supervisor: Dr M.R. Edwards

December 2009

This page left intentionally blank.

ABSTRACT

The intention of this thesis is to define a guideline for the creation of a safety case for use in the field of civil light UAVs. It provides stakeholders with an opportunity to understand how the UAV, as a complete system, has been designed, assembled and will be operated in a safe and competent manner. Not only can it be used to create a safety argument to prove an extant system's integrity, it can be used to identify weaknesses within a new system to allow further energy to be focussed upon the delinquent areas.

The need for this approach is linked heavily to the UK's civil UAV market and the vast growth which is forecasted to occur within it over the next two decades. The requirement is also driven by the extant minimal level of regulatory guidance available from within the UK's CAA.

The final guideline also applies a more qualitative approach to safety and encompasses those elements of a system which have been predominantly excluded from the majority of safety arguments. By combining a traditional 'hard' safety engineering approach, with a more qualitative and 'people' focussed approach, an enhanced safety argument is created which applies the fundamentals of today's *Systems Engineering* regime.

It should be noted that this revised approach to assembling a safety case for light UAVs does not tackle the most demanding of current UAV challenges which is that of 'sense and avoid'. The aim of this revised form of safety case is to facilitate a more complete body of evidence so that safety engineers, safety managers (or regulators) may make a more accurate, relevant, and consolidated safety assessment of the system under scrutiny. Any decisions at national, or international level, which relates to the 'sense and avoid' issue, may be decomposed and included in further iterations of this guideline.

This page left intentionally blank.

ACKNOWLEDGEMENTS

This study at doctoral level has certainly been a journey of self discovery. From a personal sense it has driven me through massive highs and lows, predominantly due to the pressures of juggling a demanding full time job in an ever changing business environment with that of research and study, predominantly within my own personal time. Without the following people the journey would have been much more painful and for that I thank them.

I thank QinetiQ for allowing me the time to attend the taught components of the course. Of particular note was the initial support offered by Bob Burrows and Mark Pengilley by agreeing to sponsor this doctoral degree; as my bosses and mentors at the time, thank you for recognising my potential. Marc Jones, Ian McKay, Lester Pearson and Paul Rowley as friends, highly professional colleagues and honest sounding-posts, without whom I would have lost my sanity and direction quite frequently. Mr Wayne Johnson, chairman of QinetiQ's Ordnance, Munitions & Explosives safety panel, for opening my eyes to other perspectives of safety. To my colleagues in the Operations and Safety Trials Working Group, especially Steve Harper, for keeping me organised during some of the more demanding periods of work.

To my thesis panel, Prof. Philip John, Prof. Richard Ormondroyd and Dr. Mike Williams for their wisdom, support and encouragement. Special thanks to my supervisor Dr Mike Edwards for making time to travel down to West Wales and visiting me in my office; and for the hours of stimulating discussion, support and reflection over the occasional pint, it was very much appreciated.

Finally to my wonderful wife Linda, daughter Gwenlluan and son Carwyn, for tolerating my briskness, exhaustion and absenteeism for the last few years. I honestly couldn't have done it without you; I missed you greatly. Dad's home! xxx.

This page left intentionally blank.

TABLE OF CONTENTS

TITLE PAGE ……..i
ABSTRACT iii
ACKNOWLEDGEMENTS v
TABLE OF CONTENTS vii
LIST OF TABLES xiii
LIST OF FIGURES xv
ABBREVIATIONS xvii
GLOSSARY xxiii
CHAPTER 1 1
Introduction 1
1.1 Thesis Overview. 1
1.2 Research Area Catalysts. 1
1.3 The Research Question. 3
1.4 Thesis Aims. 5
1.5 Focussing Upon The Research Area. 7
1.6 A Systems Approach. 9
1.7 Thesis Structure. 11
1.8 Summary. 15
CHAPTER 2 17
Introducing the T&E Environment 17
2.1 QinetiQ's role in the management of Ranges. 17
2.2 History of the T&E Ranges. 18
2.3 Future Requirements for Ranges. 21
2.4 Integrating the Air Ranges. 22
2.5 The Foundations for an Integrated Air Range Operation. 23
2.6 Benefits from an aligned Air Range Operation. 24
2.7 Previous Attempts at Alignment. 25
2.8 Real and Tangible *Synergy*. 25
2.9 A Fully Integrated Air Range Operation. 26
2.10 The Author's Evolving Mindset. 27

CHAPTER 3 29
An Introduction to the UAV Industry 29
3.1 Introduction. 29
3.2 Civil and Military UAVs. 30
3.3 Current Civil UAV Operations. 31
3.4 Market Opportunities. 33
3.5 The Author's Involvement With Civil UAVs. 35
3.6 Civil UAV Regulations and Certification. 35
3.7 Legal Considerations. 36
3.8 Exemptions for Civil UAV Flights. 38
3.9 Certification of Civil UAVs. 38
3.10 The Light UAV Policy. 39
3.11 Civil UAV Classifications. 39
3.12 Applying the Light UAV Policy. 41
3.13 Airworthiness and the Large Model Association. 45
3.14 The LMA Standards. 46
CHAPTER 4 47
Safety Cases - A Literature Review 47
4.1 Introduction. 47
4.2 Development of Safety Legislation. 47
4.3 Health and Safety Law. 49
4.4 Evolution of the HSC and HSE. 51
4.5 Introduction to Safety Cases. 52
4.6 Purpose of Safety Cases. 54
4.7 Definitions. 55
4.8 Contents of Safety Cases. 56
4.9 Communicating the Argument. 60
4.10 Safety Case Development Lifecycle. 69
4.11 A Staged Approach to Creating a Safety Case. 71
4.12 Risk. 78
4.13 Limitations of Current Conventions. 109
4.14 The Maintenance of Safety Cases. 113

4.15 Future use of Safety Cases within Dependability Arguments. 114
4.16 Summary. 115
CHAPTER 5 117
An Integrated Air Range Operation 117
5.1 Introduction. 117
5.2 The Author's Centralised Air Range Vision. 117
5.3 The Business Rationale. 118
5.4 The Regulatory Requirements For Legal Operations. 127
5.5 The Engineering Solution. 129
5.6 The Security Aspects Of Remote Data Transfer. 134
5.7 A Preliminary Safety Case for the Proposed Engineering Solution. 139
5.8 The Extant Range Safety Cases. 143
5.9 The Human Component of a System. 150
5.10 Minimising Human Errors. 151
CHAPTER 6 155
Safety Culture - A Literature Review 155
6.1 Introduction. 155
6.2 Background. 159
6.3 Separating Culture And Climate. 160
6.4 An Overview Of Safety Culture. 161
6.5 A Definition For Safety Culture. 162
6.6 Linkages To The Causes Of Accidents. 163
6.7 A Growth Of Knowledge. 163
6.8 The Scope of Safety Culture. 164
6.9 Attributes Of A Good Safety Culture. 166
6.10 Focussing On The Safety Climate. 167
6.11 Developing Patterns Of A Safety Climate. 168
6.12 The Existence Of Sub-Cultures Within Organisations. 177
6.13 Effective Communications Within Organisations. 179
6.14 Collecting, Measuring and Analysing Safety Related Information. 181
6.15 Incidents And Near Misses. 183
6.16 Developments Within The Behavioural Aspects Of Safety Management. 186

6.17 Summary. 187
CHAPTER 7 191
A ‘Systems’ Approach To Safety Cases 191
7.1 Introduction. 191
7.2 Integrated Air Range Safety Case. 194
7.3 A Subjective View of Safety. 196
7.4 Quantitative and Qualitative Safety. 198
7.5 Applying Qualitative Data. 201
7.6 Verifying Qualitative Texts. 205
7.7 Concluding Remarks on a Qualitative Approach. 208
7.8 A ‘Systems’ Overview 209
7.9 Human Factors within System Safety. 211
7.10 A ‘Systems’ Approach for Light UAVs. 212
CHAPTER 8 215
The Safety Case Elicitation Tool 215
8.1 Introduction. 215
8.2 The Author’s Concerns and Observations. 216
8.3 The Decision to Include Human Factors and Safety Attitude in the SCET. 219
8.4 Societal Concerns. 221
8.5 Forming the Safety Case Elicitation Tool. 222
8.6 The Safety Case Elicitation Tool. 223
CHAPTER 9 257
Guidance, Validation & Discussion 257
9.1 Guidance on Completing the SCET. 257
9.2 First Level Review of the SCET by the O&STWG. 258
9.3 Validation of the SCET. 260
9.4 Discussion. 263
CHAPTER 10 269
Conclusions & Recommendations 269
10.1 Conclusions. 269
10.2 Original Contribution to Knowledge. 271
10.3 Recommendations. 272

REFERENCES 275
BIBLIOGRAPHY 291
APPENDIX A 295
Geographical layout of MoD Aberporth Range Danger Area. 295
APPENDIX B 297
Geographical layout of MoD Hebrides Range Danger Area 297
APPENDIX C 299
Regulatory & Statutory Documentation for MoD Air Ranges 299
APPENDIX D 301
Storage, Transport & Preparation (FTR4) 301
APPENDIX E 303
Gun Firing (FTR 5) 303
APPENDIX F 305
Sighter Rocket Firing (FTR 6) 305
APPENDIX G 307
Sea Skua Missile Loading (FTR 07) 307
APPENDIX H 309
Disposal of unspent OME (FTR 08) 309
APPENDIX I 311
ASRAAM OM / *Sidewinder* AIM 9 strike (FT 01) 311
APPENDIX J 313
ASRAAM TOM strike (FT 05) 313
APPENDIX K 315
Non-participative aircraft collision (FT 08) 315
APPENDIX L 317
LGB / JDAM strike (FT 09) 317
APPENDIX M 319
Non-guided store strike (FT 12) 319
APPENDIX N 321
Maverick / Sea Skua strike (FT 15) 321
APPENDIX O 323
Rangehead Gun Firing (AS90 strike) (FT 18) 323

APPENDIX P 325
Sighter Rocket strike (FT 21) 325
APPENDIX Q 327
Mirach UAV strike (FT 26) 327
APPENDIX R 329
Store Breaches the Weapon Operating Boundary (FT B3) 329
APPENDIX S 331
Competence & Professional Standing of the O&STWG 331

LIST OF TABLES

Table 3.1 Summary of CAA policy for UAVS flying in UK airspace 42
Table 3.2 Maximum permissible mass & velocity to maintain the 95 kJ limit 44
Table 3.3 Relationship between the mass & cross-sectional area of a bluff body arising from the 95 kJ limit 45
Table 4.1 Average annual risk of injury as a consequence of an activity …….....84
Table 4.2 Average annual risk of death as a consequence of an activity …….....85
Table 4.3 Non-exhaustive list of generic hazards ……..91
Table 4.4 Non-exhaustive and illustrative list of HAZOP guidewords ... …….....92
Table 4.5 Risk Likelihood Categories ……....100
Table 4.6 Risk Severity Categories.……....101
Table 4.7 Risk Classification Table ……....102
Table 4.8 Operational Risk Classification Table ……....102
Table 4.9 Road Valuations of Preventing Fatalities for Selected Years……105
Table 4.10 Risk Reduction Methods …….108
Table 5.1 Fault Tree Top Events for Activity Participants …….....145
Table 5.2 Fault Tree Top Events for Activity Non-Participants ..……..…147
Table 9.1 Comparison between SCET and goal-based safety cases …….261

This page left intentionally blank.

LIST OF FIGURES

Figure 1.1 Diagram illustrating the author's evolution of thought for the research ….....3
Figure 2.1 Geographical overview of MoD Aberporth and MoD Hebrides ……....19
Figure 4.1 Example BBN of a Range's missile tracking abilities …….……...64
Figure 4.2 GSN entities, symbols and brief descriptions …….67
Figure 4.3 Example GSN taken from Kelly & McDermid (1995).…….....68
Figure 4.4 Illustration of the alignment of Design and Safety Case Lifecycles ……...73
Figure 4.5 Framework for the tolerability of risk, based upon the HSE .....…….....81
Figure 4.6 Example of a Fault Tree Analysis (FTA) (Garman, 2006)..……...99
Figure 6.1 Trends in attributed accident causes (Hollnagel, 2004)…….....158
Figure 7.1 Diagram illustrating the procedural and residual risks of various aircraft operations……...213
Figure 9.1 Diagram illustrating how qualitative data strengthens traditional safety cases and combines the people element of systems…….266

This page left intentionally blank.

ABBREVIATIONS

A&R	Airfields and Ranges
ACMH	Advisory Committee on Major Hazards
ACSNI	Advisory Committee on the Safety of Nuclear Installations
ALARA	As Low As Reasonably Achievable
ALARP	As Low As Reasonably Practicable
AM	Amplitude Modulation
AMRAAM	Advanced Medium Range Air to Air Missile
ANO	Air Navigation Order
APM	Association of Project Managers
ASAM	A Safety Argument Manager
ASCOT	Assessment of Safety Culture in Organisations Team
ASRAAM	Advanced Short Range Air to Air Missile
ATC	Air Traffic Control
ATCO	Air Traffic Control Officer
ATS	Air Traffic System
ATSA	Air Traffic Services Assistant
AUC	Airspace Users Committee
BAES	British Aerospace Systems
BBN	Bayesian Belief Network
BP	British Petroleum
CAA	Civil Aviation Authority
CAP	Civil Air Publication
CATS	Combined Aerial Target Systems
CBA	Cost Benefit Analysis
CE & SO	Chief Examiner & Safety Officer
CEC	Commission of the European Communities
CHASE	Complete Health and Safety Evaluation
CIMAH	Control of Industrial Major Accident Hazards
CIRAS	Confidential Incident Reporting and Analysis System
CMI	Chartered Management Institute

COMAH	Control of Major Accident Hazards
ConOps	Concept-of-Operations Document
COTS	Commercial-Off-The-Shelf
DA	Design Authority
DACS	Danger Area Crossing Service
DAP	Director of Airspace Policy
DERA	Defence Evaluation Research Agency
DoE	Department of Energy
DOSG	Defence Ordnance Safety Group
DoT	Department of Transport
DTEG	Defence Test & Evaluation Group (MoD)
DWP	Department for Work and Pensions
EASA	European Aviation Safety Agency
EC	European Country
EFA	European Fighter Aircraft (*Typhoon*)
EGD	European & Great Britain Danger Areas [Restricted Areas]
ETA	Event Tree Analysis
EU	European Union
FDM	Frequency Division Multiplexing
FEPA	Food and Environmental Protection Act
FIR	Flight Information Region
FM	Frequency Modulation
FMEA	Failure Modes and Effects
FSK	Frequency Shift Keying
FSS	Five Star System
FTA	Fault Tree Analysis
FTS	Flight Termination System
GBAD	Ground Based Air Defence
GFA	Government Furnished Asset
GP	General Practitioner
GPO	General Post Office
GPS	Global Positioning System

GSN	Goal Structured Notation
HALE	High Altitude Long Endurance
HASP	Hazardous Activity Scrutiny Panel
HAZOP	Hazard and Operability Study
HERTES	Human Error Reduction Technique for Evaluating Systems
HLA	High Level Argument
HMI	Human-Machine Interface
HMSO	Her Majesty's Stationery Office
HNC	Higher National Certificate
HSC	Health and Safety Commission
HSE	Health and Safety Executive
HSW	Health and Safety at Work Act
HVM	High Velocity Missile (*Starstreak*)
IAEA	International Atomic Energy Agency
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
ICI	Imperial Chemical Industries
IET	Institution of Engineering and Technology
IPT	Integrated Project Team
ISA	Independent Safety Assessor
ISC	Interim Safety Case
ISRS	International Safety Rating System
JATO	Jet Assisted Take-Off
JDAM	Joint Direct Attack Munition
JSP	Joint Service Publication
LA	Local Authorities
LACC	London Air Control Centre
LAN	Local Area Network
LGB	Laser Guided Bomb
LMA	Large Model Association
LPG	Liquid Petroleum Gas
LTPA	Long Term Partnering Agreement (QinetiQ/MoD 25 year contact)

MANAGER	MANagement Assessment Guidelines in the Evaluation of Risk
MATS	Manual of Air Traffic Services
MEB	Maximum Energy Boundary
MoD	Ministry of Defence (UK)
MORT	Management Oversight and Risk Tree
MoT	Ministry of Transport (UK)
MPA	Maritime Patrol Aircraft
MPC	Missile Practice Camp
MTBF	Mean Time Between Failure
NATS	National Air Traffic Services
NEBOSH	National Examination Board in Occupational Safety and Health
NEC	Network Enabled Capability
NII	Nuclear Installations Inspectorate
NOMAC	Nuclear Organisation and Management Analysis Concept
NOTAM	NOtice To AirMen
O&STWG	Operations and Safety Trials Working Group
OC	Operations Controller
OM	Operational Missile
OME	Ordnance, Munitions and Explosives
ONC	Ordinary National Certificate
OSA	Official Secrets Act
OSC	Operational Safety Case
OSTI	Operant Supervisory Taxonomy Index
PGM	Precision Guided Munition
PHA	Preliminary Hazard Analysis
PLC	Public Limited Company
PPE	Personal Protective Clothing
PPP	Public-Private-Partnership
PRIMA	Process RIsk Management Audit
PRISM	Professional Rating of Implemented Safety Management
PSA	Probabilistic Safety Assessment
PSC	Preliminary Safety Case

QC	Queen’s Council
QRA	Quantitative Risk Assessment
RA	Royal Artillery
RAC	Range Air Controller
RAE	Royal Aircraft Establishment
RAeE	Royal Aerospace Establishment
RAF	Royal Air Force
RDA	Range Danger Area
RIU	Range Interface Unit
RF	Radio Frequency
ROM	Rough Order of Magnitude
RSM	Range Safety Manager (MoD Regulator)
RSSB	Rail Safety and Standards Board
RT	Radio Telecommunications
SAM	Safety Argument Management
SATCO	Senior Air Traffic Control Officer
SBAC	Society of British Aerospace Companies
SCIDA	Security Configuration and Installation Design Authority
SEPA	Scottish Environmental Protection Agency
SFAIRP	So Far As Is Reasonably Practicable
SCET	Safety Case Elicitation Tool
SHIP	Safety of Hazardous Industrial Processes
SHOLIS	Ship Helicopter Operating Limit Instrumentation System
SIL	Safety Integrity Level
SME	Subject Matter Expert
SMS	Safety Management System
SRG	Safety Regulatory Group (CAA)
SWIFT	Structured What-If Technique
T&E	Test & Evaluation
TCO	Trials Conducting Officer
TCS	Trials Control System
TDM	Time Division Multiplexing

TESD	Test & Evaluation Support Division
TEST	Trials Evaluation Services and Targets
TOM	Telemetry Operational Missile
TOR	Tolerability Of Risk
TQM	Total Quality Management
TSM	Trial Safety Manager
TSPI	Time, Space & Positional Information
UAV	Unmanned Air Vehicle
UAVS	Unmanned Air Vehicle System
UCAV	Unmanned Combat Air Vehicle
UK	United Kingdom
UNCED	United Nations Conference on the Environment and Development
US	United States
USA	United States of America
USD	United States Dollar
VIP	Very Important Person
VPF	Valuations to Prevent Fatalities
VPN	Virtual Private Network
WAN	Wide Area Network
WAG	Welsh Assembly Government
WDA	Welsh Development Agency
WOA	Weapon Operating Area
WPAM	Work Process Analysis Modelling
WWUAVC	West Wales Unmanned Air Vehicle Centre

GLOSSARY

AS90	British 155mm Self Propelled Howitzer.
AMRAAM	American medium-range air to air radar guided missile.
ASRAAM	British short-range air to air heat seeking missile.
Banshee	¼ scale sub-sonic UAV operated as Range aerial target.
Bloodhound	British medium-range surface to air guided missile.
Complexity	Quality of being intricate and compounded.
Corporal	American surface to surface guided missile.
Dependability	Trustworthy and reliable.
Emergent	Characteristic of the system as a whole, not its component parts.
Falconet	¼ scale sub-sonic UAV operated as Range aerial target.
Govier notation	Graphical notation for constructing arguments.
Hazard	Potential for harm arising from an intrinsic property or disposition of something to cause detriment.
Hermeneutics	Theory of interpreting linguistic & non-linguistic expressions.
Hermes 450	Israeli sub-sonic, single engine, intelligence gathering UAV.
Holism	Theory that certain wholes are greater than the sum of their parts.
Individualistic	Belief in the primary importance of the individual.
Jindivik	Australian ⅔ scale sub-sonic UAV.
Maverick	American air to surface guided missile.
Mirach	½ scale sub-sonic UAV operated as Range aerial target.
Nimrod	British Maritime Patrol Aircraft.
Positivistic	Knowledge based on sense experience and positive verification.
Predator	American medium-altitude tactical endurance UAV.
Rapier	British short-range surface to air missile system.
Risk	A chance that someone or something that is valued will be adversely affected in a stipulated way by a hazard.
Sea Skua	British anti-ship missile (fast patrol boat and helicopter launched).
Sea-Slug	British medium-range surface to air guided missile.
Sidewinder AiM 9L	American short-range air to air heat seeking missile.
Starstreak (HVM)	British short-range surface to air High Velocity Missile (HVM).

Stormshadow	Anglo-French air-launched cruise missile.
Systems Engineering	Application of *Systemic* thinking to an engineering system.
Toulmin form	Method of argument analysis to examine its foundational logic.
Typhoon	European twin-engined, canard-winged, multi-role jet aircraft.
Watchkeeper	British network enabled military UAV project.

CHAPTER 1

Introduction

1.1 Thesis Overview.

This chapter is designed to introduce and explain the construct of the overall thesis. Predominantly it provides context to the subject matter and explains the author's thought processes in identifying the specific area of research. The chapter identifies the catalysts for pursuing the research question and lays out how the author has subsequently addressed those issues which are fundamental to its answer. In addition to the aforementioned, this chapter defines the scope of the thesis, bounds the problem area and provides justification for the pursuit. In its latter stages it explains the relationship between the chapters as a 'storyboard', helping the reader to understand how two predominantly disparate fields are brought together to create a truly synergistic output.

1.2 Research Area Catalysts.

The author's specific role within the company at the time of this research was relatively fluid though his overarching role was that of providing safety, technical and operational guidance to a number of Test and Evaluation (T&E) Range capabilities across the United Kingdom (UK). The original intent of the research was to investigate the creation of a safety argument to allow T&E activities to be conducted at one site through the application of a remote command and control facility. In simple terms, the aim was to capture raw trajectory data at one site and to display it at a remote site so that it may be used in real-time to control assets employed in the conduct of T&E activities such as live air to air missile engagements.

During the same timeframe the author was drawn into safety management discussions within the company; these discussions had been provoked by the report of the United States Refineries Independent Safety Review Panel (BP, 2007) which had investigated the fatal incident at the British Petroleum (BP) Texas City refinery in March 2005. The incident, where five workers had died and 180 workers had been injured, had raised the profile of process safety across the world's largest organisations. The author's employer started to

review the learning and recommendations offered by the report and had begun to take active steps to investigate its own organisation's extant safety climate and safety culture.

During his time as the Range Operations Manager at the Ministry of Defence (MoD) site, Aberporth, the author had been heavily involved with reviewing safety submissions and Concept of Operations (ConOps) documentation which served as base 'safety cases' for many hundreds of trials activities. This experience, combined with a background in electronic and instrumentation radar engineering, had led to the creation of a mindset which was predominantly influenced by traditional quantitative safety approaches such as logic diagrams, Fault Tree Analysis (FTA) and a very mechanistic (ordered) method of deriving an acceptable rationale for allowing trials activities to occur. In all honesty, the author, at the time, lacked the deeper reflective and cognitive insights. Upon the arrival of a need to review the cultural aspects of safety within the organisation, brought upon by the BP incident, the author struggled to rationalise how the two, somewhat disparate fields (engineering and culture), could be interlinked; this amalgam was effectively clarified and consolidated by later studies in the field of *Systems Engineering*.

In the years leading up to the commencement of this research the author had been heavily involved in the rationalisation of the UK's QinetiQ operated Air Ranges; a role which demanded not only a technical and safety related input but also a business perspective. Ultimately, a small peninsular airfield site at Llanbedr, in North Wales, was closed and three other sites suffered heavy redundancies as a direct result of the project. Another key output from the rationalisation was the transfer of Aberporth's airfield from MoD to the Welsh Development Agency (WDA) (via other parties) in direct support of the Welsh Assembly Government's (WAG) vision to create a 'centre of excellence' for Unmanned Air Vehicle (UAV) operations. The investment of £21million to create the centre, adjacent to the MoD's Range, was based upon a 50 acre site and a vision to attract technology leaders for the development, testing and evaluation of both UAVs and future Unmanned Combat Air Vehicles (UCAVs). The infrastructure deployed has the ability to support up to 1,000 jobs (SBAC, 2005). The author, in over one hundred events, presented the Range's technical and operational capabilities, in the context of UAV activities, to many captains of industry and government leaders during the centre's formative period. It was whilst

engaged in many of the centre's marketing and strategy activities that the author became consciously aware of the future requirement for small, civilian classified, UAVs to be operated on a commercial basis to support various industries.

1.3 The Research Question.

Having identified the key catalysts for this research the reader may identify how the author has further developed the concept of creating a more cost effective, and reduced timeline, safety case model. This new model would need to not only encompass the majority of the system's engineering facets but would also need to look at the 'softer' and cultural aspects of the operating organisation. Figure 1.1 illustrates how the author's thoughts, subjected to the preceding influences, led to the topic of research.

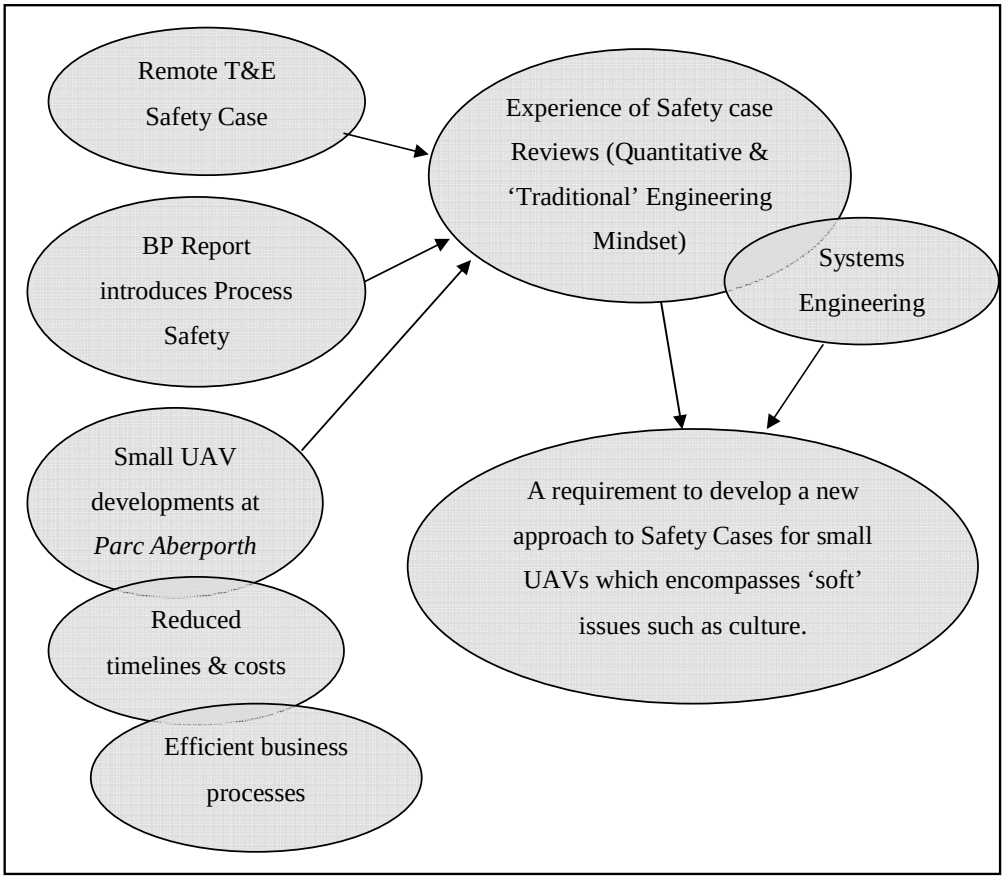


Fig 1.1 - Diagram illustrating the author's evolution of thought for the research.

It should be noted that the prime driver amongst all of the requirements highlighted was that of creating a safety case model which was going to be realistically useable by the smaller companies which were being drawn into the civil UAV market. If these organisations were going to be subjected to the industry's extant and preformed views of safety cases, predominantly driven by the military's hard-line and costly approach, then the industry as a whole could suffer. As in most other industries, it is the absence of barriers to entry which allows a positive contribution to technology transfer and evolution. The author believed, by creating a simplified and more holistic model for developing a safety argument for civil light UAVs, that it would appear not only as being more acceptable to those small companies seeking market entry but that it would act as an enabler and demonstrate the industry's cognisance of its current limitations and willingness to evolve.

The author is very much aware of the need to effectively analyse and decompose many complicated sub-systems within the heavier and larger UAV platforms to create an effective safety argument prior to allowing it to operate. The concept of a simpler safety case is not in any way designed to undermine those processes which underpin the larger UAV platforms; on the contrary, much of what is proposed within this thesis has been evolved from the way that larger platforms have been effectively and safely managed by the defence industry for over fifty years. The author advocates that as technology and society advances then reviews must be conducted periodically upon any long standing processes where lessons may be learnt and best practices adopted. In a similar vein the author believes that there are occasions where processes may need to be adapted to more suitably and effectively manage the subject material; in more common terms there are always opportunities to 'use the most appropriate tools for the job'.

Finally, as the author started to research the small UAV environment in more detail the initial concept was very much given a boost when it was uncovered that the Civil Aviation Authority's (CAA) light UAV class exhibited a minimal level of regulatory control and guidance. The classification relies heavily upon long standing extant practices which fail to take into account the quickly advancing environment of commercial civil UAV development.

The research question that was finally distilled out of the earlier mélange of thoughts and challenges was;

"Can a revised, time efficient, 'fit-for-purpose' and more holistic safety case elicitation tool be created to support the activities of lighter and smaller scale civil UAVs which are to be operated within the UK?

1.4 Thesis Aims.

This thesis has been written to both clarify expectations and to support safety management within the UAV industry. It attempts to provide clear guidance for operators within a defined UAV class and also support to those who are charged with ensuring the safety and integrity of the operation. The thesis specifically addresses the following five key areas;

- The author, from research and experience, is unaware of any definition or prescriptive requirement for a safety case to support the activities of civil light UAVs (<150kg). The safety case elicitation tool created within this thesis is the first ever attempt at formalising the requirement.
- Research and experience in the field of safety cases suggests that there are clear, but relatively high-level, definitions to safety cases. Whilst this approach may be adequate for extremely large systems, where support tools (e.g. HAZOP) may be used to identify key areas which require investigation, smaller systems, such as civil light UAVs, require a clearly identified and more granular series of cues to support the safety case development. This observation and requirement is especially driven by the potential for such systems to be designed, built and operated by lesser experienced organisations given the commercial opportunities which may become available as the UAV environment grows. The safety case elicitation tool created within this thesis is the first ever attempt at providing a formalised, specific and granular approach to civil light UAV safety planning and management.
- Safety cases, from the author's experiences, are becoming extremely bureaucratic in structure and in nature, often resulting in an abundance of pages and even volumes of text and diagrams. Lord Cullen highlighted in the Ladbroke Grove Rail Inquiry that the purpose of the safety case regime was to "*encourage people to*

think as actively as they can to reduce risks"(Cullen, 2001). The creation of a safety case for an activity or a system is likely these days to be sub-contracted to either a different sub-division within the company or an external organisation as the task is often seen as 'too difficult' and/or 'requires specialist skills' to be generated from within. By 'exporting' the task the draft safety case quite often requires a degree of correction and ratification by the service demander; this in turn suggests that there is a degree of misunderstanding of the system under scrutiny being demonstrated by the safety case author. This also suggests that competency is relatively low, especially in those areas where human interactions are important (granular and technical user levels) and that ownership of the safe processes is not embedded within the system's operating regime. The author suggests that the wrong people are involved in the process. At times it may be considered that the creation of such a safety case is purely driven by the need to support the regulatory requirement (compliance) and not to underpin safe operations. The simplified and holistic safety case elicitation tool created in this thesis attempts to minimise the need to sub-contract and to refocus safety ownership.

- Irrespective of the robustness and/or the depth and breadth of any safety case, the integrity of the final operation is limited by the safety effectiveness of those humans who control and exercise the system under scrutiny. The simplified safety case elicited from this thesis combines and integrates traditional 'hard engineering' principles with 'people' issues, predominantly those elements concerned with an organisation's safety attitude and culture. From both experience and research, the author believes that this is a first within the field of UAV safety cases.
- Safety cases are predominantly driven and managed by safety managers with an engineering background. Engineering, within itself, is very much a quantitative discipline; it relies upon and uses a quantitative approach to deliver tangible outputs to the real world. Mathematics and statistics are used to support designs, developments and analysis of most environments whilst any qualitative input is often relegated and assigned to a poor second place. This thesis, and the simplified safety case elicited from within it, attempts to identify and communicate the need to re-assess the importance of qualitative information within the field of safety engineering and any subsequent creation of a safety argument. The simplified

safety case relies heavily upon qualitative, and even subjective appraisals, in creating a safety argument; this in itself is a new form of approach to civil light UAV safety.

Formatted: Bullets and Numbering

1.5 Focussing Upon The Research Area.

The overall objective of this thesis is to define a guideline for the creation of a simpler safety case for use in the field of civil light UAVs; this field is of great interest to the author given the potential within the industry. The lack of a heavy regulatory regime offers opportunities to develop a relatively new approach to their safety management. Such UAV systems fall within the CAA's light UAV (<150kg) class.

The final output of this thesis is a simplified safety elicitation guideline which assesses not only the technical integrity of the owning/operating organisation but also its inherent safety culture and safety climate. Such organisations are predominantly low business scale/low budget organisations which cannot afford to conduct a full scale safety assessment and analysis of their vehicles and sub-systems. Quite often such systems use Commercial-Off-The-Shelf (COTS) component parts which have a limited engineering integrity and would be extremely difficult to qualify using quantitative safety tools. The author's experience of such approaches would suggest that safety engineers are easily drawn to err on the side of optimism in assigning failure modes and probabilities to low integrity components. The failure effects are also often exaggerated by the demonstrable lack of system awareness and ignorance of the interactive way by which single component failures may effect a systematic failing.

The civil UAV industry is, by and large, relatively slow to develop within the UK whilst the military arena has been operating UAVs for many decades, both as reconnaissance and target vehicles. One of the major current drawbacks in the UK is that the rules for flying UAVs are extremely restrictive. Military UAVs are heavily regulated and are forced to fly within permanent segregated airspace such as military danger areas. Such activities and environments are heavily regulated and rely upon large volumes of airspace augmented by technically superior and costly surveillance services. Civil UAVs, predominantly recreational model aircraft, may be flown without the protection of any segregated airspace,

often in green field sites with virtually no surveillance facilities. Such civil UAVs fall within the <150kg classification and are predominantly restricted to flying within visual distance (500m) of the operator and at a maximum altitude of typically 400ft.

Having been involved in the development of the West Wales UAV Centre (WWUAVC) at *ParcAberporth* the author has always had concerns over the safety assessment of those civilian UAVs which would be operating from its airfield. Some of these UAVs would certainly fall into the <150kg classification. Such classifications of UAV operations have in the past been largely unregulated though in more recent years the CAA have started to address these requirements through the development of a Light UAV Policy (CAA, 2004a.). This policy will be further examined in Chapter three of this thesis. This policy outlines the structure and inter-relationships between Civil Aviation Policy (CAP) 722 (UAV Operations in UK Airspace-Guidance), CAP 393 (The Air Navigation Order (ANO) 2000 (as amended)) and CAP 658 (Model Aircraft: A Guide to Safe Flying).

Formatted: Bullets and Numbering

The author's vision was to develop an approach to creating a safety case for smaller scale projects which did not rely as heavily on the highly quantitative and often probabilistic approaches which is the norm within his industry of aerospace and defence. Whilst the author is cognisant of the fact that most, if not all, of the projects that he has been involved with to date have been relatively large and coupled to the management of relatively large hazards, he strongly believes that there is an opportunity to develop a more condensed, less laborious and cheaper model for safety management. The author believes that there is an opportunity and a need to develop a simpler form of conveying a safety argument for smaller and more simplistic projects. This belief has been amplified in recent years by his involvement with the WWUAVC and the clear need to simplify and condense the process of flying civil light UAVs.

To create a more rounded, realistic and reliable form of safety case for these lighter UAVs the author has adopted a *Systems Engineering* approach.

This revised approach to assembling a safety case for civil light UAVs does not tackle the most demanding of current UAV challenges which is that of 'sense and avoid'. The aim of

this new type of safety case approach is to facilitate a more complete body of evidence so that safety engineers, safety managers and/or regulators may make a more accurate, relevant, and consolidated judgement of the system under scrutiny. The decision upon how to manage the 'sense and avoid' issue may be incorporated into the safety case, at a later stage, once an agreed policy and procedure has been identified by the relevant regulatory authorities.

1.6 A Systems Approach.

Whilst there are subtle variations in the definitions offered to what constitutes a system, (Hitchins, 1992 & Weinberg, 1975) there is an underlying consistency in the opinion that any system is comprised of a set of interacting elements which work towards a common theme or purpose within a specific environment (Skyttner, 2001). To allow these elements to qualify as components of a system they must display a number of fundamental characteristics such as holism, complexity and emergent properties (Flood & Carson, 1993). Such notions may be illustrated by applying them to a modern airliner. The common goal for the system is that of transporting people and/or freight across large distances within an agreed network of routes. The aircraft itself may be broken down to its prime sub-components of engine, control surfaces and aircrew. Whilst each sub-component serves a function in isolation, they may only transport people or freight when brought together as a single entity. When assembled they provide a synergistic benefit which is greater than the sum of the individual parts.

The modern airliner, especially the new Airbus A380 super jumbo with its leading edge application of advanced technology, is a prime example of current day systems thinking developments. Whilst in the early periods of systems design a project would be predominantly controlled by one individual who relied upon his own knowledge and experience, the modern application of systems thinking necessitates an input from many experts from many specialised fields. Whilst early projects relied upon the knowledge contained within one person's head the ideas and visions were easily converted into a completed system through the use of local skilled labour which was co-located within the same workshop. As technology advanced then so the degree of system complexity grew; quite often this led to the use of larger and disparately skilled teams located in different

places. This, coupled to the use of more components led to a system whose complexity was too great for one person to understand. As both systems and project teams grew in size and complexity a need arose to maintain a structured and well defined regime for managing the complete entity. When assembling the ideas and views of many experts to enable the design of a complete system there is an inherent requirement to define an approach which both ensures and assures thoroughness and completeness of the final creation. Such an approach supports the management of these complex tasks as well as minimising the likelihood of poor component integration and/or creating a final product which does not fulfil its design criteria. As technology and specialisms grow then so the need for a common language such as systems engineering must develop with them.

Through embracing a systems approach and by focussing upon both the technological and human domains of a system under scrutiny the whole system may be systematically broken down and analysed in a logical manner. Hitchins (1992, p3) allows these domains to be classed as socio-technical, where quantifiable engineering elements are fused with dynamic, unpredictable and un-quantifiable humans (Waring, 1996). Any applications and/or assumptions should therefore take account of a human's ability to modify the behaviour of a system under scrutiny in either a positive or negative sense. This is a very important observation and property; within the context of a safety critical system and in the creation of a safety argument, cognisance and due diligence to the human interaction should be applied if the analysis is to be both accurate and veritable.

Safety fits relatively naturally within the general systems engineering process and the methodology of problem solving that it brings with it. Such a problem solving process involves several stages. The first stage requires the problem to be specified in terms of its objectives which must satisfy any specified criteria; the process then continues to synthesise all options in an iterative fashion to create a set of results which will reflect upon all of the alternative options. Having analysed and evaluated the options against the stated objectives and design criteria a final solution is agreed upon. In the creation of a refined final solution the results of latter stages are fed back into some of the former stages so as to help modify the objectives and design criteria and thus create an optimally refined and more mature entity. System safety and therefore safety cases should be treated as an

integral component of systems engineering which is a current and common practice within the defence industry (Leveson, 2002).

1.7 Thesis Structure.

This thesis has been divided into nine chapters in order to effectively, and progressively, lead the reader through its development and to reflect the logical and systematic method in which a systems approach has been applied to the problem.

Due to the quite specialised environment of aerospace T&E, especially within the field of end to end weapon testing and UAV proving, the author has included a chapter (chapter two) to explain the operating environment in detail. The chapter also provides essential peripheral information to the reader and therefore provides much needed context. As with many other specialised and discrete working environments there is a specific and quite indigenous culture and language presence; the chapter helps to clarify any such occurrences.

Chapter two provides the reader with an overview of the history of the T&E Range capabilities, a comprehensive description of their technical and operational facilities and also constructively identifies some of their weaknesses within the context of the 21st century. This chapter also sets the scene for the concept of a more integrated operation across the two prime Air Range capabilities and the requirement to create a consolidated safety argument (safety case) for such an arrangement.

Chapter three introduces the reader to the world of both civil and military UAVs. It highlights the prime regulatory differences between both types and focuses upon the virtual absence of any formal and in-depth regulations for controlling the airworthiness of civil UAVs which have a mass of less than 150kg. The chapter also introduces the role of the Large Model Association and the part that it plays as the regulating body for recreational civil UAVs within the 20kg to 150kg limitations.

The chapter also introduces the reader to the market opportunities and potential for growth as technology advances. Whilst the demand for smaller scale civil UAVs is growing there is a clear identification of a need to create a formal regulatory framework to support it.

Chapter four consists of a thorough review of the academic, regulatory and industry related documentation related to the production, application and use of safety cases. This chapter looks at the need for safety cases and how they have evolved into most modern safety-related industries, especially those where hazards could have potentially catastrophic results (e.g. nuclear power, mining, and weapons proving). A comprehensive review of the structure of a safety argument is discussed in addition to the numerous methods and tools available to its author(s) including Risk Identification, Risk Assessment, Risk Reduction, Risk Management and ultimately, Risk Acceptance.

Of relative importance is the need to differentiate and clarify between the terms *Risk* and *Hazard*; two terms which are used interchangeably (colloquially) in an incorrect manner; chapter four clearly explains these differences. This chapter also provides the foundational underpinning for pursuing the research question.

Chapter five is a high level study of the need to remotely command and control the Hebrides Air Range Capability from the Aberporth site. The chapter demonstrates to the reader that the requirement must be considered as a whole entity, encapsulating a full 'systems' approach rather than a series of discrete work packages. By adopting a systems approach the concept must include not only the 'hard' engineering requirements such as data highways and equipment but operational processes, security and integrity, regulatory requirements, business drivers and overall system safety.

Due to the sheer size of the proposed project this chapter will focus ultimately upon the creation of a suitable preliminary safety case using some of the tools and concepts identified within chapter three. This chapter not only identifies and lists some of the typical issues and problems which may be encountered within the project but also attempts to offer forms of mitigation which may be utilised if the project is fully realised within the author's host company.

One of the prime concepts carried forward from the preceding is that of a need to create a safety case which must be inherently intertwined and matured as the project grows. It is imperative that the safety case is treated as a living document and as a constructive tool for an effective safe delivery rather than an isolated 'bolt-on' for project path and/or regulatory compliance.

This chapter concludes by raising the issue of organisational culture and the pivotal role that it plays in delivering compliance to a safety case. Organisational culture is identified by the author as fundamental in maintaining and implementing those control measures and mitigations raised and documented within the safety case. Without cognisance of, and due diligence to, these facets of an organisation, the whole safety process becomes stale and somewhat defunct.

Chapter six takes its cue from the preceding chapter's introduction to organisational culture. This chapter constitutes a thorough review of the academic and industrial literature related to the study of safety climate and safety culture within organisations. It begins with an introduction from JAC Brown's '*The Social Psychology of Industry*' which sets a context to the attitudes and beliefs of industrial organisations.

The chapter proceeds to delve into various industries, predominantly those of off-shore oil and gas, nuclear energy and mining; all of whom are renowned for their high risk activities, catastrophic accident consequences and strong insular sub-cultures. From a global perspective the author notes that some of the 'lesser' regulated nations, predominantly third world countries, are now adopting a more refined and stringent policy towards safety management, especially if they fall under the operating umbrella of a multi-national company. In such environments the cost of near-misses, incidents and fatalities are seen to limit turnover and erode profit. Though equipment down time and the cost of training new personnel remains a prime driver for this change in mindset, globalisation and the reality that investors are more selective over image (branding) is starting to apply even more leverage to this facet of business. The chapter concludes by highlighting the importance of safety culture for a continued and effective safe operation.

Chapter seven reviews the deficiencies and lessons learnt within chapter five and discusses them within the context of the theory of safety cases (chapter four) and safety culture (chapter six). The discussion is delivered from a systems perspective and identifies how a safety case cannot be argued to be effective or robust unless the 'people' element of the project is appropriately engaged.

The chapter proceeds into the civil UAV arena and the requirement to create suitable safety cases for their operation. Extant guidelines for the creation of a safety case for civil light UAVs is extremely limited; the accepted and general approach is that based upon large model aircraft which are used for recreational purposes. The chapter concludes by critically examining the CAA's light UAV policy and its lack of formality and rigour when applied to the construction, maintenance and operation of commercial civil light UAVs. Observations and recommendations emerge from this work which lead into the following chapter.

Chapter eight picks up on the preceding chapter's observations and recommendations to create an effective yet simple method of analysing a light UAV's operation. The chapter introduces the concept of a '*Safety Case Elicitation Tool*' (SCET) where a time and effort efficient safety case may be relatively quickly created to support those civil UAV operations which fall within the CAA's light UAV class. The SCET is configured as a guideline document which offers specific socio-technical cues for use by both the operator/constructor and any regulatory party. Each sub-heading within the SCET is accompanied by an explanatory text which explains to the user what approaches could be considered during its application to a new system. The SCET is qualified by a peer review of Subject Matter Experts (SMEs) from within the field of T&E. The chapter strengthens the observations and relationships between the theoretical and academic safety cases of chapter four with that of the concept discussed within chapter seven.

Chapter nine subjects the SCET concept to a critical peer review by a number of internal (QinetiQ)T&E SMEs to both judge and qualify its construct and potential for use. One of the key issues identified during such an evaluation was that of the competency of the accepting or regulatory body; the peer review, conducted as a workshop facilitated by the

author, identified by gap analysis that this new model for conveying the safety of a light UAV demands additional competencies and skills within those individuals and/or teams who are the receptors of the information. Traditional and long standing safety engineers rely upon a very quantitative and 'hard' engineering based competency upon which to make judgements on any safety integrity argument. What evolves from this qualification workshop is that here is a need to augment these traditional engineering skills with those of 'soft' skills such as social science and/or psychology.

The chapter concludes the thesis through discussion, critical analysis and the provision of recommendations for the future; it also identifies how the work offers an original contribution to knowledge.

Formatted: Bullets and Numbering

1.8 Summary.

System complexity continues to increase as technology advances; within the UAV environment it is becoming more evident that there is a need to embrace *systems of systems* thinking which must include both the hard engineering trades (e.g. mechanical engineering, software engineering, aeronautical engineering, *et al*,) as well as the soft engineering environments of culture and socio-technical interfacing.

This thesis attempts to provide a simple, '*fit for purpose'* and relatively bespoke method of assessing the safety components within a small, lightweight, yet complete, civil UAV system. The output allows the operator and/or an independent body to attain a degree of confidence that its operation is safe, to a relatively high degree of integrity and practicality, and is justified in accordance with the Health & Safety Executive's (HSE's) model of risk management.

This page left intentionally blank.

CHAPTER 2

Introducing the T&E Environment

2.1 QinetiQ's role in the management of Ranges.

Since its formation in 2001, QinetiQ has been managing and providing many T&E and training facilities for the MoD across the whole of the UK; its ability to deliver such a specialised service is underpinned by a 25-year Long Term Partnering Agreement (LTPA) with the MoD. Amongst its portfolio of bespoke facilities are the four Air Range capabilities sited across England, Scotland and Wales. QinetiQ's management team works in partnership with the MoD in the co-ordination, management and execution of various activities at the four sites. In alphabetical order these sites consist of;

- MoD Aberporth, Cardigan Bay, West Wales,
- MoD Hebrides, Benbecula, Western Isles, North West Scotland,
- MoD Larkhill, Salisbury Plain, South East England,
- MoD West Freugh, Wigtownshire, South West Scotland

All four sites are steeped in decades of history combined with a strong sense of pride, professionalism and experience. Their capabilities were primarily formed as a response to the outbreak of the Second World War whilst subsequent additional facilities were added and evolved as the Cold War took its hold, predominantly in the 1960s and 1970s.

The Ranges themselves have been involved in many specialised in-service practice and T&E activities for more than 60 years. Such a rich background in safe methods of working have laid the foundations of what is regarded today as a premier service for the safe, professional and competent delivery of aircraft, weapons and UAV testing in the world. Though UAVs are a relatively new concept for the majority of the aerospace industry, these Ranges were actively flying and managing such platforms on an experimental and aerial target basis since the 1950s. From the early days of surface to air weapons such as *Bloodhound* and *Sea Slug* through to modern day weapons such as *Stormshadow*,

ASRAAM, and *Starstreak (HVM),* all of these Ranges have performed an essential part in their development and testing.

2.2 History of the T&E Ranges.

The MoD Air Range sites at Aberporth, Larkhill and West Freugh were created between the 1910s and the mid to late 1940s and have evolved through various guises within the MoD for in excess of 90 years. At inception the sites were operated through many departments of the government until they were finally aggregated within the Procurement Executive under the banner of the Royal Aircraft Establishment (RAE). As the European space programme grew stronger and the Ranges' facilities were used to support such activities then so the Ranges were renamed as Royal Aerospace Establishments (RAeE) in the early 1990s. Finally, in response to the Public-Private-Partnership (PPP) agenda of the 1980s the Ranges went through numerous transitions in the lead-up to the formation of QinetiQ in 2001.

The Hebrides Range at Benbecula was established in 1957 by the Royal Artillery (RA) as a Guided Weapons Range primarily for the incoming *Corporal* missile system which was delivered in 1959. Since this period and up until 2001 the site had been managed by the British Army though it attained agency status in 1998 as it joined the T&E Ranges under the Defence Evaluation Research Agency (DERA). During the 1970s, Ground Based Air Defence Missile Practice Camps (GBAD MPCs) in the guise of *Rapier* missile firings were introduced and have formed its core business activity until the present day. Such activities involved its inner Range Danger Area (RDA) and the flying of small scale UAVs as training targets. During the same timeframe the Range was involved in a number of large exercises which allowed surface, subsurface and air assets to be co-operatively deployed within large and multi-disciplined exercises.

Figure 2.1 gives a geographical overview of the Aberporth and Hebrides sites and an indication of the physical dimensions of the danger areas afforded for the conduct of in-service practice and T&E activities at each Range. These two larger Air Ranges, and the ability to integrate their operations, will be discussed further within this thesis.

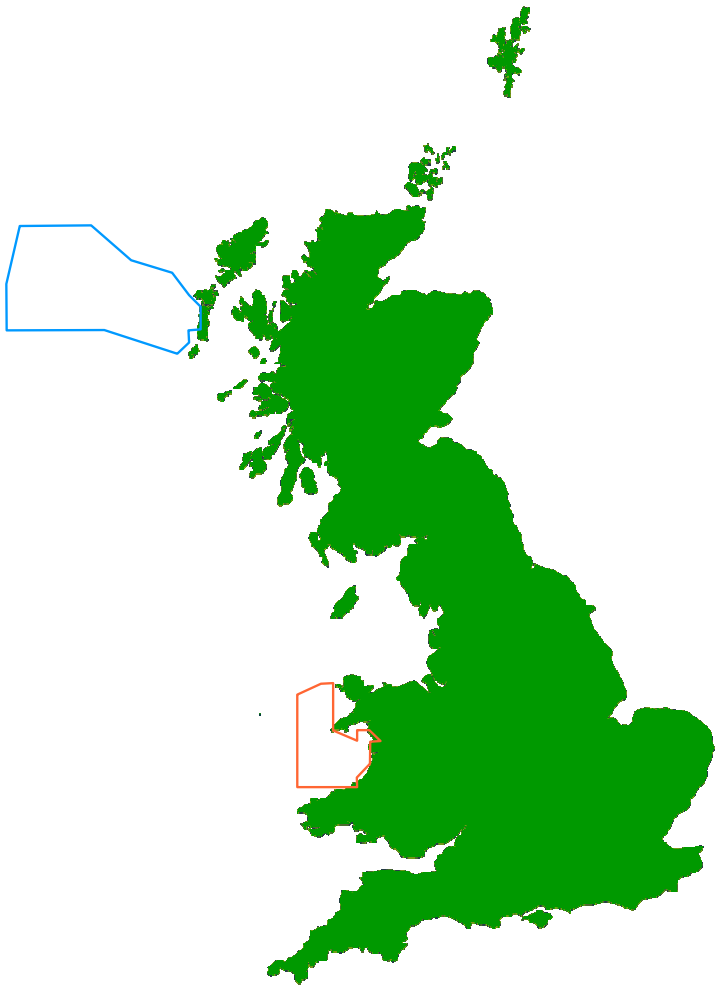


Figure 2.1 - Geographical overview of MoD Aberporth and MoD Hebrides.

Formatted: Bullets and Numbering

2.2.1 The Aberporth Range.

Aberporth Range in West Wales covers virtually all of the sea area of Cardigan Bay, and extends north-west beyond the Lleyn Peninsula; a detailed geographical map of the Range is included at Appendix A. It is comprised of the airspace contained within the permanent Danger Areas of D201 and D201A, together with the associated Danger Areas of D201B, D201C and D201D which may be activated by issuing an appropriate NOTice to AirMen (NOTAM). Each component part of the Danger Area complex, when active, offers an

unlimited operating height combined with a Danger Area Crossing Service (DACS) for any traffic which may require transit through the environment. The Range covers a surface area of 5,900km² (D201) which is extendable to 6,200km² (by NOTAM action) and offers a maximum linear dimension of 120km.

The Range's trials experience covers air to sea, air to air, surface to air and surface to surface guided and unguided weapon activities. Trialled systems include rocketry, artillery, missiles, UAVs, laser designators and many non weapon activities such as airborne instrumentation verification and satellite tracking.

Due to its relatively concave geographical location on the coast of Cardigan Bay the main Aberporth Rangehead site is supported by many coastal observation posts both to the north and to the south. These observation posts host many radar, communication and optical data gathering instruments which provide not only surveillance information but also behavioural data on any platform or store activity.

Formatted: Bullets and Numbering

2.2.2 The Hebrides Range.

QinetiQ's most Northern Air Range is located in the Western Isles, off the north-west of Scotland. Based on Benbecula, it is supported by installations on the North and South Uists as well as Hirta, the main island in the St Kilda group, which is 70km north-west of Benbecula; a detailed geographical map of the Range is included at Appendix B.

The Range comprises of two main components; the Inner Range and the Outer Range. The former comprises of the airspace contained within Danger Area D701 which is primarily used for surface to air missile firings (GBAD) and UAV flying. The Outer Range conforms to the airspace contained within D701A, B, C, D & E and extends into the Atlantic Ocean, including St Kilda, and is used primarily for high energy missile engagements.

When fully activated the complete complex offers the largest Air Danger Area in the United Kingdom offering maximum linear dimensions of 260km by 140km. Operating heights are controlled and operated in accordance with customer requirements.

The Range's experience is primarily in the live weapon engagement of aerial targets by GBAD missile batteries. Other activities include a limited number of state of the art high energy air to air missile engagements of subsonic and supersonic aerial targets in support of the MoD's procurement programme. The high energy air to air engagements executed at the Hebrides cannot be executed at any other Range facility within the UK due to the requirement for a large volume of airspace which must be sanitised prior to a safe weapon release. This large airspace requirement is predominantly a function of the high velocities and agilities demonstrated by third generation weapon systems; it is also reinforced by the current doctrine applied to air to air engagements where many of the flight profiles demand supersonic launch speeds and medium to high altitudes for weapon release.

2.3 Future Requirements for Ranges.

During the 1990's questions were raised regarding the continued use of the UK's Air Range capabilities. The majority of the UK's current air launched weaponry is procured from the USA and can be regarded in general terms as Commercial Off-The Shelf (COTS) items. The T&E activity on such procurement programmes is generally limited to safe separation and interfacing to the UK's launch platforms. This in turn limits the work carried out upon the UK's T&E capabilities resulting in an utilisation downturn of expensive and often bespoke T&E assets. When this procurement approach is coupled to multi-national collaborative ventures and a need to demonstrate profitability under the PPP rationale a question over the sustainability and future requirement of such facilities is raised periodically. The argument over maintaining these facilities is largely driven by the political arena and is outside the scope of this thesis; it is raised here to purely provide additional context.

Though modelling and simulation has replaced the greater part of T&E there is still a need to verify the theory or to replicate and understand any deviations from the ideal. Environments such as the near field turbulence around airframes are difficult to predict and model so real-world separation trials must be executed to ensure the safety of the airframe and correct functioning of the separation mechanism. Furthermore, aircrew are being asked to serve in many theatres around the world and it is only through live weapon practices at

the Ranges that they develop tactics and hone their skills to minimise collateral damage and optimise the probability of achieving their mission objectives.

In addition to offering specific T&E services the Ranges are developing further capabilities alongside the needs of the customer base. A more synergised approach to the operational management of the sites and the customer base allows the creation of battle space environments using both combined forces and multi-national deployments. To further augment the training afforded to the country's military, and to deliver a 'value added' facet to what the Ranges can deliver QinetiQ are developing methods of combining data from both real and synthetic sources. The resulting picture offers battle space commanders with an augmented picture of all possible deployable assets combined with the ability to develop new strategies in a relatively benign environment. Such battle spaces can be augmented with state of the art electronic warfare, UAVs and UCAVs where participants can practice in a carefully controlled, monitored, but relatively realistic, environment.

Formatted: Bullets and Numbering

2.4 Integrating the Air Ranges.

Though QinetiQ has a 25 year contract (LTPA) to manage the Range facilities on behalf of MoD it is subject to clauses designed to ensure that the capabilities and facilities are evolved and morphed to maintain alignment with technology advancement, defence doctrine, and of course, effective cost management.

Many practices in use on the Ranges today are the result of a bygone era which include, but are not limited to, archaic technologies and military protocols. Though essential during the formative years of weapon research and development, these systems now appear candidly onerous, arduous, illogical and even Herculean when compared to the modern lean way of thinking and executing business. The signing of the LTPA in 2003 acted as a catalyst for many business visions within both the investment and cost saving arenas. Given the relatively low individual utilisation of the Ranges the creation of an integrated Air Range operation would deliver business benefits to both the MoD and QinetiQ.

As weapon systems have become more intelligent and energetic, and battlefield operations have evolved to require a multi disciplined environment, then the concept of discrete and

individualistic Ranges has its limitations. Adopting a synergised and integrated approach to the operation of the Air Ranges would provide the UK with a greater capability not only for the military environment but also for any potential civil users.

The task of attaining a synergised operation is essentially one of '*change management*' and demands concepts for implementing change not only at a technical level but at a personal level for the individuals concerned and the teams that they serve within. The author was appointed as the *Synergy Delivery Manager* for the QinetiQ operated Air Ranges in April 2006, a role aimed primarily at aligning the processes and practices across the four sites. Having established that the business orientated facets of the operation were controlled and managed by corporate and regulatory processes (e.g. financial reporting, human resource management, procurement, etc.) the author turned his attention to the operational and safety related parts of the business.

Formatted: Bullets and Numbering

2.5 The Foundations for an Integrated Air Range Operation.

Effective change management requires planning combined with relatively sensitive implementation; above all it requires consultation and involvement of the people affected by the changes. The change needs to be understood and managed in a way that people can cope effectively with it; it cannot be 'sold' or forced upon them as this will often cause problems. Change in the majority is very unsettling; most staff find that change in itself creates insecurities and they find it deeply disturbing and threatening (Mullins, 2007).

Certain industries and disciplines have a high concentration of staff which require, or attract, highly reliable and/or dependable personality profiles. Ranges, as an ex-civil service department, are a classic example of such an entity. People with strong, reliable and dependable character profiles tend to find change very difficult to absorb whilst the change welcomers are generally not the best at carrying out work in a reliable and process led fashion. Additionally, it is often observed that a strong resistance to change is often rooted in deeply conditioned or historically reinforced cultures.

Whilst managing the *Synergy* project the author adopted an approach which involved and informed staff as progress was attained. The creation of small focus teams and the use of

Formatted: Bullets and Numbering

informal workshops enabled wide participation in the planning of any changes and created a sense of ownership and familiarity amongst those affected, right from the beginning. The workshops helped develop a collective understanding and was used as a springboard to further new ideas and solutions which were developed from within the affected areas.

2.6 Benefits from an aligned Air Range Operation.

To achieve both an effective and long term alignment of a pan-site trials management system all process owners, process users and stakeholders must play a constructive role in its evolution. The alignment of processes as a deliverable from within the *Synergy* project was seen as the first step in gaining true operational integration, i.e. in creating a positive interaction and co-operation from two or more sites which would produce a business enhancement.

A truly synergised approach to Air Range operations allows business objectives such as cost savings and resilience to be optimised. Under cost savings the business may benefit from the matching of staff numbers to activity requirements through the use of deployable, flexible and multi-skilled teams providing much needed resilience and facilitating the natural migration of best practices across the sites. Such an approach helps minimise the impact of staff turnover, especially within the more specialised roles, which are trials participative and demand real time skills. Lead times to recruitment may also be better managed under such a networked and harmonised environment.

In addition to the benefits delivered to QinetiQ and the MoD on the financial and business resilience axes, customers will benefit from an aligned approach. The ability to engage with identical structures, protocols and trials methodologies across the four sites will ease congestion, minimise lead times and avoid the current problem of varying standards of documentation submission from site to site. The use of common roles, titles and structures would clearly minimise customer burdens such as the need to familiarise themselves with any local protocols and/or nuances.

2.7 Previous Attempts at Alignment.

Formatted: Bullets and Numbering

One of the key stumbling blocks met during the execution of the *Synergy* project was that of apathy and negativity which was caused predominantly by the failure of a previous and remotely similar project called *Ranges Harmonisation*. This project was created in 2001 and quickly became a formidable task which grew beyond all sensible boundaries in the development and support of change across the sites. Whilst the *Synergy* project of 2006/07 was focussed upon the four Air Ranges, the 2001 project included the Air, Land and Sea environments; a total of 22 sites across three disciplines. The project failed miserably due to the fact that the facilitating team at the time lacked commitment, technical experience and any focus upon reality. The author was especially cognisant of maintaining a degree of realism whilst delivering the *Synergy* requirements.

2.8 Real and Tangible *Synergy*.

The prime and long term objective of the *Synergy* project was to deliver the foundations of a wider reaching change management project. The final output was the creation of a single document (*The Air Ranges Handbook*) complemented by an established working group which had eroded most of the long standing issues relating to the lack of communications and networking across the Air Ranges. The author is proud to say that the final outcome was a tangible document combined with a more congenial community which did much to aid the daily delivery of trials conduct.

Formatted: Bullets and Numbering

The changes that have been initiated through the *Synergy* project have affected not only decades of processes and methodologies but also the work culture of all of the Air Ranges. The current condition of process alignment and the delivery of a truly synergised Air Range capability is far from ideal but the most difficult part of change, the initiation, has begun. It is now for the management team at all levels to maintain the momentum created.

Having demonstrated through the *Synergy* project that many of the cultural boundaries could be relatively quickly broken down an opportunity arose to capitalise upon a technical investment which was being delivered at Aberporth. Both MoD and QinetiQ were conscious of the £9 Million investment in the Aberporth Trials Control System (TCS) during a period when the Air Ranges were suffering a downturn in demand. The author

believes that the utilisation of Aberporth is circa 50% whilst the Hebrides is around 40% (based upon a professional, personal and qualitative judgement in 2008). Such low utilisations combined with the fact that both Ranges conduct more or less the same activity and that some alignment in process had been achieved through the *Synergy* project led naturally to the thought of controlling one Range from another. By gathering the prime data from the instrumentation at the Hebrides and transmitting it to the new Aberporth TCS an integrated operation could be developed which could potentially deliver many operational and financial benefits.

2.9 A Fully Integrated Air Range Operation.

During early 2008 the MoD announced that QinetiQ should investigate all opportunities to integrate the trial conduct activities across its Air Ranges. Given the relatively low cost base of MoD West Freugh, combined with its resident small team of staff and relatively high utilisation, the site was removed from the investigative study. MoD Larkhill, given its geographical closeness to MoD Boscombe Down and low trials utilisation was naturally targeted as a site which could be campaigned, on an ad-hoc basis, from the latter as demanded by the customer. QinetiQ are in the process of finalising their proposals for an integrated Air Range operation which considers using the new TCS based at Aberporth to control trial activities at the Hebrides. This study was submitted to the MoD during the Spring of 2009.

The author has been involved in the development of the foundational safety argument for such an integrated Air Range operation. Whilst he has facilitated the early 'Brainstorming' and 'HAZOP' workshops in order to help identify areas of risk or technical concern, he has not been engaged by the integration project team on a daily basis. This system of working has allowed the author to maintain a degree of independency and offers opportunities to objectively peer review ideas and to constructively challenge any developments from within the project team.

The reality of the situation is that an integrated Air Range operation would have been very difficult to deliver if the *Synergy* project had not started the process of 'change management', especially within the socio-technical and cultural areas of the business. In

direct comparison to the movement of a heavy flywheel, overcoming the initial static state of inertia is the most difficult part of the exercise. Once change is commenced its perpetuation is relatively easier (Mullins, 2007).

2.10 The Author's Evolving Mindset.

The author was trained and qualified as an electronic engineer with relatively rigid ideas on what constituted 'real' engineering; predominantly those skills and components which fall easily into domains such as electrical & electronic engineering, civil engineering, aeronautical engineering and even chemical engineering to name but a few. The experience of managing a project such as *Synergy* brought a completely different perspective to his view of safety management in both specific and holistic terms. Safety management is very often pigeon-holed as a series of defining instructions or prescriptive and specific entities which are predominantly treated in isolation to the social or cultural interferences that they may be subjected to in both their immediate and wider environments. This new way (to the author) of thinking was spawned during the *Synergy* project but was greatly enhanced during latter studies within the *Systems Engineering* arena of his doctorate.

The following chapter looks in depth at safety cases and their construct from carefully defined guidelines which focus so much upon a rigid, predominantly mathematical, perspective which is so revered by the 'dyed-in-the-wool' engineers who so often produce them. What is clearly missing from the literature review on safety cases is a specific requirement to consider the human element of the system under scrutiny. Other activities that the author has been involved within over the past five years have included the UAV activities at *ParcAberporth* in West Wales. Civil manned aviation has included the human factors component for decades but it is still relatively weak within the UAV environment. It is only in recent years, and then only within the military (defence) environment, that some diligence has been given to the competence of operators and maintainers. Relatively recent safety cases for military UAVs used as targets within the author's working environment do demonstrate some awareness to competence and training but do not look at the complete process safety aspects of the system. It is this latter vacuum that has triggered the author to pursue the more systemic role that safety culture has to play in the maintained delivery of a safe operation irrespective of how robust the technical element of the safety case is.

Having ignorantly, though quite innocently, reviewed many safety cases as part of his working role within Ranges over the past decade, the author has reflected on how weak the overall safety argument has been due to the lack of demonstrable cognisance to the human environment and the wider system components. Experience, during his latter years, in UAVs (especially in the development of *ParcAberporth*) has provoked many ideas on the need to include components which convey the system's underpinning safety culture within any deliverable safety case.

The following chapters illustrate how the author has evolved his safety management thinking to include the cultural and human side within safety cases. His early thoughts and reflections upon what is required to underpin the integrated Air Range operation is contained within chapter five. Having reviewed the literature available on safety culture within chapter six the author discusses and reflects upon some of the key lessons learnt from the preceding chapters within chapter seven.

CHAPTER 3

An Introduction to the UAV Industry

3.1 Introduction.

Even a fleeting dip into today's current affairs will probably lead to either hearing or reading about military missions within Afghanistan or Pakistan which involve the deployment and use of UAVs. Within these environments they have been used for many years to identify and hunt down senior members of al-Qaeda and/or other alleged members of terrorist groups (Richards, 2009). Such highly technical platforms, with names like *Predator* and *Reaper*, are predominantly controlled, not by personnel in relative proximity of the activity zone, but by personnel located in America. Such vast and inter-continental operations rely heavily on satellite communication links and onboard sensors to locate, identify and even to engage targets from a varied arsenal of weaponry including Precision Guided Munitions (PGMs). Reports from varied intelligence sources suggest that some of the alleged terrorist organisations have been forced to replace their casualties with men who they have never seen due to the colossal and very effective ways by which these machines have impacted upon the battle grounds (Richards, 2009).

The underpinning logic of using such platforms is very clear. It is predominantly due to the absence of onboard human life. Without such an arguably weak component the platforms may fly long endurance flights, often across continents, without concern if they crash or are engaged by enemy forces. If a 'fatal' engagement occurs or the platform is subject to a critical failure there are no inhabitants aboard to either lose life or to be captured and used as political tools in any follow-up scenario. From a financial and purely material perspective the downing of an UAV is considered to cost a fraction of that involved in losing a modern manned military aircraft.

It should be noted that UAVs are not only optimally suited for the dangerous tasks of war but are also well suited for many civilian tasks where the activity may be seen as hazardous, monotonous, dull and even dirty; a sector which will become increasingly more important within the next few years (Richards, 2009). Though the military have quite a

long-established, extensive and varied requirement for UAVs the potential for their use within the civil sector is vast and almost holds no bounds. Civil applications may include geological surveying, crop spraying, border controls, pollution monitoring, maintenance and fault identification of power lines, remote monitoring of gas lines and even providing real-time situational awareness to incident commanders in the rescue services.

Given the aforementioned, the consensus of opinion from within the civil UAV industry suggests that the only limitations to their use is in the designers' imagination (Richards, 2009). Also of note is the fact that within this emerging market there are equal opportunities for both small and medium-sized enterprises as well as the large companies that dominate the present military UAV market (Richards, 2009).

3.2 Civil and Military UAVs.

Whilst there is a potentially massive market out there the ability to fly UAVs above our towns and cities is still not feasible. Whilst military UAVs are operated under many specialised government authorities and are justified by those authorities as being just, (predominantly as they are 'at war') the consequences of any unsafe activities, such as crashing on innocent bystanders, is deemed to be acceptable. In a non-war type scenario, such as over-flying a town on a simple pollution monitoring activity, any inadvertent occurrence such as a crash, which injures or kills an innocent third party, may be considered unacceptable, depending upon the tolerability of risk associated with the activity. The prime focus for any military UAV is that of accomplishing its mission; within the civil sector primacy falls almost uniquely to that of safety. Currently, the risk of any crash from a civil UAV must be as low as the probability of a crash from a manned aircraft (Richards, 2009). Within the UK, the control and command systems for a civil UAV currently needs to comply with CAA regulations and must demonstrate that it is sufficiently safe to operate; this therefore suggests that the platform must contain in-built redundancies such as the *quadruplex* systems utilised within modern fly-by-wire manned aircraft (Richards, 2009).

3.3 Current Civil UAV Operations.

UAVs have been flown in various environments across the world for many decades but never has the pressure to utilise them in a purely civilian and flexible role been greater. The success of recent military operations utilising UAVs has not only raised public awareness of their use but has offered excellent opportunities to prove their operational viability in both military and civilian applications. These opportunities have led to an increase in the demand to operate UAVs in a variety of applications, especially civilian, across the world. The current regulations for flying are purely focussed upon inhabited flight; there are no regulations in place which permit uninhabited flight in shared airspace within the UK.

In researching this topic and during discussions with representatives from the various national regulatory bodies the author found minimal information on the operation of UAVs outside segregated airspace. In summary, any UAVs flown outside segregated airspace were done under special task clearances (*one-off*) from the host government (diplomatic approval) or under the auspices of an operational environment during periods of military conflict. One exception to the above are those UAV operations carried out by Israel though the author would argue that the Israeli circumstances are very close to that of an operational theatre. In the UK, an example of an UAV flight under a special clearance occurred during the summer of 2005 when a relatively large UAV (*Hermes 450*) operated out of *ParcAberporth*, West Wales in support of the WAG's UAV public flying event. The operation entailed take-off and landing from *ParcAberporth* airfield, transiting through segregated airspace and further flying operations within the Aberporth RDA. This whole activity was sponsored under the auspices of a diplomatic clearance with the additional support of temporary operating instructions.

During any major conflict the current western doctrine is to establish air superiority and thereby control the air traffic environment. The resultant low volume of air traffic helps to minimise the risks caused by UAVs to third parties, especially civilians; the consequences of any incidents occurring during such conflicts can be offset by the contextual argument of being at war; *the lesser of two evils.* Such benign operational conditions create a somewhat false sense of security and optimism of the risks involved in the operation of an UAV system. This lack of information on the risks and consequences involved during UAV

operations has yet to be fed back to the greater part of society; especially those who are proactively driving their usage forward. The majority of UAV development has been conducted in the USA where such systems can operate over very large and sparsely populated land areas (predominantly deserts) where the risk to third parties is small enough to be tolerated. Due to the fact that UAV development has been virtually wholly driven by the military the wider reporting of any occurrences such as the loss of control or casualties resulting from incidents such as crashed landings are not freely available. Though there are many sources of information pertaining to current UAV flight operations they are either not pertinent to this thesis or do little to support the safety argument for civilian UAVs.

Many articles are freely available which discuss the many and varied requirements for UAVs to have the ability to 'sense and avoid' and therefore carry out manoeuvres to maintain safe separation from other aircraft as currently demanded and exercised by the manned aircraft sector. This thesis will not discuss these requirements or abilities any further. Whilst the 'sense and avoid' issues are valid and an essential component of any UAV safety case the author does not plan to address such a massive component within this thesis; the requirement is known, according to the current thoughts on flying UAVs in unsegregated airspace, but is outside the boundary for this work. This thesis and its SCET is based upon creating an easier route for small UAV manufacturers and operators to achieve a positive response from a regulatory type body for flights within a segregated environment. Such a segregated environment is considered to be that of a restricted or prohibited volume of airspace predominantly assigned to the conduct of potentially hazardous flying activities such as a T&E Range. It is perfectly feasible to further develop the SCET for flights outside segregated airspace where any bespoke and/or discrete safety argument for the 'sense and avoid' component may be inputted at the appropriate point. The author believes that the first civil UAVs that will be flown in unsegregated airspace will probably use an extensive quantitative safety assessment very much along the lines of a military UAV as the risks of damaging the industry's reputation, and therefore defer any advancements in the field, will be too great. The author also believes that the final decision on what approach will be taken will predominantly be a political one.

Flying has been extremely well regulated for decades but the fact that UAVs can be constructed and operated for a fraction of the cost of an inhabited air vehicle has drawn interest from civilian parties who are not familiar with the flying industry. Predominantly these parties are focussed upon business and the application of minimal cost, and therefore technology, to optimise financial gain. In direct contrast the formative years of UAV flying were virtually wholly driven by the military environment and the accompanying high level of regulatory and engineering methodologies with little or no concept of creating a cost effective solution. A complete step change in the approach to UAV development and operation is being forced by both the business environment and the market demands.

Formatted: Bullets and Numbering

3.4 Market Opportunities.

A study by the Teal Group in September 2006 (Gerold, 2006) predicts that the world market for UAVs will exceed $54 billion (USD) (£28 billion) over the next 10 years. Prime examples of this market growth is illustrated through the following examples; the US Army alone is looking to increase its current UAV count from 1,200 to 10,000 by 2011 whilst the UK has embarked on its *Watchkeeper* UAV Network Enabled Capability (NEC) which is worth £800 Million (Thales, 2004).

The CAA, in 2004, issued its policy for light UAV Systems (UAVS) where it predicted how the civil UAV market was to grow (CAA, 2004a). Within the document it highlighted three possible areas, identified in terms of mass and altitude capability. These were;

- High Altitude Long Endurance (HALE) operations;
- Medium altitude applications primarily based upon extant military platforms such as *Predator*;
- Local operations at low altitude using light UAVs for inspection and surveillance using miniature payloads.

Out of these potential areas for development the least restrictive in terms of technological advancements was that of the light UAV applications where early platforms had already been developed by many organisations. A survey of existing UAVS worldwide indicated that a large proportion (79%) of those employed in purely civil, research, or combined

activities (military & civil) were focussed on this market. Indicators suggest that this trend is to continue well into the foreseeable future.

The current aerospace industry market is worth circa £20 billion per annum to the UK but a displacement of 5% into UAV systems over the next 5 to 10 years would create a new market worth in the region of £1 billion per annum (Clott, 2005). Specifically it is the emergence of a civil UAV market which will revitalise the UK's aerospace industry as well as a variety of associated technology sectors including sensors and data links (La Franchi, 2005). In 2004 the WDA invested £21 Million to create an UAV Centre of Excellence at *ParcAberporth,* adjacent to the MoD Aberporth Range capability (SBAC, 2005). The 50 acre facility and infrastructure has the ability to support up to 1,000 jobs and aims to attract technology leaders for the development, testing and evaluation of both UAVs and UCAVs in both unrestricted and restricted airspace (e.g. Range Danger Areas).

All military registered UAVs must follow a very robust and well recognised regulatory and airworthiness route which has been in operation for many years. The civil regulation of UAVs is yet to be established. Work carried out at *ParcAberporth* in recent years has established who the key shareholders are and has identified some of the principal areas, predominantly regulatory, which must be satisfied before a formal regulatory and licensing route can be established. Herein lies an opportunity for the SCET of this doctoral project to be used to support and facilitate the operation of civil UAVs.

The author is not suggesting that the SCET will in itself be the answer to all safety case problems but will offer opportunities and direction for potential UAV systems to be assessed in an holistic manner by taking a more systematic approach. Many low cost and low technology UAVs are currently being developed and it is these smaller companies which need support at the early stages of safety case design. These organisations are predominantly low business scale/low budget organisations who cannot afford to conduct a full scale safety assessment and analysis of their vehicles. Quite often, such systems use COTS component parts which have a limited engineering integrity and would be extremely difficult to qualify using quantitative safety tools. The author's experience of such

approaches would suggest that safety engineers are easily drawn to err on the side of optimism in assigning failure modes and probabilities to such low integrity components.

3.5 The Author's Involvement With Civil UAVs.

The author has many years experience of working with military UAVs used as targets and aerial laboratories within the T&E environment. In more recent times the author has participated, in part, as an operational, regulatory and safety advisor on a working group at *ParcAberporth*. This role has been primarily focussed on supporting the WWUAVC with establishing an effective airspace management policy which conforms to the regulatory requirements of both MoD and the CAA.

The author was involved in the creation of the first ever civil sponsored segregated airspace environment during 2007. This has personally engendered a great deal of interest in the safety management of those UAVs which do not fall under the auspices of any clearly identifiable regulated management system; these are almost exclusively those civil UAV systems which fall within the 150kg class.

3.6 Civil UAV Regulations and Certification.

One of the prime problems that many of the working groups and industry leaders are stumbling over is the regulatory side of civil unmanned flight. Whilst the regulations require the UAV's system to be "as good as a pilot" there are no clearly identifiable specifications for what this means, and how to replicate it with electronics (Richards, 2009). This statement by Richards (2009) directly relates to the CAA's civil UAV airworthiness certification standards guideline paper (CAA, 2002a) which suggests that civil UAVs will be required to qualify for certificates of airworthiness through demonstrating compliance with extant airworthiness standards derived from those applied to civil manned aircraft (CAA, 2002a). The CAA has chosen this stance in order to provide the public with the confidence that civil UAVs will present no greater hazard to third parties than manned aircraft (CAA, 2002a).

Whilst the UAV designers, manufacturers and operators must understand the requirements of the regulators the regulations themselves have been written, and evolved, for manned flight. There are currently no UAV-specific regulations in place, especially for crucial events such as last-moment collision avoidance which is required of manned systems (Richards, 2009). In manned systems this functionality is performed by the on-board human sensor who will take a pro-active approach to collision avoidance; this is linked to the primeval action of self-preservation.

Some guidance is offered to the environment through publications such as the CAA's CAP 722 where regulatory judgements may be made on a case-by-case basis. Whilst being relatively basic, these guidelines are subject to constant scrutiny and evolution as various learned working groups and research programmes agree and sign-up to any advances which may bring about some mandatory and more specific regulations.

In addition to the regulatory regime that must be created to allow UAVs to fly there is a need, as per manned flight, for the vehicles themselves to be certified as fit for purpose. In a similar manner to the regulatory issues, unmanned air vehicle certification is subject to the same degree of pitfalls and lack of formality. Whilst the CAA have issued some guidance in the guise of CAP 722 the generalised approach for any UAV which has a mass less than 150kg is for it to be treated as a recreational model aircraft. It is this gap within the industry which acted as one of the prime catalysts for the author to pursue the research question and therefore the creation of a SCET. It should be duly noted that the author has not explicitly consulted with the small and medium enterprises, who are actively involved with UAV development, manufacture and operations, during this research. The following text details the extant legal considerations and certification for small UAV operations.

3.7 Legal Considerations.

As a signatory to the Chicago Convention and a member of the International Civil Aviation Organisation (ICAO), the UK undertakes to comply with the provisions of the convention and the standards within its annexes; with the exception of any differences that it has filed to those standards (CAA, 2004b).

3.7.1 Policy.

Article 8 of the Convention states that no aircraft which is capable of flying without a pilot shall be flown, without a pilot, over the territory of a Contracting State without special authorisation by that State (CAA, 2004b).

3.7.2 Law.

European Country (EC) regulation has established the European Aviation Safety Agency (EASA) and makes provision for implementing the rules that deal with aircraft airworthiness certification, including continued airworthiness. Detailed requirements for these provisions are identified within two Implementing Rules. Certain categories of civil aircraft are exempt from the need to comply with the EASA Regulation and its Implementing Rules (CAA, 2004b). The exemptions which are of direct relevance to UAV activities are;

- Aircraft specifically designed or modified for research, experimental or scientific purposes and likely to be produced in very limited numbers.
- Aircraft whose initial design was intended for military purposes.
- Unmanned aircraft with an operating mass of less than 150kg.

3.7.3 UK Specific Regulations.

Within the UK there are two regulatory regimes, these being the military and the civil. Military registered aircraft, as specified by the Secretary of State for Defence, fall completely within the MoD's regulatory regime.

All other aircraft not classified as military, must, in accordance with the UK's aviation safety legislation, comply with its civil aviation requirements. There are no special provisions for those aircraft registered and/or operated by the police, customs & excise, or other similar services (CAA, 2004b).

The main civil aviation requirements are laid out in the Air Navigation Order (ANO) and the Rules of the Air Regulations. The provisions contained within these two documents

relate to many specifics such as operational rules, licensing and aerodrome regulations and are directly applicable to all non-military aircraft, organisations, individuals and facilities. However, whilst they are national requirements for certification and airworthiness they only apply to those aircraft which are exempt from the need to comply with the EASA regulations and rules. A non-military aircraft registered within the UK which is exempt from the EASA regulation and rules must have a certificate of airworthiness or a permit to fly issued by the CAA under the ANO (CAA, 2004b).

The ANO includes exceptions for 'small aircraft'; these 'small aircraft' are defined within the ANO as any unmanned aircraft weighing not more than 20 kg. Within this classification of aircraft, none of the preceding requirements are applicable; instead, a set of conditions are included at Article 87 of the ANO which allows flights to be conducted without complying to airworthiness, crew licensing or Rules of the Air. These conditions also include a prohibition on flight within controlled airspace or within aerodrome traffic zones unless permission has been granted by the air traffic control unit and that flights are limited to 400ft in height. Other conditions also apply for aerial work (commercial use) activities. It should be noted that these flying rules for 'small aircraft' have been predominantly developed for the purposes of regulating recreational model aircraft activities.

3.8 Exemptions for Civil UAV Flights.

An UAV which weighs more than 20kg, according to the ANO, is not classified as a 'small aircraft' and therefore all of the requirements highlighted in the preceding paragraphs must be complied with. If an UAV cannot comply with all of these requirements then the CAA may be prepared to issue an exemption under Article 127 of the ANO. To operate an UAV which weighs less than 20kg but more than 7kg for aerial work purposes requires specific CAA permission.

3.9 Certification of Civil UAVs.

Whilst it has already been stated that UAVs with an operating mass of less than 150 kg are excluded from the EASA regulatory and certification process the CAA, as the UK's national authority on aviation, has developed policies for general UAV activities. These

Formatted: Bullets and Numbering

policies apply to general UAVs, and cover their certification and standards. In addition to the aforementioned the CAA have issued a policy which predominantly addresses light UAV systems; these are predominantly line-of-sight activities and are restricted to flying within visual distance (500m) of the operator and at a maximum altitude of typically 400ft.

3.10 The Light UAV Policy.

This policy offers an alternative route for the CAA to grant exemptions to the ANO regulations as long as the UAVS meets certain specific criteria and is operated within those limitations stipulated by the CAA. Any intent to operate outside of these limitations must be formally discussed with the CAA.

Light UAVS exhibit many parallels to model aircraft used for recreational purposes. By reviewing the model aircraft world's safety record and their operating practices the CAA have concluded that a similar level of regulation may be applied to UAVS, provided that they exhibit no greater capability than the majority of the existing model aircraft fleet and are subjected to the same procedures and limitations applied to model aircraft (CAA, 2004b).

UAVS that are specifically designed or modified such as not to exceed the defined maximum speed and kinetic energy levels which are representative of the existing model aircraft fleet may be exempted from compliance under certain conditions. The applicable operating conditions and classifications are discussed in the following text.

3.11 Civil UAV Classifications.

Within the context of the CAA, and indeed for this thesis, an UAV is defined as;

> *'An aircraft which is designed to operate with no human pilot on board'*
>
> (CAA, 2004b)

There are several different types of UAV and subsequently various forms of classifications used by various organisations to identify them. The following two classifications are the most widely and formally applied;

Formatted: Bullets and Numbering

3.11.1 By Airspace Requirements.

For the purposes of airspace management the CAA and the MoD, through Joint Service Publication (JSP) 550 use the following classifications;

- **Group 1 -** Those intended to be flown in permanent or temporarily segregated airspace (e.g. Danger Areas) over an unpopulated surface (normally the sea following a 'Clear Range' procedure).
- **Group 2 - T**hose intended to be flown in permanent or temporarily segregated airspace (e.g. Danger Areas) over a surface that may be permanently or temporarily inhabited by humans.
- **Group 3 -** Those intended to be flown outside controlled airspace (Class F&G) within the United Kingdom's Flight Information Region (UK FIR).
- **Group 4 -** Those intended to be flown inside controlled airspace (Class A – E) within the UK FIR and the United Kingdom Upper Information Region (UK UIR).
- **Group 5 -** Those intended to be flown in all airspace classifications.

Whilst the above classifications are not used by the author within this thesis, the classifications have been included to provide additional context to the field of UAV operations. The topic of 'sense and avoid' was briefly discussed in preceding parts of this chapter and whilst it is not to be further pursued here it is noteworthy to point out that all related issues on the subject will need to be finalised before flights within Groups 3,4 and 5 are considered appropriate. Whilst the author is experienced with UAV flying activities within Group 1 he is of the considered opinion that the work of other bodies, and that of this thesis, would act as fundamental building blocks to allow UAV flying activities to occur within Group 2.

3.11.2 By Operating Mass.

Formatted: Bullets and Numbering

The following classifications, based upon the air vehicle's mass, is directly related to the CAA's Light UAV policy and the focus of this thesis; table 3.1 summarises these categories. This approach identifies 4 distinct categories;

- **Small aircraft** (< 7kg mass). These fall within the 'Small Aircraft' definition of the ANO and are exempt from most regulatory provisions.
- **Small aircraft** (7kg - 20kg mass). These again fall within the 'Small Aircraft' definition of the ANO and are excluded from the majority of regulatory provisions provided the operator does not act in a negligent or reckless manner so as to endanger person or property. This class of small aircraft has some additional operational constraints which are imposed to ensure adequate safety.
- **Small aircraft** (20kg – 150kg mass). For the 'Small Aircraft' which fall into this category the CAA have recommended that the Large Model Association (LMA) are engaged for their expertise. The CAA recommend that the LMA inspect and satisfy themselves that this classification of UAV has been designed and built to a representative and acceptable good practice. Following the granting of a CAA 'exemption for flight testing' the LMA will oversee a programme of demonstration of 'function & reliability' flight trials. Following a successful series of trials the LMA will recommend to the CAA that a renewable exemption is issued for operational flights.
- **Small aircraft** (> 150kg mass). The Light UAV policy does not apply to any 'Small Aircraft' which have a mass greater than 150kg.

Formatted: Bullets and Numbering

3.12 Applying the Light UAV Policy.

Whilst it has already been stated that the Light UAV policy is limited to civil UAVs which have no greater capability than the existing model aircraft fleet there is a need to effectively bound this requirement. Safety standards for model aircraft are established to address the risks to both third parties on the ground and also to other airspace users. The former is measured in terms of the UAV's kinetic energy upon impact whilst the latter is controlled

through compliance to the Rules-of-the-Air and the procedural avoidance of aerial collisions.

	Recreational Use	Commercial Use (Aerial Work)
< 7kg	'Small Aircraft' under ANO Art 129 • Minimum operational constraints. • No airworthiness standards.	'Small Aircraft' under ANO Art 129 • Minimum operational constraints. • No airworthiness standards
7 – 20kg	'Small Aircraft' under ANO Art 129 • Operational constraints required by ANO Art 87. • No airworthiness standards	'Small Aircraft' under ANO Art 129 • Operational constraints required by ANO Art 87. • CAA permission required under ANO Art 87 subject to and additional CAA limitations. • No airworthiness standards
20 -150kg	• Exemption required against ANO incorporating limitations from CAA. • LMA recommendation (or equivalent) in lieu of airworthiness standards.	• Exemption required including limitations from CAA. • Impact kinetic energy must be no more than 95kJ. • Airworthiness recommendation from an accredited body.
> 150kg	Not Applicable	Use of national operating rules or application of EASA airworthiness standards.

Table 3.1 – Summary of CAA policy for UAVS flying in UK airspace (CAA, 2004b).

3.12.1 Kinetic Energy Limitations for Light UAVs.

An UAV system eligible for consideration under the Light UAV policy must consist of a vehicle whose maximum kinetic energy upon impact on the ground does not exceed 95kJ. To attain rigid control over these energy limitations a maximum take-off mass of 150kg must not be exceeded whilst the vehicle's maximum sustainable speed, in level flight, should not exceed 70kts. These conditions have been chosen to maintain a degree of

equivalence with the model aircraft fleet and are based upon philosophies developed and discussed within the CAA paper 'Aircraft Airworthiness Certification Standards for Civil UAVs' (CAA, 2002a).

The aforementioned paper presented research from a wide range of aircraft varying from small scale platforms up to and including major commercial airliners. The research was predominantly based upon two scenarios; the first looked at an emergency landing under control whilst the latter looked at a complete loss of control. In the specific case of light UAVs, which are limited to an operating height of 400ft, it was deemed appropriate to select two scenarios; the first was a free-fall from maximum height (400ft) whilst the second would accommodate UAVs which could attain a relatively high forward velocity. For all fixed-wing aircraft a maximum impact speed of 1.4 times the maximum operating speed was chosen for the calculated kinetic energy limitations (CAA, 2004a).

The first scenario is akin to a 'free-fall' scenario and is designed to take account of an aircraft which has suffered a primary structure failure such as a fractured wing spa in the case of a fixed wing platform. In the context of a rotary wing platform the scenario covers the complete loss of power or separation of the main rotor. Additionally, in the case of a lighter-than-air platform the scenario encapsulates the possibility of a burst or detached gas envelope. The latter scenario takes into account the loss of control mid-flight such as flying out of radio control and achieving an optimal final terminal velocity at ground impact generated from maximum applied power and a gravitational component.

For an aircraft of mass 75kg which can attain a maximum level speed (V_{max}) of 70kts the calculated kinetic energy level at impact is 95kJ, using the 1.4 x V_{max} application. To ensure that a consistent application of hazard management was applied to all possible scenarios this maximum kinetic energy figure is also applied to the free-fall condition. The result is that a single maximum kinetic energy limit (95kJ) was published by the CAA which all Light UAVs must comply with (CAA, 2004a).

One of the benefits offered by stipulating a maximum kinetic energy level is that slower platforms, which are limited in speed, may be allowed to fly with a mass greater than 75kg. A mass of 80kg, if dropped from 400ft, exhibiting negligible aerodynamic drag will strike the ground at a terminal velocity of 95kts giving a calculated kinetic energy at impact, of 95kJ. Clearly, any object which exhibits a significant degree of aerodynamic drag, without reliance upon any in-built arrestor system, will have a reduced impact velocity and therefore comparable increases in mass may be allowed as long as the 95kJ impact energy maxima is not breached.

The following tables (Table 3.2 & Table 3.3), extracted from the CAA's Light UAV systems policy (2004a), show the relationships between mass, maximum operating speed and aerodynamic drag characteristics applied within the light UAV policy.

Mass of UAV in kg.	Maximum velocity in level flight ($V_{max.}$) in Kts.	Maximum impact velocity (1.4 x $V_{max.}$) in ms^{-1}.	Kinetic energy at maximum impact velocity in kJ.
60	70	50	76
70	70	50	89
75	70	50	95
80	68	49	95
90	64	46	95
100	60	44	95
110	58	42	95
120	55	40	95
130	53	38	95
140	51	37	95
150	49	36	95

Table 3.2 – Maximum permissible mass & velocity to maintain the 95kJ limit.

Mass of body in Kg.	Cross-sectional area of bluff body in m^2.	Kinetic energy at impact in kJ.
80	0 (Negligible Drag)	95
115	0.5	95
130	1.0	95
150	1.5	95

Table 3.3 – Relationship between the mass & cross-sectional area of a bluff body (with a non-dimensional drag co-efficient of circa 0.9) arising from the 95kJ limit.

3.12.2 Procedural Limitations to Avoid Aerial Collisions.

The previous text effectively describes, within the context of a quantitative analysis, why the operational limit on height is set at 400ft. From a qualitative, and probably more deep rooted perspective, the prime reason for opting for this operating ceiling is that of minimising any opportunities to cause conflict with other aircraft, predominantly manned. By restricting the lateral distances of flight to 500 metres the operator may perform the 'see and avoid' function and ensure correct handling of the aircraft at all times (CAA, 2004a).

For UAVs which are above 20kg, and within the 150kg limit (the third category), the CAA rely heavily upon the UK's LMA design and build standards; an organisation recognised by the CAA as being capable of providing expertise in the area.

3.13 Airworthiness and the Large Model Association.

The LMA have advised the CAA that it exists purely for the benefit of recreational model aircraft flying and does not offer any technical support to commercial UAV operations. Consequently, as a result of this declaration by the LMA, there is clearly a need to identify another competent body which will provide similar recommendations to the CAA on Light UAV systems.

In the absence of such a recognised competent authority the CAA accepts assurances from other learned bodies with related expertise in aeronautical engineering such as commercial aerospace companies and university departments. Until such a recognised body is

established the CAA will continue to assess each application on an ad-hoc basis; upon each occurrence the CAA will take account of the experience and knowledge of the operator and make recommendations, as appropriate, provided it is assured that the standards applied are as vigorous and demanding as those applied by the LMA.

3.14 The LMA Standards.

The LMA website was interrogated by the author during 2008 and 2009 to gain an insight into the 'regulatory' regime which is applied by the organisation to support its position as a competent authority for large recreational model aircraft.

The website is relatively specific in terms of the CAA's regulatory requirements for model aircraft which have a mass of over 20kg; it also points the reader towards contacting a single individual within the LMA for the appropriate advice. The first stage in gaining approval for flying a recreational model aircraft with mass exceeding 20kg is to ensure that an approved inspector is appointed to oversee the construction of the model. Information gathered during construction is used to facilitate the issue of a Certificate of Design and Construction by the LMA's Chief Examiner and Safety Officer (CE&SO). The issue of such a certificate allows the CAA to issue an exemption thus allowing the aircraft to be flown for test purposes in the presence of an LMA examiner or other approved person. During this exemption phase, which predominantly runs for one year, the aircraft will be flown by a named pilot and that all flights are to be recorded in a Flight Test Log.

Whilst the author believes that the current modus operandi is sufficiently robust for recreational purposes the lack of any referenced formal engineering practices on the website suggests that they may not be suitable for commercial UAV activities. This completely aligns with the LMA's stance but gives some cause for concern if the CAA believe that they are suitably competent for assessing non-recreational light UAVs.

CHAPTER 4

Safety Cases - A Literature Review

4.1 Introduction.

This chapter introduces the origins and requirements of a safety case, the prime legal drivers which are mandatory under government legislation and the application of typical rationales. This literature review also introduces and contrasts some of the established best practices which have been adopted by industries such as rail transport, aerospace, mining and nuclear power.

Formatted: Bullets and Numbering

4.2 Development of Safety Legislation.

On the 16 January 1862 the main structural beam of a water pumping engine at New Hartley Colliery, near Newcastle-on-Tyne, Northumberland sheared and fell into the only mineshaft and means of ventilation for the "*Low-Main*" seam. Hundreds of men tried, over a period of seven days, to rescue those who were trapped underground. Five men were killed immediately by the machinery, rubble and wooden liners as it fell down into the shaft and through their lift as they ascended to the surface. Another 199 individuals slowly suffocated from the lack of oxygen and the build up of gas over the coming days as the obstruction proved too heavy and awkward to move (Seymour, 2008). In total, 204 men and boys died. As a direct consequence of this accident new mining legislation was introduced in 1864 which stipulated that every seam, at every mine, should have a minimum of two access/egress points (Cullen, 1996). A comment from the Illustrated London News, 25th January 1862 sums up the impact that this event had upon the nation at the time;

'So dire a misfortune attended by such horror of circumstance is not recorded in the history of mining.' (McCutcheon, 1963).

At about 4:53 p.m. on Saturday 1st June 1974 a large cloud of a cyclohexane mixture ignited causing extensive damage and numerous fires at the Nypro (UK) chemical plant at Flixborough, Lincolnshire (HSE, 1975). Twenty-eight workers were killed on-site and

another 36 were injured off-site as a result of a badly designed maintenance modification and subsequent operational implementation to the plant's processing facility. Eighteen of the fatalities occurred within the control room where the roof collapsed and the windows shattered; not one individual escaped from it. The fires remained burning for many days and were still hampering rescue workers ten days after the initial event. The whole installation was severely damaged whilst a total of 1,821 houses, shops and factories were extensively damaged off-site. As a direct result of the Flixborough disaster, the HSE assembled a body of Subject Matter Experts (SMEs) to study the control of major industrial hazards and to give advice on best practice adoption. This body was called the Advisory Committee on Major Hazards (ACMH) (De Cort, 1994).

In 1976 a major environmental disaster occurred in Seveso, Italy, when highly toxic substances from a major pesticide manufacturing plant were released and caused the contamination of circa 2,000 hectares (≈ 5,000 acres) of land and the deaths of over 70,000 animals (De Cort, 1994). The UK's thoughts and policy were seen as major influencers on the direction taken by the Commission of the European Communities (CEC) when it subsequently introduced a directive (Directive 82/501/EEC; *The Seveso Directive*) for the control of industrial major accidents after reviewing a series of other major (preceding) accidents within the European community. These included the 1966 Liquid Petroleum Gas (LPG) explosion at Feyzin, France where 18 people died and a further 81 were injured (Lees, 1996); as well as the 1975 propylene explosion at Beek, Holland where 14 perished and a total of 107 were injured (Lees, 1996).

As awareness of the need to effectively manage the safety of major industrial operations with the potential for catastrophic failures grew then so did the maturity applied to the risk management process at both national and European levels. Both the Flixborough and Seveso incidents were deemed to be catalytic in the creation of various committees and subsequent directives which eventually resulted in the enactment of the Control of Industrial Major Accident Hazards (CIMAH) Regulations issued in 1984 (later evolved (1999) into COMAH – Control Of Major Accident Hazards, (De Cort, 1994)). This regulation required manufacturers of products which used certain dangerous substances to prepare a safety case which had to be submitted to the HSE. The safety case was intended

to show that any potential major hazard had been effectively identified and assessed and that adequate controls were provided for any residual risks (Cullen, 1996).

Though the Hartley Colliery accident outcome differed greatly from that of the Flixborough accident they can be used readily to illustrate how safety legislation has evolved and developed over the years. The colliery accident imposed a single, universal, but quite specific requirement upon mine owners to install a separate means of ventilation and emergency escape; the chemical plant outcome imposed a more general safety objective, the only specific condition related to the requirement for a safety case. Whilst the colliery outcome was decreed to be essential for every mine the chemical plant outcome indicated and recognised that major accidents are often the result of a series of coincidental events which have collectively realised their potential hazards (Cullen, 1996). Whilst "lightning never strikes twice" and "history is unlikely to repeat itself exactly" a need remained whereby any lessons learnt from such incidents could be used to mitigate and minimise the possibility of any future repeat occurrence.

Formatted: Bullets and Numbering

4.3 Health and Safety Law.

The Robens report on "*Safety and Health at Work*" was published in June 1972 and still remains the basis for the majority of the UK's extant Health and Safety legislation. Lord Robens was charged with the task of;

…reviewing the provision made for the safety and health of persons in the course of their employment (other than transport workers while directly engaged on transport operations and who are covered by other provisions) and to consider whether any changes are needed in;

- *the scope or nature of the major relevant enactments, or*
- *the nature and extent of voluntary action concerned with these matters, and*
- *to consider whether any further steps are required to safeguard members of the public from hazards, other than general environmental pollutions, arising in connection with activities in industrial and commercial premises and construction sites, and to make recommendations* (Robens, 1972).

Following the publication of the Robens report in 1972 the government, in 1974, passed the Health and Safety at Work etc Act (HSW Act) and created both the Health and Safety Commission (HSC) and the Health and Safety Executive (HSE). An additional and important component which was also created at the same time was a role for local authorities (LAs) to implement a new regulatory framework for workplace health and safety in Great Britain (HSE, 2004a).

The Act, which largely reflected the recommendations of Robens' report, introduced a non-prescriptive model which advocated the principle that "*those that create risk are best placed to manage it*". Up until the Act all of industry was managed through highly prescriptive and detailed regulations. A new era had dawned whereby a flexible system of goals, targets and principles, supported by codes of practice and guidance, would be used to deliver a proportionate, targeted and risk-based safety environment (HSE, 2004a).

As stated previously, the HSW Act established two new bodies, the HSC and the HSE. Their prime role was to effectively implement the framework that had been identified by the Robens report and to realistically deliver the requirements of the Act. The HSC first met in 1974 and remains responsible for preserving the health, safety and welfare of workers and the public who may be affected by any work activities. The Commission is responsible for proposing new laws and standards, conducting and directing research and also providing advice and information to anybody who requests such support. The HSE assists and supports the HSC with its activities but has specific responsibilities of its own; together with the LAs, the HSE is predominantly tasked with enforcing health and safety law (HSE, 2004a).

The new bodies offered an opportunity to amalgamate a largely fragmented array of policymakers and inspectorates to create an unified and wide-ranging health and safety entity. The future would now not only be focussed but would rely upon flexibility and "*extensive consultation*" (HSE, 2004a) to create legislation that was "*fit for purpose*" (HSE, 2004a). The model created relied upon the fact that the HSW Act had established a regulatory framework and that the HSC and HSE would deal with the details.

4.4 Evolution of the HSC and HSE.

Formatted: Bullets and Numbering

Since the HSW Act was enacted in 1974 the structure of Britain's industry has changed dramatically; manufacturing has taken a massive downturn whilst the service industry has risen greatly (HSE, 2004a). The number of small firms has continued to grow; 99% of all firms in 2003 were classified as small (< 50 employees) whilst 0.2% were classified as medium (50 to 250 employees) (HSE, 2004a). Small and medium sized firms now employ virtually 60% of Britain's workforce whilst over 70% of business enterprises in Britain have no employees (HSE, 2004a). In addition to these changes in workforce structure there have been changes in the composition of the work force. During the 1970s part-time workers made up a sixth of the total workforce whilst in the early 2000s they were reported as constituting a quarter of it. Women now make up 50% of the workforce whilst in the 1970s the female element of the workforce was less than 40%; the adoption by industry of the employment of temporary and contract staff, as well as more flexible working hours, as driven by the modern economy, has encouraged many of these changes. The change in work patterns and the increased use of migrant workers has also helped to catalyse and accelerate such changes (HSE, 2004a).

Prior to the HSW Act large numbers of British workers were excluded from the relatively limited safety offered by the sector-specific regulations; areas such as the self-employed, local government establishments, hospitals, schools and other sectors now fell under the control of the HSC. An immediate effect of the HSW Act was that a further 8 million employees were afforded health and safety protection overnight. Shock and disbelief reverberated through industry as the self-employed, designers, manufacturers, "*anyone affected by work activities*", had duties of care placed upon them; they now had to take ownership for their actions and/or ignorance. In summary, they now had criminal liability added to their extant civil liability culpability.

As time has progressed the responsibilities of the HSC have expanded into various new arenas as it has been obliged to deal with new issues and/or to investigate major incidents such as the Piper Alpha oil installation accident, the Clapham train crash and the King's Cross fire. Following such incidents the regulatory aspects of the specific areas were transferred from the various government departments (e.g. Department of Energy (DoE),

Department of Transport (DoT)) to the HSC. These changes were driven not only by the need for regulatory independence but also by changes in the work environment, the emergence of new risks, advancements in technology (e.g. nanotechnology) and also a step change in society's perceptions and demands of risk acceptance (HSE, 2004a).

The public's attitude to the regulation of risk has changed considerably since the HSW Act was passed in 1974. In the past there was a degree of fatalistic acceptance of accident causation whereas today many who are caught up in the occurrences, even in the periphery, call for inquiry, accountability (blame) and even financial recompense. Additionally, the aggrieved show an element of distrust in the opinions of SMEs and demand a consolidation of assurances that any control mechanisms are robust and 'fit for purpose'. The HSE's long term view is for health and safety to be developed and acknowledged as a "*cornerstone of a civilised society*" by encouraging the HSC, the HSE and the LAs to work in unison (HSE, 2004a). Such an approach would help to nurture, establish and maintain an effective and realistic safety culture so that both the employer and the worker would take complete ownership of the issues raised. The Robens Report is about managing risks in a practical, realistic and reasonable manner and not to try and remove them completely; to maintain such an outlook on safety it is the individuals who work within the environment who are best placed to manage and control those risks.

In April 2008 the Department for Work and Pensions (DWP) announced that the HSC and the HSE would merge to form a single national regulatory body, responsible for promoting the cause of better health and safety at work. The merged body would be called the Health and Safety Executive (HSE) and would provide greater clarity and transparency whilst maintaining its public accountability (HSE, 2008b).

Formatted: Bullets and Numbering

4.5 Introduction to Safety Cases.

Modern systems, especially safety related systems, are continually evolving in complexity as technology both allows and demands more integration; as sub-systems are integrated to create more intricate structures then so the intra- and inter-dependencies grow. This approach is also bolstered by established "*systems thinking*" (Hitchins, 1992) whereby every sub-component or sub-system must be designed and operated to link holistically into

both the immediate and extended environment. Whilst such safety related systems are developing in one direction the environment of regulation and standards is growing in another; such highly integrated, complex and often critical systems require much more detailed, comprehensive and exhaustive analysis. With this in mind it is clear to see how the task of creating a modern safety case for an integrated system (of sub-systems) is becoming very onerous; they are becoming time consuming to produce, costly and very difficult to manage. From personal experience with the reviewing of safety cases related to weapon systems, UAV systems and major capabilities (T&E Range Safety Case) the author would suggest that as the complexity and magnitude rises then the ability to understand the causal paths and any reactionary effects of any changes from the base condition diminishes. The "*beast*" can become unmanageable.

Safety cases usually form a component part of a larger and holistic Safety Management System (SMS) (MoD, 2004) which address elements of a major project such as (non-exhaustive);

- The overall strategy for managing safety within the project.
- The definition, allocation, identification and responsibilities of key safety related components including final 'sign-off' authority.
- The interfacing engagements with any other SMS or sub-systems.
- Training and/or competency requirements of any key personnel involved with ensuring delivery and/or compliancy.
- Arranging for feedback, in various forms such as incident reports and near miss occurrences, to be appropriately and effectively managed and acted upon to ensure continuously safe operations. (Such feedback would use the extant Safety Committee, part of the overall SMS, as a formal conduit for continuous safety monitoring.)

Another important pre-requisite of a robust safety case is that of a '*systems*' approach (Hitchins, 1992, p255 and Sage, 1992) where safety must be considered as an intrinsic part of the overall project and not as a separate entity (MoD, 2004). This is especially so within large and complicated projects where poor safety management can result in quite

significant risks to the project's final delivery. An omission of cognisance and/or compliance to safety during the project's conceptual phase may not be easily recognised until very much later when key and costly decisions have been made and implemented. Applying corrective actions at such a late stage may be costly, embarrassing and even impossible in some highly regulated and safety critical industries. The author cites an example from within his industry to illustrate such an issue.

During the 1990's a decision was made by a UK defence related project office to opt for a financially cheaper Flight Termination System (FTS) to be integrated within a new surface to air missile system for use by the UK military. This decision was based not only upon delivering cost savings but upon a limited amount of safety related information offered by one small part of the project team. This safety information was appropriate for the early developmental stage of the project as it was to be trialled at an European T&E capability. As the project matured and more extensive T&E trials were to be conducted at UK locations then so the limited and inappropriate safety system was embarrassingly uncovered; the project had developed and matured so much that re-engineering its FTS was considered to be too costly. In a wider context and with much embarrassment, having been delivered to the UK's military, the system could not be fully exercised during peacetime within its own UK-based capabilities. Hence, any doctrinal requirements and practices afforded to the new weapon system would now have to be conducted in an un-instrumented part of the world (wasteful and un-productive) or in a foreign nation's test facility.

Formatted: Bullets and Numbering

4.6 Purpose of Safety Cases.

The *raison d'etre* of a safety case is to identify, assess and mitigate serious risk (Haddon-Cave, 2009, p259). A safety case (generically) is a thorough and proficiently assembled argument, supported by a body of suitable evidence, that a system is acceptably safe (safe enough when compared against a definition or notion of tolerable risk) to operate within a particular context or environment (Despotou & Kelly, 2004). Safety cases have been adopted across many industries, especially those where risks (and subsequent consequences) are predominantly greater and the argument for safe operation cannot be wholly argued by a simplistic quantitative approach. Examples of industries which

currently utilise safety cases in a similar context include railways, aerospace, defence, nuclear energy and offshore oil & gas.

Safety cases should be seen as an effective means for communicating concepts, methodologies and information to third parties such as the general public and regulatory bodies. It should be noted that having created a safety case the author(s) may be required to justify the safety argument, often within a court of law, if an incident subsequently occurs. The body of work underpinning the safety case on these occasions may need to be defended and the rationale explained. The safety case concept may refer to or include anything from software configurations or physical items of engineering through to a series of work instructions or even strict operating procedures.

Safety case reports are predominantly large and complicated pieces of work (Kelly, 2001) which convey to the reader how a complex system, quite often covering many disciplines, is argued to be safe. From both research and personal experience such safety cases are seldom created by single individuals; they are predominantly assembled by a team of specialists, each bringing a different and valued perspective to the overall output. Quite often such teams may not be co-located or work within the same organisation.

Formatted: Bullets and Numbering

4.7 Definitions.

There is no recognised or definitive statement of what a safety case should be composed of but there are many variations across many industries of how a safety case should be presented and what components should be included within it. (Wilson *et al*, 1995). Though safety case definitions differ slightly from one environment to another the fundamental concept remains the same;

"*…a safety case should communicate a clear, comprehensive and defensible argument that a system is acceptably safe to operate in a particular context.*" (Despotou & Kelly, 2004, and Kelly, 1998).

This rather generalised definition reinforces some of the key issues that must be considered when creating any safety argument for a system; the emphasis should be placed on the fact

that it is to be used to effectively convey an argument. It is used to demonstrate how an individual (or body of individuals) can reasonably conclude that a system is acceptably safe from the evidence presented.

Formatted: Bullets and Numbering

4.8 Contents of Safety Cases.

A safety case should consist of three principal elements (Despotou & Kelly, 2004);

- Safety Evidence.
- Safety Argument.
- Safety Requirements & Objectives.

Evidence is any information which indicates whether a belief or proposition is true or valid (facts). These could be based upon established scientific principles and/or prior research. In the context of safety cases, evidence may be in the form of assumptions which are necessary to bound a condition and to facilitate the creation of an argument.

An argument will communicate the relationship and rationale between the assembled body of evidence and the overall objectives of the safety case. An argument without any supporting evidence is unfounded and is therefore not convincing; in a similar manner, evidence which has no supporting argument is unexplained and therefore may not convey that the safety objectives have been met. It can therefore be appreciated that both the evidence presented and the argument must be aligned for credible delivery against a safety requirement.

The actual form of the argument and any inferences made in the causal links can vary as a function of the system's design and/or safety case strategy (Bishop & Bloomfield, 1995). Arguments may be delivered in many ways, the following documents four different industry established and acceptable methods.

4.8.1 Deterministic.

Formatted: Bullets and Numbering

The evidence offered may be in the form of axioms where an accepted statement is regarded as being self-evidently true. The inference mechanism on such occasions relies upon the rules of predicate logic whilst the argument is a function of using those rules. An example from the author's working environment is where a missile has insufficient energy (e.g. fuel, height, launch airspeed, aerodynamic abilities) to breach a maximum energy boundary; hence proof of launch speed, aerodynamic modelling and rocket motor energy is required as evidence that an unplanned hazardous event is incredible. Such evidence may require explicit validation (especially those concerning modelling) or an independent review of the formalised argument.

4.8.2 Probabilistic.

Formatted: Bullets and Numbering

The evidence offered may be based upon or adapted to a theory of probability; such an approach involves chance variations. The evidence could be in the form of a sub-system or component failure (e.g. Mean Time Between Failure (MTBF) calculations) and the inference mechanism for the argument would be the statistical analysis conducted to support the argument.

A probabilistic argument often combines qualified estimates of a system's parameters to support a high level event/goal such as a catastrophic event or dangerous occurrence. Statistical analysis in support of the argument may include Bayesian networks, basic statistical analysis, established approaches (human failure predictions) or stochastic models such as Fault Tree Analysis (FTA). Probabilistic arguments not only look at the discrete sub-components of a safety case but also look at the underlying model of system behaviour and the intra-relationships which percolate between and across the various forms of evidence.

One form of the probabilistic approach which is currently very much in vogue, certainly within the aerospace industry, is that of the Quantified Risk Assessment (QRA). QRA is a very valuable tool, especially when there are many uncertainties within the environment though the secret in its constructive and realistic use lies in striking a balance between it

and good engineering judgement (Wilkinson, 2002). QRA is further explained in more detail at 4.11.

Formatted: Bullets and Numbering

4.8.3 Qualitative.

This approach can be very subjective as the evidence offered to support such an argument may be as intangible as stating that a certain standard has been adhered to or that expert guidance has been sought. The inference mechanism may be constructed from a form of validity or approval process agreed from such concepts and policies.

Qualitative arguments are extremely important to safety cases; whilst many purists advocate the binary form of arguing safety through a quantitative approach the more subjective and often intangible qualitative approach also has its benefits. Qualitative assessments are often scored or categorised using terms such as “good”, “indifferent” or “bad” (Bishop & Bloomfield, 1995) by using expert judgement and/or peer review. If the system or sub-system being reviewed is to be subjected to, for example, a compliance regime or conformance to a certain standard then its acceptance can be binary in nature. The use of a “tick-list” to demonstrate acceptability is a prime example of a binary qualitative argument and is especially valid if designed and constructed upon previous work which has a proven heritage for delivering the required level of safety (Bishop & Bloomfield, 1995).

In reality it is extremely unlikely that a safety case will be constructed using an entirely deterministic or probabilistic approach. Overall, the safety case may consist of numerous arguments and claims relating to the many ‘sub-components’ of the total system but these may not necessarily be in the same approach. Additionally such deviations in the approach may be a function of the hierarchical order within the system as well as the most befitting or suitable argument to use for the sub-component (sub-claim) (Bishop & Bloomfield, 1995).

It is also important to recognise that safety cannot be argued to be acceptable or not without any consideration to the application of context (Despotou & Kelly, 2004). Any system may be considered as unsafe if applied to, or operated within, an unsuitable or inappropriate

context. One of the major tasks that befalls a safety case is that of the provision of context for the argument. It is quite self evident that any system may be accepted as being unsafe if used outside its design parameters or is used in an inappropriate manner; by explaining within the safety case how the system is to be operated the argument may be contextually bounded.

As the safety case matures and evolves through its various lifecycle stages the safety argument is decomposed into smaller and clearer entities which reflect the author(s)' understanding of the system(s) in question. During the preliminary stages of the project life cycle the argument may be extremely limited; this will therefore be reflected in the use of high-level objectives within the safety case yield. As progress is made and the project matures then so the level of safety knowledge grows allowing the argument to be expressed in ever increasing realistic and definitive terms.

Safety cases should be clear, logical and free-flowing throughout. Quite often additional contextual information can be provided through the use of a more qualitative approach; the use of an extended textual account quite often provides the 'mortar' that holds the main quantitative 'block work' together. Without such a textual input much of the argument can be lost leaving third parties questioning if the objectives have been fully met or worse still that an argument is seen to be weak when challenged following an incident. One of the major requirements of a safety case, especially for projects which are complicated, emotive, and at the periphery of social acceptance such as those within the defence and aerospace environments, is that any textual content is clear and concise. It should be duly noted that in the event of an incident, especially one which involves a fatality, the safety case may be scrutinised by a court of law and the information contained therein will be reviewed by both other expert witnesses and a broad cross-section of the public. Delivering a clear, concise and unambiguous argument is therefore very important in such circumstances.

The overall approach taken by the author(s) of a safety case must ensure that all parties are agreed on a common theme and route to achieve the final objective. Any misalignments will create inefficiencies and ultimately a weakened safety case which cannot stand up to a rigorous and bona fide challenge. One of the most difficult issues to overcome in the

creation of any safety case is that of ensuring that all stakeholders involved in the process have a similar understanding of the overall safety argument (Despotou & Kelly, 2004). In the absence of such a consolidated and shared approach the management of the safety case becomes quite onerous and ownership of any safety issue may become diluted. Various tools have been utilised by many industries to help define, express, present and manage safety arguments. These are further discussed within this chapter.

Formatted: Bullets and Numbering

4.8.4 Established Good Practice.

In addition to the use of quantitative and qualitative tools (as discussed in the preceding text) it is also acceptable to apply relevant and established good practice in the demonstration of risk management and its reduction to the required level (HSE, 2006a). Good practice may change over time due to increased understanding or changes in technology and the criteria for such approaches and the application of such evolutions is set out within the HSE's guidance upon the concept of 'As-Low-As-Reasonably-Practicable' (ALARP). ALARP is further discussed within this chapter. In situations which are considered to be unusual, exceptional and appropriate, such as that of the T&E Ranges, the use of authoritative good practice can be considered to set the risk benchmark. Whilst good practice informs, it does not constrain or substitute the need for professional judgement. In the case of this project the author has had access to many safety and operational subject matter experts which have given opportunities to create a safety case which can be assembled not only upon quantitative foundations but also utilises a professional qualitative approach, drawing upon professional judgement in a truly holistic and systematic manner. This approach draws upon many of the principles which are so vigorously advocated in today's systems engineering environment.

Formatted: Bullets and Numbering

4.9 Communicating the Argument.

Existing approaches to convey safety arguments are varied; like other environments there is a need to pick the most appropriate tool for the task. This section of the chapter investigates those approaches which have been utilised for communicating the safety argument; it concludes with a relative in-depth look at Goal Structured Notation (GSN) which is currently heavily used in the author's industry.

4.9.1 Free Text.

Formatted: Bullets and Numbering

Early safety cases, predominantly for relatively uncomplicated organisations and/or projects, relied heavily upon the use of textual narratives to convey the safety argument to the reader. The approach relies upon the use of clear, concise and well structured English language to convey how a safety requirement is interpreted and achieved within a system (Kelly, 1998). When correctly used it will not only describe the higher level safety requirement but will effectively reference the supporting evidence which underpins it. Such an approach for expressing safety arguments may be very effective but can show its limitations when applied within certain environments.

Safety cases are predominantly written by engineers who, by default and circumstance, tend not to be highly polished in the use of the written word; (though the author accepts that there are exceptions to this subjective and rhetorical view). For this reason, the meaning of any text, and therefore the structure of the safety argument may be confused and appear irrational. Another limitation of the free text approach which is prevalent and valid at the current time is that due to the creation of highly complicated "*systems of systems*" which are created as a result of technology growth and integration. As the number of supporting evidential elements grow within the more complicated scenarios then the number of cross-references within the text become more awkward to the point that the flow of the argument becomes disjointed and disrupted.

4.9.2 Tabular Presentations.

Formatted: Bullets and Numbering

Kelly (1998) highlights the fact that tabular methods were first used within the Safety of Hazardous Industrial Processes (SHIP) project (An European Union (EU) Environment Programme to define an approach to assuring safety despite the presence of design faults). The approach relies upon the creation of a table of three columns (Kelly, 1998);

- Claim (The overall objective of the argument)
- Argument **(**Descriptor of argument given in support of the claim)
- Evidence / Assumptions **(**Evidence or Assumption to support the argument)

From a positive perspective this form of structuring a safety argument is extremely simple and, when compared to free text, is easy to demonstrate the argument in its decomposed state. It is this simplistic method which ultimately limits the use of tabular structures to the uncomplicated arguments; i.e. tabular structures make it possible for just two steps to be recorded in the decomposition of any argument;

'Claim' → *'Argument'* → *'Evidence'* / *'Assumptions'*

Where arguments are complex and/or when a single *'Claim'* is supported by many strands of *'Evidence'* or *'Assumptions'* the text within the *'Argument'* column must be expanded to allow the argument to be communicated fully. Another option is that of breaking the argument down into smaller sub-components and further decomposing them in other tables. Despite attempts to use good argument descriptors or cross referencing techniques both options can lead to a rather disjointed argument which suffers from a lack of clarity and flow. Despite much research by the author there is minimal guidance available on how to formally approach and document the information for tabular safety arguments.

Formatted: Bullets and Numbering

4.9.3 Claim Structures.

Claim structures are constructed by fusing together a number of argument claims through the use of AND and/or OR gates; where OR gates are used to indicate an independent form of argument. The overall claim for the system under scrutiny is decomposed by using a hierarchical technique until foundational or *undeveloped* claims are reached. The foundational (or *base*) claims are supported by evidence though their role is not shown diagrammatically within the structure.

Claim structures have been used by the MoD to present process safety arguments in the development of processes such as the Ship Helicopter Operating Limit Instrumentation System (SHOLIS) project (Kelly, 1998 & MoD, 1997b).

There seem to be some synergies between the use of claim structures and goal structures; Kelly (1998) suggests that there is evidence that GSN has had an influence on the claim structures methodology. Claim structures are typically abridged versions of GSN which do

not express the arguments of the over-riding strategy in any enrichened form; they rely wholly upon the binary outputs of the AND & OR gate methodologies. By using such a simplistic and stark approach their arguments often suffer from a lack of context, reasoning and justification. Again, despite much research by the author, there is minimal guidance available on how to construct and apply this form of safety argument.

Formatted: Bullets and Numbering

4.9.4 Bayesian Belief Networks.

Bayesian Belief Networks (BBNs) provide a means to communicate claim intra-relationships within a safety argument (Kelly, 1998). BBNs do not explicitly present the claims, they communicate the safety argument implicitly; the '*belief*' in the argument is created by the conditional probabilities associated with the information contained within nodes and the arcs which join them. BBNs are also known by other terms such as; Probabilistic Cause-Effect Models, Probabilistic Causal Path Models, etc. BBNs, when applied to safety arguments, are graphical diagrams which help to communicate the probabilistic causal relationships which exist between the argument's variables. Nodes, which contain text represent variables whilst arcs between the nodes indicate a causal dependency between the variables. Conditional Bayesian probabilities are used to express the beliefs in dependency between the differing variables. Figure 4.1 shows an example of a BBN. Within the example a relationship is revealed between the ability of a tracking radar's operator to track a missile in flight and his competency & training, the weapon's flight profile and the equipment's tracking capability.

BBNs are very good in constructing a safety argument by allowing causal relationships to be identified between both qualitative and quantitative safety elements. In a similar manner to fault tree analysis they yield and contain important evidence which can be used to qualify a quantitative claim within an argument. This quantitative derivation offered by BBNs is extremely useful when trying to predict the value of variables based upon uncertain or unqualified data such as human error and/or equipment functional failure (in the absence of technical data). As with many other predictive type approaches, one of BBNs weaknesses lies in the derivation of the conditional probabilities and its use to reveal the degree of causal interference between the different variables. From the author's experience of developing Range Safety Cases using causal path analysis identifying the

probabilities can become very subjective and arduous, especially when the forum is formed from a varied background. In the case of the more subjective variables the BBN model can be re-visited periodically if and when qualified data becomes available (true further technical analysis and/or historic trend analysis) and the overall conditional probabilities improved to align with reality.

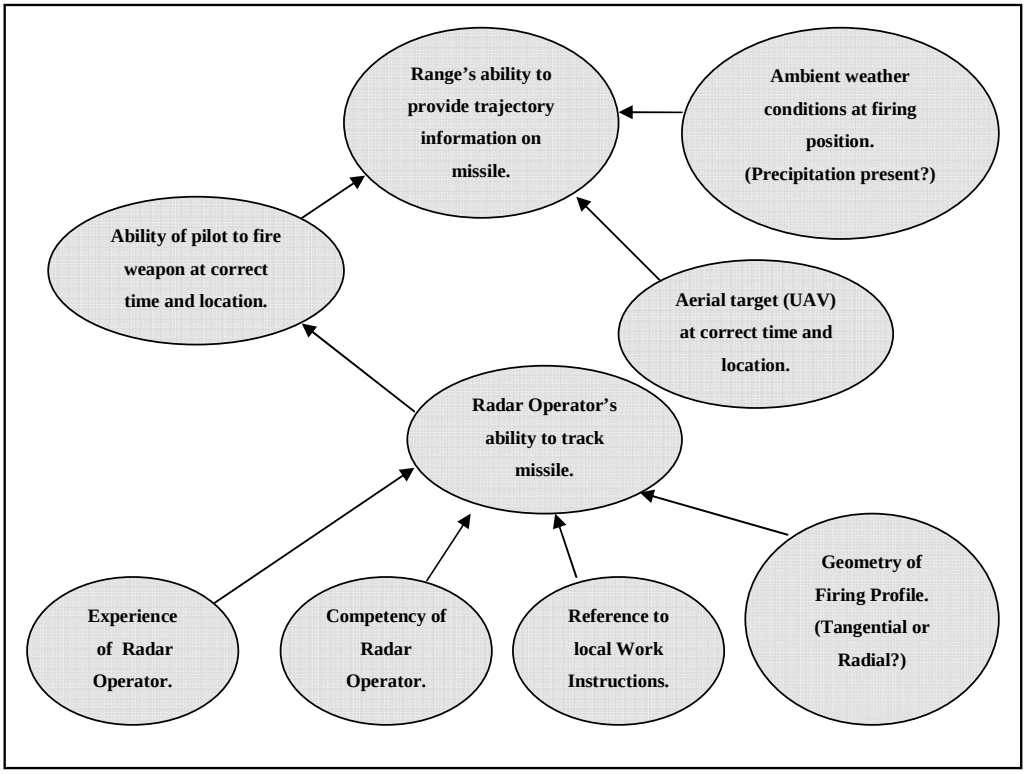


Fig 4.1 - Example BBN of a Range's missile tracking abilities.

Formatted: Bullets and Numbering

4.9.5 Goal Structuring Notation.

Kelly (1998) states that Goal Structuring Notation (GSN) was first developed for the presentation of safety arguments within the ASAM-II project. The original ASAM (A Safety Argument Manager) project was led by the University of York to investigate and develop a system for structuring the rationale applied to safety cases.

The project approached the problem by adopting the concept of structuring arguments in the Toulmin form (Toulmin, 1958) whereby the concept of typed premises and patterns of an argument are inserted to augment the use of Govier notation (Govier, 1992). It should be noted that both Govier's and Toulmin's notation may be used to convey any argument as they have been devised to be fully universal and do not explicitly record safety related concepts. GSN builds upon this typed argument framework to create a notation which is ideally suited to the safety justification domain (Kelly, 1998). A prototype Safety Argument Management (SAM) tool was borne out of the initial ASAM project which facilitated the management of sub-arguments so that they could effectively be assembled to construct the overall safety argument. Despite such encouraging results the project identified a number of critical areas which required more research. Of the criticisms raised the dominant two were;

- That the Toulmin approach was deemed to be very restrictive and did not readily support the forms of safety case argument commonly found within the real world.
- And that the tool should support the supporting evidence of a safety case and not just the high level argument.

The ASAM-II project, a collaborative DTI-EPSRC funded project with industry was initiated to address these issues. The project focussed on two prime concepts;

- The development of a goal based notation for structuring the high level argument of a safety case, and…
- The management of the inter-relationships that occur within the most common safety analysis techniques such as Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA).

The project ended in 1996 with the issue of a prototype tool SAM 3.25, published later by Kelly (1998). Minimal further development allowed the SAM tool to be offered as a commercial tool for the management of safety cases. In 1997 a consortium of European commercial companies who were involved in the development of safety-critical systems

created the ‘SAM Club’. Version four (SAM 4) of the SAM tool was issued in 1999 (Kelly, 1998).

GSN is a graphical argumentation notation which can explicitly represent the individual elements of any safety argument such as the requirements, claims, evidence and context (Despotou & Kelly, 2004). Of possibly greater importance is the fact that GSN can represent the relationships between these discrete elements such as how requirements are supported by specific claims or how the claims are supported by evidence. Furthermore, GSN can specify and/or define contextual information which is extremely important to real-world applications.

GSN currently utilises twelve principal elements which are linked together in a network to describe a goal structure (Kelly, 2003). The principal purpose of the goal structure is to demonstrate how claims about the overall system (goals) can be decomposed into various sub-goals until a point has been reached where they may be directly substantiated by clear and definitive evidence (solutions). Through the use of GSN in this decomposition phase it is possible to communicate the context (overall system application or the prescribed operational state), the strategies (quantitative or qualitative approach) and rationale of any argument (Kelly, 2003).

Succinctly, GSN has been designed to facilitate hierarchical structuring of the large amount of information which must be recorded and managed in the process of constructing a safety case. Primarily, GSN is used to capture high level arguments, including corresponding linkages, to any supporting evidence; it is also used to capture process descriptions including any relevant links to contextual information regarding the processes and/or solutions produced. In the application of GSN the system safety requirements are expressed as Goals. Through the use of decomposition (sub-goals/sub-requirements) or through direct appeal to supporting evidence (e.g. results of individual component analysis) these primal level goals may be shown to have been met. GSN notation, predominantly through evolution, has developed into a very useful and rich ‘language’ allowing assumptions, justifications, general proof and even rationale to be effectively captured and communicated.

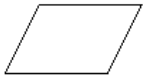
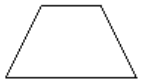
Entity	Symbol	Description
Goal		A statement of a requirement/target to be met by a system/item. Or some activity to be performed.
Strategy		A statement of how to break down a set of parent goals into a set of sub-goals.
Choice		A decision strategy for selecting between alternative strategies.
Solution		A solution to a goal. This can be almost any kind of technical data, such as a Fault Tree, Argument, FMEA, design reference etc.
Model		A representation of the system, sub-systems, or environment over which other goal structuring elements are articulated.
Context		Context provides the inputs or background information that a goal or other goal structuring element requires for it to be understood, amplified, or carried out.
Justification	 J	A statement justifying the use of a goal, strategy, choice, constraint, criteria, solution or model. The name indicates the file name where the details of the justification are stored in a separate file.
Assumption	 A	An assertion that some element of the goal structure has to rely upon in order for it to be satisfiable. It may relate to the environment, system, or be a theoretical.
Problem		A fact about the environment or system which may be expected to cause a problem in the solution of a particular goal, strategy or some other GSN element

Fig 4.2 - GSN entities, symbols and brief description of use (non-exhaustive).

The overall approach of creating a safety case using GSN starts with the construction of a High Level Argument (HLA) to which more discrete components of evidence, arguments and computations are attached; ultimately, a logical mass of data which supports the HLA is formed. The elements of GSN can be sub-divided into two main categories (Garman, 2007);

- Spinal - *Goals, Strategies, Choices, Solution.*
- Contextual - *Models, Contexts, Stakeholders, Criteria, Constraints, Assumptions, Justifications, Problems.*

Figure 4.2 lists (non-exhaustively) some GSN entities, their symbols and gives a brief description of their appropriate use. An example of a typical goal structure is shown in Figure 4.3.

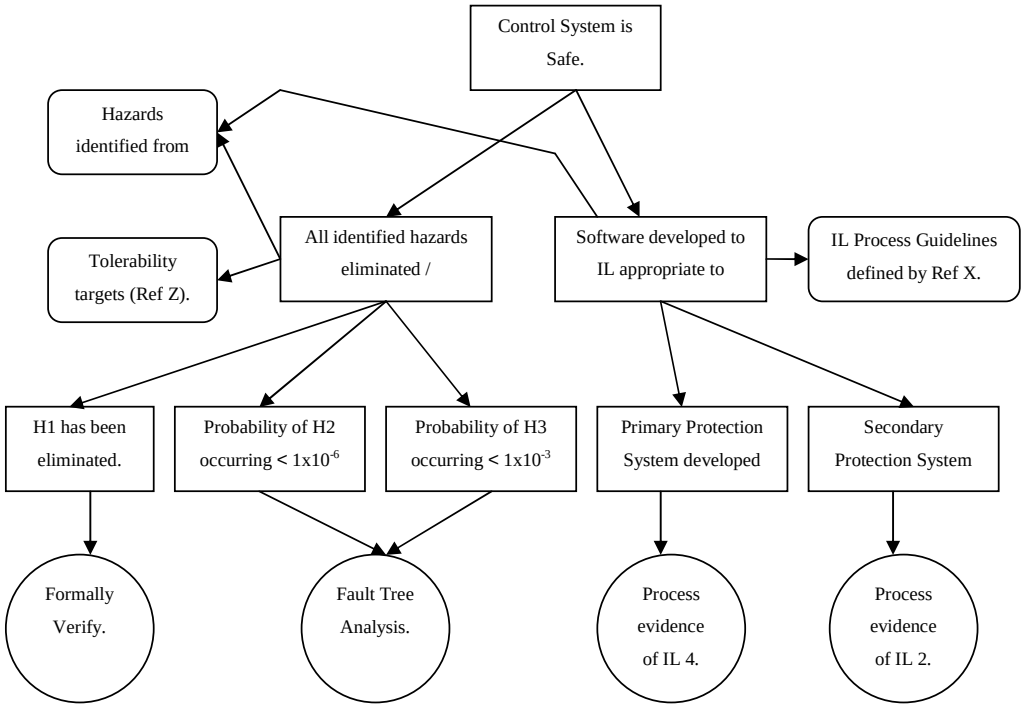


Fig 4.3 - Example GSN taken from Kelly & McDermid (1995).

GSN has been widely accepted by many safety-critical industries (e.g. aerospace, rail travel, defence) for the development and presentation of safety related arguments within safety cases over the past decade. The author's own industry of aerospace and weapon system development/evaluation has adopted GSN as the prime tool for safety argument development, especially in the field of UAV operations. It should be noted that the concept

of goal decomposition is not limited to the field of safety argumentation; in fact the approach of breaking down a primary element into its constituent elements has been employed within the *requirements engineering* and *systems engineering* industries.

Formatted: Bullets and Numbering

4.10 Safety Case Development Lifecycle.

It is certainly recognised within the author's industry that the development of a safety case cannot be left until the latter part of a system's lifecycle and that its creation for an already operational system can be very limited in value if the system already 'appears' to be safe.

In the case of the latter, and from experience, the author recalls how safety cases were constructed in direct response to changes in the regulatory regime of the T&E Ranges (MoD, 1997a). The creation of these somewhat immature safety cases should not be wholly denigrated but should be seen as the first few steps of an evolutionary and edifying process; certainly the extant safety cases within the author's business environment appear adequate. Nevertheless, constructing a safety case for an existing system (an application of the reverse engineering concept) is extremely limited and basically results in a formal report which documents the systems' activities under many assumptions. This is predominantly cogent for long-established systems where sub-system reliability and functional understanding is very limited. Assumptions for such safety cases are often made due to a lack of design evidence or large changes in technology and/or regulation; electromechanical and early software systems are prime examples of such systems. Approaches often used by safety case authors in the creation of a safety case for an extant operational system include "proof through usage" (analysis of historical data such as MTBF) or the apportioning of standard human failure and/or error probabilities from regulatory guidelines.

From the former's perspective, many problems have been experienced when the development of a safety case has been left until a project has been designed, implemented and is about to become operational (Kelly, 2003). These problems include the following (non-exhaustive) causes;

Costly and demanding re-design of some, or all aspects, of the system due to the late recognition that an adequate safety argument cannot be constructed. Quite often, a project will be initiated and driven forward by a business requirement underpinned by engineering or scientific SMEs. In the absence of a suitable safety engineer (safety case author) at the outset the project quickly grows and decisions are made to commit resources (e.g. financial, contractual, human) which may be both difficult and expensive to re-direct without loss of money, professional standing and time.

By omitting the safety case author from the early conceptual and developmental stage of the project the safety argument has to be constructed from a fait accompli rather than as an integral component which has evolved innately and inherently from within the project. Such an approach does not give the author an opportunity to influence the project's design in a way which could improve both its operational safety and its safety argument. Often in such circumstances the argument conveyed is weak and less convincing due to, for example, the use of more probabilistic components within the structure rather than the more plausible and definitive deterministic components.

Quite often the decisions and assumptions made on how to approach a problem in a particular way (justification, context and boundary conditions) are not recorded in any detail at the time. This is exacerbated if the decisions are made in the absence of a safety engineer. By opting to capture such important contextual information at such a late stage there is a real risk that some of the safety related information may be omitted to the detriment of the overall final safety argument.

An effective and robust safety case cannot be created as a singular event within the lifecycle of a system or project; it is an iterative and evolutionary process which commences at the conceptual stage of the project. It is developed and refined as the project matures. Many industries such as the MoD, the CAA, the UK's rail transport and the nuclear energy industries now require a safety case that is evolved and developed as part of an integrated approach when embarking upon any new project. For example, Defence Standard 00-56 (MoD, 2004) states the following;

"*The safety case should be initiated at the earliest possible stage in the Safety Programme so that hazards are identified and dealt with while the opportunities for their exclusion exist.*"

Whilst the HSE's Safety Assessment Principles for Nuclear Facilities (HSE, 2006b) states that;

"*For each life-cycle stage, control of radiological hazards should be demonstrated by a valid safety case that takes into account the implications from previous stages and for future stages.*

The safety case for each stage should take account of other life-cycle stages, i.e. it should build on the safety case for previous stages and show that the safety intent for subsequent stages can be achieved. The specific content and depth of information in a safety case will vary from stage to stage, and should be commensurate with the nature of a particular stage and interrelationships with other stages. For example, in the early stages (e.g. design concept) the safety case will be more a statement of future intent and principles, whereas a safety case for the operational stage will contain far more detail and analysis."

Formatted: Bullets and Numbering

4.11 A Staged Approach to Creating a Safety Case.

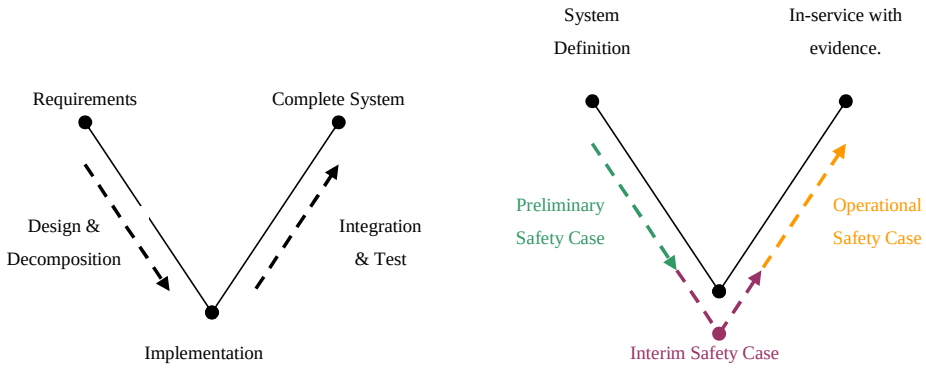
Defence Standard 00-56 (MoD, 2004) provides further advice on the development of safety cases. Though it suggests using a three stage approach for the creation of a robust safety case when dealing specifically with software the author considers that it should be adopted as good practice for the development of virtually all safety cases ;

- A **Preliminary Safety Case** (PSC) should be created upon defining and reviewing the system requirement specification.
- A further **Interim Safety Case** (ISC) may be created upon completion of a proposed system design and the successful conduct of some preliminary verification and validation exercises.
- A full and final **Operational Safety Case** (OSC) should be constructed prior to the period by which the system is to be operational. Such a safety case will include

evidence which corroborates any earlier assumptions and/or models which may have been used to bound the original conceptual stage. The evidence will not only support the user requirement but will be used to satisfy the requirements of any third parties such as Independent Safety Assessors (ISAs) and regulators such as the HSE, MoD and the Civil Aviation Authority (CAA).

Operational safety cases present an argument that a system is acceptably safe in a given context (McDermid & Kelly, 2005). Operational safety cases differ somewhat from the more isolated or independent type of safety case which is often created for a piece of equipment or a system of sub-systems. Special considerations should be applied when developing and managing operational safety cases such as considering lessons which have been identified from major accidents or incidents where causation may have been attributed to operational sources. Specifically, operational aspects include elements such as the external environment, culture, human factors, competence and even procedures as they are all holistically linked into the way that the system is operated and managed (McDermid & Kelly, 2005). Operational safety cases may often have many operational omissions, especially if the equipment has been built and the overall context or strategy of how and when it will be used has not been finalised. It should be noted that civilian and military operational safety cases may have both similar and different elements within their operational safety cases; examples may include contingencies for terrorist attack, sabotage, commercial gain, etc.

Though the safety case requirements of various industries differ, predominantly due to regulatory dissimilitude, the overall approach of creating a final safety case from a number of evolutionary phases is increasingly being accepted as a principal concept across most disciplines (Kelly, 2003). Figure 4.4 depicts graphically how the evolutionary safety case concept (Safety Case Lifecycle) aligns with established methodologies for project engineering (Design Lifecycle).



The Design Lifecycle **The Safety Case Lifecycle**

Figure 4.4 - Illustration of the alignment of Design and Safety Case Lifecycles (Based upon Kelly, 2003).

Core to the evolutionary safety case concept is the developing safety argument and its ability to clearly demonstrate how an initial concept consisting of foundational elements has been developed into a mature, well structured and consistent argument. The evolution and maturity is demonstrated through the revisiting of any pre-worked argument components with new knowledge gleaned as the project progresses. As the final operational phase is approached then data and evidence may be gathered from test-runs, site acceptance checks or commissioning work to further validate any models or to qualify even the most fundamental of engineering calculations. From both an engineering and business perspective this form of approaching the final stages of a project is logical and very effective for de-risking and verification prior to becoming fully operational.

The ability or opportunity to introduce a safety engineer into a safety-related project at its inception (PSC phase) is paramount if the project is to achieve an optimal balance between its engineering solution and safety related certification. Quite often the early identification of safety objectives allows the final design to be influenced to allow a more compelling safety argument to be established.

Many decisions are made at the earliest of stages whilst discussing various solutions. Even at the conceptual phase, decisions, often unconsciously, are made which bias the mindset

being applied to create a solution to the problem. Immediately after a relatively minor conceptual decision is made certain key assumptions will register in the minds of those present which will drive the project along a particular route. It is again re-emphasised that the presence of a safety engineer at such an early point in the project's lifecycle will help to both focus and keep a perspective on the final deliverable as well as improving its efficiency. The ability to 'weed out' any extraneous technical notions or to minimise any ill-educated safety assumptions plays an important part in the creation of an optimised and cost-effective timeline. Such an approach can help to reduce or remove nugatory developmental activities which may be expensive in both materials and time as well as demanding on labour. Misdirected or needless effort in any business is not only damaging to the profit margin but can be very injurious internally to a company's staff morale; additionally, if the wasted effort is made public then its professional reputation may suffer.

It is therefore suggested that the preliminary phase is one of the most important stages in the safety case lifecycle. Kelly (2003) suggests that the following activities will have been conducted prior to, and in preparation for, the Preliminary Safety Case;

- **Production of a Safety Management Plan** which will define the key safety processes, roles and responsibilities to be enacted during the system development (author's comment - this would be created as part of the adopted Safety Management System).
- **An Identification of Required Safety Properties** including identification of any applicable safety standards and their application to the system under development. This activity would also involve the customer, if applicable, and ensure that the system met their safety related requirements.
- **A Preliminary Hazard Analysis (PHA)** which looks to identify all of the possible system hazards by conducting a thorough systematic review of the system's high-level design. Such an approach has been used extensively within the author's environment in the development of safety and operational procedures in support of Civil UAV Operations at West Wales UAV Centre (Parc Aberporth), the creation of the Ranges' Safety Cases and the development of new facilities such as the Mirach aerial target facility at MoD Aberporth. One of the most useful tools used in

identifying the potential hazards within a project is that of performing a Hazard and Operability Study (HAZOP). A HAZOP is a proven technique which utilises concepts such as structured brainstorming, zonal analysis, causal path analysis and even check lists to identify and record the possible hazards which may be associated with the development and operation of a system. Any hazards identified will be recorded in a hazard log together with a qualitative and/or quantitative estimate of risk. The topic of hazard identification and the use of HAZOP is discussed further within 4.12.2.1.

- **Risk Estimation.** Having identified the hazards and logged them appropriately there is a need to apportion risk to each hazardous component. Risk is usually estimated (or calculated if appropriate) through the use of severity and likelihood distributions; both quantitative and qualitative approaches may be used. Risk is specifically defined and discussed within 4.12.
- **The Identification of Failure Rates (or Modes) and Integrity Levels Required.** Having assigned the risks there is a key requirement to ensure that the project is developed and delivered according to the integrity levels identified within the previous exercise.

It should be reiterated that the PSC is predominantly constructed before any definitive or detailed system design has been created and therefore the amount of information at this time may be extremely scant or nebulous. Despite such a lack of information the creation of an early safety approach offers the following positive contributions to the project's lifecycle;

- Focussing the minds of the whole project delivery team to not only look at the business aspects such as investment, depreciation and/or marketing opportunities but to holistically understand the legal and/or regulatory obligations and boundaries.
- Supporting the definition of scope for both the final safety case and the final project deliverable (Kelly, 2003).
- By conducting an early hazard analysis (PHA) the key safety issues and objectives are easily identified and focussed upon (Kelly, 2003). Quite often within major

projects the output of a PHA is paramount to the decision making process in order to understand what path to take in the developmental and evolutionary stages. Customers will at times request an article to be developed which may not be aligned with extant industry safety policies or regulatory guidelines. Such requests are often driven by existing operational systems where the customer merely wants a 'like for like' replacement; both technology and legal requirements may have changed significantly during the life span of the existing article and therefore an 'up to date' approach may be required which will need interfacing with the existing system(s). By adopting a systems thinking approach any project team would instantly recognise that conducting a PHA is completely aligned with the concept of 'unpacking' a customer (or user) requirement into its foundational components. The author is extremely supportive of utilising a systems approach with any project as it helps to define and refine all aspects of the requirements, safety engineering being a prime component.

- The PHA offers the project team an early view of the strategy being taken to enable an optimised safety argument to be developed; it also highlights some of the techniques, tools and supporting evidence which will need to be made available to support it.
- Whilst preliminary safety information can help to evolve a relatively safe engineering solution there will be occasions when the final solution for operational safety will be heavily reliant upon developed safety procedures. Such procedural safety dependencies may simply augment the designed-in safety mechanisms or may in fact be part of the fundamental requirements to attain the designed-in safety targets. These procedural prerequisites may be formally highlighted to the ultimate operators of the system in the form of work instructions such as procedures and operational protocols. By evolving the work instructions from early developmental activities conducted as part of the de-risking phase benefits may be delivered in both the business and safety environments (e.g. near misses and/or accidents which occurred during laboratory work). From a safety perspective the work instructions may be more closely aligned with the residual risks within the system and therefore mitigate the risks in a more apt and specific manner. From a business perspective the evolved work instructions will take less time and effort to initially document

and put in place. Additionally, the business will benefit from having the more appropriate and intelligent work instruction in place as it will minimise the potential for accidents within the workplace which can affect production.

Formatted: Bullets and Numbering

4.11.1 The Preliminary Safety Argument.

Whilst the PSC reviews many elements of the safety argument within the early stage of a project's life one of its prime objectives is to gain a mutual understanding between the customer and the safety engineer(s) as to what is an agreeable approach for the project's safety argument.

Distilling the project's requirements into discrete, yet inter-related, elements is an extremely strong and important part of this phase. One tool which is heavily utilised within the author's working environment for interpreting safety requirements and documenting the possible paths that may be followed to demonstrate such claims is that of GSN. Kelly (2003) also suggests that GSN is an useful means of mapping out such primary and emergent safety arguments. In his example Kelly (2003) demonstrates how a preliminary safety argument for a new braking system is developed which consists of three threads; a conventional hazard mitigation argument, a compliance with standards argument, and a comparative argument claiming improved safety over existing systems.

Having adopted GSN as a tool to allow for the development of complicated safety arguments the overarching need to define context becomes even more accentuated (Kelly, 2003). The author, from his work within the T&E environment supports this view very strongly. One of the key pieces of information required within any safety related text such as a safety case or even a safety instruction is that of context. Without context any information or instruction loses its ability to provide a just means of control; context provides a host of both conscious and unconscious constraints which are realised both physically and psychologically in the subject's mind. Context provides a frame of reference and forms many of the engagement conditions for an activity; it is further discussed and analysed in depth in following chapters of this thesis.

4.12 Risk.

Formatted: Bullets and Numbering

No review of safety cases would be complete without a discussion on the topic of risk. All safety cases are based upon the identification of and subsequent management of risk.

The terms hazard and risk are used interchangeably in our every day life though the HSE have made a formal conceptual distinction between both (HSE, 2001a). A hazard is described by the HSE (2001a) as "*the potential for harm arising from an intrinsic property or disposition of something to cause detriment*", whilst risk is described as "*the chance that someone or something that is valued will be adversely affected in a stipulated way by the hazard*". The HSE, from a health, safety and welfare of people perspective, frequently utilise the aforementioned conceptual distinctions in any guidance offered by requiring that hazards are identified, the risks that they create are assessed and appropriate controls are introduced to address the risks (HSE, 2001a). This concept, when applied to everyday life, reflects the fact that for most instances due diligence should be taken of occurrences where people and management systems interact with a hazard (HSE, 2001a).

When describing or managing hazards it is often possible to regard any hazard as having remote and/or indirect origins which themselves constitute a 'real hazard'. An example of such an event is the storage of an explosive material such as ammunition. It may be argued that the storage per se is not the hazard but rather it is the intrinsic properties of the material being stored (HSE, 2001a). Despite this argument, it is generally considered to make sense to consider the storage as the basis for the estimation of risk since such an approach will be the most appropriate for identifying the practical control measures necessary for managing the risks efficiently. The outcome of such an approach may identify that (i) the material should not be stored at all, (ii) should be stored in smaller quantities, (iii) should be replaced for a safer variant of material, or, (iv) the storage facilities may have to be upgraded.

The HSW Act does not contain the term 'hazard' (HSE, 2001a). Since the Act was created the law courts have ruled that (with reference to Section 3 of the Act) 'risk' means 'possibility of danger' rather than 'actual danger'. Therefore, from this concept, the HSE regards anything presenting the 'possibility of danger' as a 'hazard'. So as not to place an

excessive and pointless burden upon any duty holder for the management of all possible hazards within the workplace, the HSE does not expect any hazards, "*other than those which are reasonably foreseeable causes of harm, taking account of reasonably foreseeable events and behaviours"*, to be addressed. Whether a reasonably foreseeable but unlikely event (such as an earthquake) should be considered depends upon the consequences for health and safety following such an event (HSE, 2001a).

One of the fundamental principles which underpins the HSW Act is that those who create risks from any of their activities are responsible for protecting both their workers and the general public from any consequences. The HSW Act therefore "*places specific responsibilities on employers, the self-employed, employees, designers, manufacturers, importers, suppliers and people in charge of premises."* (HSE, 2001a). Additionally, supporting and associated legislation is levelled at owners, occupiers, licensees and managers.

Regulations have also been introduced to help clarify many of the responsibilities now impressed upon so many, such as requiring employers and the self-employed to assess risks and to base their control measures on those assessments. When the consequences forecasted are relatively insignificant or inconsequential then basic written risk assessments (generic risk assessments) and/or method statements are sufficiently robust enough to capture the process and to provide context for the whole process. Where hazards which may result in severe consequences are highlighted, the industry trend over recent years has been to focus upon and amplify those duties and to request the creation of more specific safety cases. Such an approach requires duty holders to both document and submit their extant or proposed control measures to the HSE to demonstrate their ability to meet their legal obligations and ensure safe and healthy systems of work (HSE, 2001a). This system of HSE 'moderation' ensures that duty holders understand the hazards associated with their work activities and how to control them; additionally, it allows the HSE an insight into the duty holders' management of health and safety.

Since the passing of the HSW Act (1974) the model for managing risk at work has been to align and consolidate the authoritative bodies responsible for occupational health and safety

and to further clarify those responsibilities within criminal law for managing risks. Of particular note is the inception of regulatory regimes where "*broad general duties*" are explicitly put on those who are best placed to act in the prevention or control of risks. In such circumstances the foundational broad duties are often augmented by more specific and specialised regulations (HSE, 2001a). A clear example of the application of more stringent and specific regulations, in addition to the creation of a specialised regulatory body, lies within the UK's nuclear energy industry. The process may also place stringent and absolute duties on specific (and named) duty holders.

In other arenas where the *broad general duties* are not augmented by supportive, specialised and/or explicit regulations the guiding principle for managing risk at work is qualified by expressions such as "so far as is reasonably practicable" (SFAIRP). Such an approach evades the need to impose duties upon duty holders that are virtually impossible for anyone to actualise; absolute safety cannot be guaranteed (HSE, 2001a). The SFAIRP approach ensures that the preventive and protective actions taken are commensurate with the risks involved. In addition to the SFAIRP qualification there are other similar qualifications such as "as low as reasonably practicable" (ALARP) and "as low as reasonably achievable" (ALARA).

Formatted: Bullets and Numbering

4.12.1 HSE's Risk Criteria.

Whilst the assessment of risk may be conducted against a wide range of criteria (e.g. financial loss, national security etc.) the convention used to assess the risk of industrial accidents and/or their potential to injure members of the public is to assess the risk of death. This approach includes the risk of death to both members of the public as well as workers. In practice the actual fatality rate for workers in even the most hazardous of industries is usually well below the upper limit of a risk of death to any individual of 1 in 1,000 per annum for workers and of 1 in 10,000 per annum for the public who have a risk imposed upon them 'in the wider interest of society' (HSE, 2001a).

The criteria used by the HSE for assessing risk, both in a qualitative and quantitative manner, are provided in their discussion document '*Reducing risks, protecting people; HSE's decision-making process'* (colloquially known as '*R2P2'*), (HSE, 2001a). Within it

the HSE explains and defines how it has adopted a framework, known as the tolerability of risk (TOR) model, to accommodate the three primal criteria used by their regulators in the decision management of risk. The criteria are "*equity-based, utility-based and technology-based"*. Though the aforementioned 'pure' criteria work very well in most cases they do suffer from some disadvantages when attempts have been made to apply them in a more universal way (HSE, 2001a). In an attempt to provide a more wide reaching and holistic approach to the decision management of risk the HSE have stated that the criteria should not be applied as separate entities but rather as a mutually exclusive system (HSE, 2001a).

The framework is illustrated in Figure 4.5 where the inverted triangle represents an increasing level of risk for a particular hazardous activity (measured by the individual risk and societal concerns it engenders) as we move from the bottom of the triangle (apex) upwards towards the top (or base) (HSE, 2001a). Though the HSE's discussion document (HSE, 2001a) shows a single coloured, though vary-shaded triangle, the overall message conveyed remains the same. Figure 4.5 includes additional and appropriate data (risk of death to workers) for application within the author's industry. These figures will be further discussed in the following text.

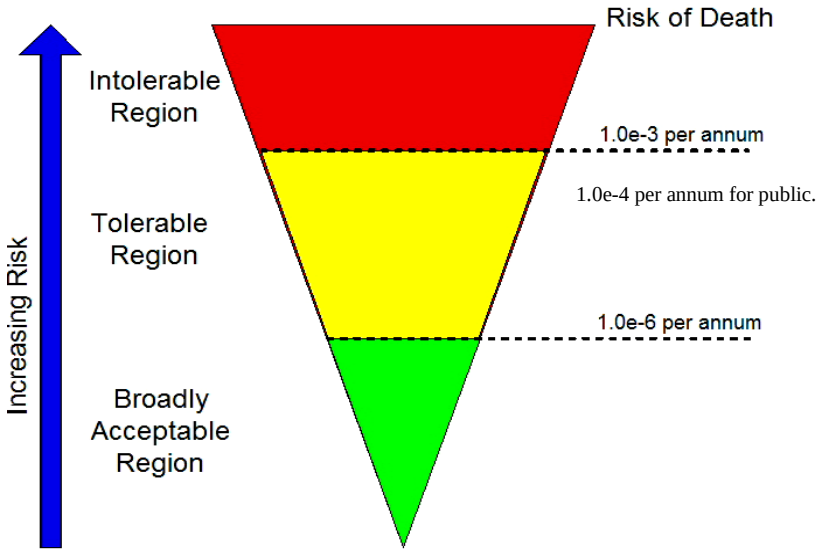


Figure 4.5 - Framework for the tolerability of risk, based upon HSE (2001a).

The red zone at the top represents an unacceptable or *intolerable*, region. This region is where the overall risk is deemed too high and completely unacceptable whatever the level of benefits that could be associated with the activity. Any activity or practice which generated risks falling into this region would, as a matter of principle, be removed unless it could be altered to minimise the level of risk or there were exceptional reasons for the activity or practice to remain (HSE, 2001a). This region, without many exceptions, is bounded by an upper limit of risk of death to an individual, in this case $1x10^{-3}$ per annum for workers and $1x10^{-4}$ for the general public.

Within the green zone, or *broadly acceptable region*, risks falling into this category are usually regarded as less than those to which we may be exposed to in everyday life activities. Risks falling into this region are generally regarded as insignificant and are deemed to be adequately controlled (HSE, 2001a). This region is bounded by a lower limit of death to an individual (in this case, $1x\ 10^{-6}$) and any activities which lie below this limit do not require any additional investigation before the activity is allowed to proceed unless reasonably practicable measures are available (HSE, 2001a). The levels of risk within this region are comparable with those risks that people regard as trivial in their daily lives; typically they may be risks from non-hazardous activities or those from hazardous activities that can be, and are, readily controlled to produce very low risks (HSE, 2001a) such as re-fuelling a motor car or driving heavy plant machinery.

The yellow zone represents the *tolerable region*. Risks within this category fall between the unacceptable and broadly acceptable regions. Risks falling within this category are typical of those risks raised by certain activities within which society (or individuals) is (are) prepared to tolerate in order to secure certain benefits (HSE, 2001a). It is expected though, that these benefits, will be delivered under risk with the expectation that;

- "*The nature and level of risks are properly assessed and the results used properly to determine control measures. The assessment of the risks needs to be based on the best available scientific evidence and, where evidence is lacking, on the best available scientific advice.*" (HSE, 2001a).

- "*The residual risks are not unduly high and kept as low as reasonably practicable (the ALARP principle).*" (HSE, 2001a). The ALARP principle is further discussed in the following text.
- "*The risks are periodically reviewed to ensure that they still meet the ALARP criteria, for example, by ascertaining whether further or new control measures need to be introduced to take into account changes over time, such as new knowledge about the risk or the availability of new techniques for reducing or eliminating risks.*" (HSE, 2001a).

The tolerability of risk framework may, in principle, be applied to virtually all hazards. In determining reasonable and practicable control measures for any particular hazard, i.e. if the option chosen is sufficient and suitable, depends to some extent upon where the boundaries are drawn between the unacceptable, tolerable or broadly acceptable regions (HSE, 2001a). The final risk framework model adopted by a particular industry will be an output from extended negotiation and deliberation during the course of policy development and/or evolution. This developmental process will reflect the value preferences of all stakeholders and the practicality of all possible solutions, ultimately driving the figures at the aforementioned boundaries of the three regions.

In practice the actual and real fatality rate for an individual, even in the most hazardous of industries, is usually well below the upper limit of a risk of death of 1 in 1000 ($1x10^{-3}$) per annum for workers and 1 in 10,000 ($1x10^{-4}$) per annum for members of the public who have a risk imposed upon them 'in the wider interests of society' (HSE, 2001a). Illustrative examples of annual fatality rates are issued by the HSE and help provide context to the concept of hazardous activity management and the consequential risks within various industries. The annual fatality rates quoted for 1999/2000 (HSE, 2001a) were;

- Agriculture, Hunting, Forestry and Fishing (Sea Fishing excluded) - 1 in 12,984.
- Construction - 1 in 21, 438.
- Mining and Quarrying (including offshore oil and gas) - 1 in 14,564.

In other traditionally less hazardous industries the annual risk of a worker fatality is even lower. The example quoted in the HSE's document '*Reducing risks, protecting people: HSE's decision-making process*' (HSE, 2001a) is that of the service sector where the figure was 1 in 388,565 during 1999/2000. Further and more explicit information can be sourced from the HSE's publication '*Health and Safety Statistics*' which is released annually and is available through Her Majesty's Stationery Office (HMSO).

The HSE believes that an individual risk of death of one in one million per annum for both workers and the public correlates to a very low level of risk and should be used as a guiding principle for the boundary between the broadly acceptable and tolerable regions of the tolerability of risk framework. With reference to Tables 4.1 and 4.2, society in general is exposed to an environment of appreciable risks of various types which contribute to a background level of risk (typically a risk of death of one in a hundred per year averaged over a lifetime) (HSE, 2001a). When compared with the background level of risk, the residual risk of one in a million, appears to be very small. It should be duly considered that many everyday activities such as using domestic gas and electricity or using air travel breach the residual level of risk identified by the HSE.

Type of accident	**Risk**	**Basis of risk**
Fairground accidents	1 in 2, 326, 000 rides	UK (1996/7 - 1999/00)
Road accidents	1 in 1, 432, 000 kms travelled	GB (1995 - 1999)
Rail travel	1 in 1, 533, 000 passenger journeys	GB (1996/7 - 1999/00)
Burn or scald in the home	1 in 610	UK (1995 - 1999)

Table 4.1 - Average annual risk of injury as a consequence of an activity, (HSE, 2001a).

The HSE do not give such clear and guiding principles for the boundary between the tolerable and unacceptable regions for individual risks entailing fatalities as they do for the boundary between the broadly acceptable and tolerable regions. This is predominantly due to the fact that the risks may be unacceptable on the grounds of high risk exposure to an exposed individual, or because of the repercussions of such an activity (or occurrence) on general society. Risk, being somewhat subjective and emotive, often generates higher

societal concerns, especially if it identifies higher levels of individual risk. Such concerns are usually driven by issues of fairness and/or equality in risk taking and in risk exposure.

Activity associated with death	Risk	Basis of risk
Maternal death in pregnancy (Direct or indirect causes)	1 in 8, 200 maternities	UK (1994 - 1996)
Surgical anaesthesia	1 in 185, 000 operations	GB (1987)
Scuba diving	1 in 200, 000 dives	UK (2000/01)
Fairground rides	1 in 834, 000, 000 rides	UK (1989/90 - 2000/01)
Rock climbing	1 in 320, 000 climbs	England & Wales (1995 - 2000)
Canoeing	1 in 750, 000 outings	UK (1996 - 1999)
Hang-gliding	1 in 116, 000 flights	England & Wales (1997 - 2000)
Rail travel accidents	1 in 43, 000, 000 passenger journeys	GB (1996/97 - 1999/00)
Aircraft accidents	1 in 125, 000, 000 passenger journeys	UK (1991 - 2000)

Table 4.2 - Average annual risk of death as a consequence of an activity, (HSE, 2001a).

Though the preceding text has considered averaged risks (e.g. per passenger journey, per flight, per operation, *et al*) to any single individual there is a need to consider aggregated or total risk for certain environments and climates. The socio-political responses to a particular event such as a railway disaster would find that the total risks to the affected populous completely unacceptable despite the relatively low individual risks calculated on a per person basis. Certainly within some specialised industries such as the nuclear power environment the HSE have suggested some guiding principles; they suggest that an individual risk of death of one in one thousand, per annum, should represent the boundary between what is just tolerable for any major category of worker and what is unacceptable for any but the fairly exceptional groups. For members of the public who have a risk imposed on them ‘in the wider interests of society’ this limit is increased by a factor of ten to one in ten thousand, per annum (HSE, 2001a).

Within the author's industry the HSE agreed boundary between the unacceptable and tolerable regions is set at an individual risk of death of one in one thousand, per annum, for a worker on a QinetiQ managed site. The HSE recommendation for this boundary is one in ten thousand, per annum, for the death of a member of the public exposed to risks resulting from the work of a QinetiQ managed site. For both workers and the general public, the boundary between the broadly acceptable and tolerable regions is identical and is set at a risk of death of one in one million, per annum.

Cognisance should be taken of the fact that workers within the QinetiQ site boundaries are further split into two distinct groups; those that are taking an active part in the trial activity and are exposed to the immediate hazards (e.g. handling, preparation and arming of explosive ordnance); and those who are not exposed to any immediate and real hazards and may be fulfilling a support role or one which is physically separated from the hazard (e.g. radar operator, air traffic control) (Garman, 2006). Both the HSE and QinetiQ management believe that there are no valid reasons for allowing the latter group of workers to be subjected to a higher degree of risk exposure than that deemed appropriate for the general public. To this end, the risk criteria used for this group of workers is aligned with that for the general public; additionally, those members of the public who have a requirement to access a QinetiQ managed site (e.g. delivery drivers, regulators) are included within the same risk criteria.

Though the HSE have issued guiding principles to help identify and qualify the risk boundaries that should be used by industry they very rarely give business a difficult time. As hazard levels rise then so do the risks subjected to individuals increase which in turn raises societal concerns; it is often these latter concerns which play a deciding role in deciding if a risk is acceptable or not. Additionally, the limits issued by the HSE were evolved and derived with respect to activities which are very difficult to control and risk manage; the majority reflect agreements drawn up at international level (HSE, 2001a).

Formatted: Bullets and Numbering

4.12.2 Managing Risk.

Effective risk management is an activity which considers the risks emanating from any hazard presented by an activity, process or project. Within the context of this thesis, risk

management involves the identification, quantification and management of both initial and residual risks. The whole activity can be broken down into the following key elements (MoD, 2004);

- Hazard Identification.
- Hazard Analysis.
- Risk Estimation.
- Risk & As Low As Reasonably Practicable (ALARP) Evaluation.
- Risk Reduction.
- Risk Acceptance.

This six stage process should be conducted as an iterative process with the aim of achieving continual risk management (risk reduction if appropriate) through the life of the activity.

Formatted: Bullets and Numbering

4.12.2.1 Risk Identification.

Risks may be identified using a number of methods though they all rely predominantly upon the experience and knowledge of a broad, varied and numerous collection of individuals. Though different techniques exist, the principal and most important component which is common to all is that of the body of intelligence assembled. The assembled group which is performing the hazard identification must have a total knowledge base which is likely to encompass all of the possible hazards that may manifest themselves during subsequent operations. Any deficiencies within the group's knowledge base will appear as weaknesses in the hazard log; the danger being that those unidentified potential hazards may remain dormant for some period of time. This is of particular importance when an activity or project is considered to have potentially catastrophic outcomes and the development and/or operational period is relatively lengthy. During the dormant period the hazard identification group and related management team may be drawn into making decisive decisions in relation to an activity's direction and will have committed resources (e.g. financial); a false sense of security and blissful ignorance may often descend upon the whole organisation during this period only to be shattered by the occurrence of a hazard which was not foreseen and highlighted in the first instance. As discussed earlier within this

chapter, it is important, after creating a PHA, to critically revisit the work periodically and maintain a living document.

The tangible output of this type of exercise will be a tabulated list of hazards identified (Hazard Log) which will record the hazard details, descriptive texts and any comments relating to its status and management. Hazard logs may quickly become quite onerous to manage when trying to identify potential hazards within a large and complex system or system of sub-systems. For such eventualities hazard tables which are cross-referenced to repositories may be used, especially when dealing with complicated or confidential (emotive) methods of risk management. The overall hazard log may still be used as the definitive tool to demonstrate hazard management though the information recorded may only be high-level in nature.

One method of identifying hazards is that of brainstorming where a group of experienced and knowledgeable individuals produce ideas and/or solve problems from spontaneous discussions. In the context of hazard identification the use of brainstorming encourages participants to propose, probable or improbable mechanisms by which hazards may be present (MoD, 2004). During such a session, the hazard mechanisms uncovered are not synthesised or explored, this being done at a later stage. The focus during the session is to allow free flowing thought though the overall context and boundary conditions must be carefully managed by a facilitator.

In preparation of a brainstorming session for hazard identification the facilitator should have a relatively deep understanding of the general hazard environment but not necessarily the specific and deeply specialised elements of the planned activity. The facilitator should be willing to explore the environment with a typical ‘soft systems’ mindset (Checkland, 1981) where many of the unidentified risks may lie in the nebulous and/or intangible regions of the activity. As systems grow in complexity there is a need to not only look at the traditional engineering components but to take serious cognisance of the ‘social systems’ concepts which are so interwoven into modern systems.

During the brainstorming session the facilitator usually writes down the ideas and threads which are raised and discussed and may start to link then together as a form of early mind-map or causal link pattern. Humour and light hearted debate is useful to allow the more reserved or junior individual to feel comfortable within the environment; many key hazards are often sparked by discussions which were originally quite obscure and tangential in nature when compared with the overarching topic. In situations where the activity or project is complicated there may be a requirement to facilitate more than one session.

Once the brainstorming process is deemed to be exhausted then the suggested hazards may be grouped into a relatively logical manner (e.g. reliance on processes, related to the environment, etc.). Due diligence should be considered before rejecting some of the ideas raised; a peer assessment by a number of experts may be considered useful before rejecting any suggestions. Once the final list of identified hazards has been agreed then so they can be analysed in the next stage.

Whilst conducting a brainstorming exercise or any other hazard identification process the facilitator may decide to use various tools to help structure and focus the activity. One simple tool that is often used is that of a checklist where a list of potential hazards is peer reviewed by the group session; basically the list operates as an aide-memoir where each component of a system is considered for its hazards and inter-relationships with other components.

Caution should be applied when using checklists as they can limit the degree of freedom available within the brainstorming session; by default, the checklist will narrow the field of thought within the session as it will have been constructed by an individual (or small team of individuals) with a pre-determined mindset. Through inference the group's output will not have been free-thinking and will have been skewed by some of the conditions introduced by the checklist(s).

A further development of the checklist method is that of the Structured What-If Technique (SWIFT) where open ended questions about the system are asked which will identify the hazards within. Such questions cannot be answered with a simplistic "No" or "Yes"; they

will typically begin with words such as “What?”, “How?”, “Who?”, “When?” etc. In a similar manner to brainstorming, the exercise requires the involvement of an appropriately experienced and well informed group of individuals.

The specific checklist(s) used for these exercise(s) may be derived from a more generic list of hazards such as those in Table 4.3 (non-exhaustive). As the group carefully considers the consequences of the hazards in each part of the system the mitigations and control mechanisms are carefully noted in a Hazard Log. The information recorded will include any safeguards and protective measures which are either in place or require installation to either prevent the event from occurring or to help minimise any consequential hazardous output.

A more structured method for identifying hazards within a system is offered by conducting a HAZOP analysis. This is a systematic method of methodically producing a set of possible outcomes and identifying those that are undesirable (Hollnagel, 2004, p183). The HAZOP approach was developed by Imperial Chemical Industries (ICI) in the UK during the early 1960s to try to identify all possible aberrations from a system’s designed and expected operation and to record all potential hazards associated with them. The most critical and fundamental part of any HAZOP exercise is to interrogate and analyse each step in a process or procedure using a set of HAZOP guidewords which represent the following conditions; ‘*negation, quantitative increase and decrease, qualitative increase and decrease, logical opposite, and substitution*’ (Hollnagel, 2004, p184). The whole concept behind the process is to simply combine each step of the system with the list of guidewords and to consider whether something could happen other than what was intended. A typical example set of guide words to support a HAZOP activity is shown in Table 4.4.

For example, if a capacitor supplying power to a laser emitter is to be charged by a high voltage power supply, the HAZOP guidewords will force the analysts to consider possible scenarios such as, no applied voltage, too low a voltage is applied, too high a voltage is applied or a voltage is applied at an incorrect time in sequence.

Hazard Location	Potential Source of Hazard
Hazardous Components	Lasers
	Explosives
	Asphyxiants, Toxic or Corrosive Substances
	Pressure Systems
	Electrical Systems
	Ionising or Non-ionising radiation sources
	Flammable Substances
	Hydraulic Arms or Rotating Machinery
	Passive Obstacles
	Cut and puncture Projections
Safety Related Interfaces between Sub-systems	Material Incompatibilities
	Electromagnetic Interference (EMI) and Compatibility (EMC)
	Inadvertent Activation
	Fire and Explosion Initiation and Propagation
	Hardware and Software Controls
Factors Due to the Operating Domain	Drop
	Shock and Vibration
	Extreme Temperatures, Pressures and Climatic Conditions
	Noise
	Exposure to Toxic and/or Corrosive Substances
	Fire or Explosion
Operating, Test, Maintenance and Emergency Procedures	Human Factors Consideration, User Errors,
	Life Support Systems
Damage Control Measures	Damage and Hazard Containment
	Egress, Rescue and Survival
Facilities	Training
	Provisions for Proof Testing, Storage and Assembly of Hazardous Material
Defences against Common Mode Failures	Fail Safe Designs
	Interlocks, System Redundancy and Diversity
Threats to Programmable Electronic Systems	Security Breaches, Virus Susceptibility

Table 4.3 - Non-exhaustive list of generic hazards (Garman, 2006).

Guideword	Meaning
No	This is the complete negation of the design intention. No part of the intention is achieved and nothing else happens.
More	This is a quantitative increase.
Less	This is a quantitative decrease.
As Well As	All of the design intention is achieved together with additions.
Part Of	Only some of the design intention is achieved.
Reverse	The logical opposite of the intention is achieved.
Other Than	Complete substitution, where no part of the original intention is achieved but something quite different happens.
Early	Something happens earlier than expected relative to clock time.
Late	Something happens later than expected relative to clock time.
Before	Something happens before it is expected, relating to order or sequence.
After	Something happens after it is expected, relating to order or sequence.

Table 4.4 - Non-exhaustive and illustrative list of HAZOP guidewords (Garman, 2006).

The principle of combining guidewords with textual descriptors of an activity in order to explore all possible potential hazard combinations is not unique to risk analysis; the concept has been used at least since the 1940s (Hollnagel, 2004, p184). Though the HAZOP guidewords were originally developed for the risk analysis and hazard prediction of technical systems they may be used somewhat loosely for socio-technical systems. In more specific social or human failure applications there may be a requirement to revise the guidewords somewhat; more detailed information for such applications is available through more specialist sources such as Duncker (1945).

It should be noted that the use of HAZOP, or any other systematic list of failure modes, is not a *magic bullet* to identify all possible failure modes. The approach is simply one method of trying to ensure that each and every possible combination has been considered by using the guidewords as useful catalysts or aide memoirs as the whole system is unravelled. The guidewords are helpful but cannot and should not be seen as a substitute for human reasoning and/or imagination; their purpose is to improve the requisite imagination of those who are participative in the activity (Hollnagel, 2004, p184).

In practice a typical HAZOP exercise commences with a simple block diagram of the system under scrutiny. The diagram may be a block diagram of the system's components where the linking pathways are shown or it may be in the form of a flow chart of processes within the system. Each block or process is systematically considered to determine its attributes such as operator action, output signal, input signal etc. Each individual attribute of the system is then scrutinised and challenged using the guidewords in order to establish what could happen if that particular block or process was to not function as planned. In each case, consideration is taken of any hazard(s) that may occur by the action of applying a guideword. Note that due consideration must be taken of multiple faults and hazards being generated from a challenge by a single guideword. The output of each discussion should be recorded in an appropriate log showing what part of the system was being reviewed, the attribute identified, the guideword which was applied and the nature of any hazards identified. Additionally, and of great importance, are the reason(s) behind the study group's identification of the hazard, which should also be recorded within the log. The author believes that this final piece of information is extremely useful when it comes to revisiting the log as part of a review process or in determining the root cause of a hazard occurrence which may have been omitted from the initial HAZOP exercise. In the case of an inquiry into a serious occurrence or death the textual descriptions within the reasoning help to understand and convey the mindset of the study group to an investigative panel.

Formatted: Bullets and Numbering

4.12.2.2 Analysing Hazards.

Having identified the potential hazards within a system there is a need to determine if each one of them is realistic and feasible. It is often found during this detailed, and frequently in-depth analysis, that some of the hazards cannot be realised due to the fundamental design concept of the system. When such hazards are identified they may be closed down within the Hazard Log together with the reasons for such an action. For hazards which have a form of mitigation within the system design they should be appropriately described and recorded within the Hazard Log. It is important that such hazards have their mitigations recorded so that any subsequent changes to the system, or its components, do not undermine the mitigations and allow these hazards to become real. The remaining hazards which appear to be realisable and realistic should remain open and valid within the Hazard Log. The author suggests that caution and due diligence should be applied at all times when sentencing

hazards and/or reviewing their mitigation mechanisms; it is extremely easy for those who have been heavily involved in the creation of the initial Hazard List to make erroneous, simplistic and unconscious assumptions during this phase of hazard sentencing. A form of independent peer review or the use of an accredited professional such as an ISA is recommended (IET, 2008a).

Having completed the initial review of the identified hazards the remaining hazards within the Hazard Log require categorising according to their risk level. This activity determines the likelihood of a hazard resulting in an incident and the severity of an injury or damage resulting from the occurrence. The process used in such an approach is identical to that used in the qualitative assessment of risk which is described in the following bullet points. The process of qualitative risk assessment is often used to eliminate those hazards that represent negligible or acceptably low risk conditions from any further analysis.

Having classified the risks from the identified hazards, the classification data should be entered within the Hazard Log accompanied by the predicted outcome of the occurrence. Note that it is possible for more than one outcome to result from a single hazard and that more than one hazard could have the same outcome. Garman (2006) states the example that the outcome of an engine failure in an aircraft could be that the aircraft crashes to the ground yet other hazards may cause a similar outcome such as a catastrophic structural failure. Another outcome could be a forced landing with an implied lower severity.

Those risks which are classified (see following text on qualitative risk assessments) as trivial or broadly acceptable require no further action and may be formally recorded as such within the Hazard Log. Risks which are classified as trivial or broadly acceptable should not be duly forgotten or ignored; if there are further simple and relatively cheap methods of further reducing the residual risk then further risk mitigation should be implemented though they are considered of lower importance.

If, during the risk analysis activity, any risks within the system have been classified as higher than (worse than) trivial or broadly acceptable then further analysis should be conducted to enable a more detailed understanding of the likelihood and consequences to

be developed. Further analysis often requires a quantitative approach and the use of more refined tools which are discussed in the following text.

Formatted: Bullets and Numbering

4.12.2.3 Quantitative Risk Estimation.

Estimates of the likelihood that a hazard will be realised are often qualitative rather than quantitative, and generally speaking, duty holders under the occupational health and safety legislation should adopt authoritative good practice to address any significant hazards which may arise from such activities (HSE, 2001a). Before we can effectively move ahead with a discussion on either the quantitative or qualitative risk assessment arena there is a need to understand some of the foundational concepts applied to risk management.

Risk assessment and risk management procedures employ a number of safeguards which ensure that the applied approaches are inherently precautionary and are in line with the precautionary principle (HSE, 2001a). This principle has been defined, for example, by the United Nations Conference on the Environment and Development (UNCED) in 1992 as;

"*where there are threats of serious or irreversible environmental damage, lack of full scientific certainty shall not be used as a reason for postponing cost effective measures to prevent degradation*" (HSE, 2001a).

This example, though originally conceived to support the environment, (in particular those of a 'global' context such as ozone depletion and climate change), helps to illustrate the precautionary principle. The principle describes a philosophy that should be adopted for addressing hazards which are a subject of high scientific uncertainty and dismisses the lack of scientific knowledge as a reason for not taking preventive action (HSE, 2001a).

Many sectors of industry, especially those where the potential consequences are serious (e.g. Nuclear Power, Aerospace), have used quantitative risk assessment (QRA) as part of their routine safety management system for many years. QRA is a powerful tool for demonstrating the relationship between and within different sub-systems and the intra-dependencies within context of the whole system. Though QRA is frequently used to both demonstrate and support safety arguments care is required to avoid some of the pitfalls that

can be suffered (HSE, 2001a). For example, when estimating the likelihood of an event by analysing historical incident data, caution should be taken when selecting, the sample, the time period and/or the statistical method employed for analysis. The use of an inappropriate data set or data manipulation tool may give rise to a false set of conclusions and recommendations which may result in a misaligned risk management strategy.

Despite the potential for such pitfalls, the process of QRA can lead to a much better understanding of the prime components which contribute to the weaknesses within a system as well as allowing a mathematical estimation of the inherent and residual risk(s) to be derived. The standard of the data, its manipulation and its interpretation can grossly affect the numerical output and must be borne in mind when being used to underpin a risk management decision. The HSE states that the use of numerical estimates of risk by themselves can, for many reasons including those listed above, be misleading and cause decisions to be made which do not meet adequate levels of safety (HSE, 2001a). In general terms, the numerical estimates from QRA should be combined with qualitative learning and any other information available from engineering and operational analysis in order to make a more refined and matured overall risk management decision.

Many tools are available to conduct a QRA. The following few paragraphs provides a brief overview of the prime tools used for QRA within the author's work environment. This text is designed to provide the reader with a broader understanding of some of the techniques used.

A QRA is most likely to be performed on a single occurrence of a particular event such as the launch of a weapon or operation of an emergency release valve. During such events, the risk to persons involved in the activity or sufficiently close to the event to be affected by it can be calculated by the methods (tools) suggested within the following paragraphs. Though there are many risk criteria available to be used as the top level event (e.g. minor injury, major injury, death etc.) the author has defaulted, where appropriate, to that of death in alignment with his working environment and thesis context.

Fault Tree Analysis (FTA) is a QRA tool which was developed by the Bell Telephone Laboratories for analysing the causes of hazard, not for the identification of hazards. Prior to commencing with an FTA approach it is necessary to identify and understand the top level event which requires analysis; this is predominantly done by the hazard identification and analysis process discussed previously in 4.12.2.1 and 4.12.2.2 respectively. The FTA approach is designed to link the top level event(s) to all of the basic hazards and causal components; in most cases the top level event(s) will have been identified and logged within the system's Hazard Log. In reality, many of the intermediate steps which link the top level event to the bottom events (causes) may not exist; in the majority of cases they are created from the varying combinations of the individual causes and are used to help evolve and calculate the risk associated with the top level hazard.

FTA is based primarily upon Boolean logic and is used to describe combinations of individual causes. A Boolean AND gate is used to link a number of individual events where all of the events must occur together if a hazardous outcome is to be attained; similarly, if any of the incoming events do not occur then a hazardous outcome is not attained. A Boolean OR gate is also used to link a number of individual events where, if at least one event occurs, a hazardous outcome will be attained. On occasion, a Boolean Exclusive-OR gate may be used where a hazardous outcome will be attained from the gate when one, and only one, of the incoming causal events occurs though this application is not common.

Few people are comfortable working with Boolean algebra. FTA allows the use of a graphical method for applying Boole's logic processes; it also allows for the effective decomposition of a top level event down to its root causes. Note that FTA is primarily a top-down construction technique which works down from a chosen top level hazard; the construction should not be confused for a time sequenced structure. Each level of an FTA should be viewed as a more detailed picture of the same top level hazard and therefore represents the same snapshot of the hazard decomposition at the same point in time. A typical example of an FTA is shown in Figure 4.6. The calculations associated with each type of gate can be simply stated. In the case of an OR gate, the probabilities of one or more of the events occurring is the sum of the incoming individual probabilities (ignoring conditions of mutual exclusivity). In the application of an AND gate, the probability of all

of the incoming events occurring together is their product (again ignoring conditions of mutual exclusivity).

Further information on the features of FTA is available from other sources such as Vesely (1987). Whilst FTA allows a top level event to be decomposed down to its root causes it does introduce some limitations; FTA may only deal with timed sequences in an extremely limited manner.

Event Tree Analysis (ETA) is based upon a generalised decision tree model which involves forward searching from an initiating event; in its simplest, and most common form, the initiating event is followed by a number of binary decisions. The various path outputs (usually two) from the binary decisions lead to one branch being a successful event and the other to an unsuccessful event. Probabilities may be applied to each branch where the sum of the probabilities, at each branch, is equal to one.

ETA can become very complex, especially when applied to very large systems or when applied to a long sequence of events. ETA is extremely useful if applied to parts of a larger system where further analysis is required to effectively understand the hazards that may exist within a particular region. Further information on the features of ETA is available from other sources such as Skelton (1997).

4.12.2.4 Qualitative Assessment of Risk.

Formatted: Bullets and Numbering

The qualitative assessment of risk, which was introduced in the previous section on hazard analysis, should be viewed upon as the foundational step in any assessment of risk. Estimates of risk are quite often qualitative in nature rather than quantitative, and they are often based upon a form of systematic observation (HSE, 2001a).

The HSE in its publication '*Reducing Risks, Protecting People*' (HSE, 2001a) uses the example of Pinner Fair on the north-west outskirts of London to illustrate the qualitative approach to assessing risk. In 1993 it observed how the whole event was set up, how it was run and how it was dismantled; they also analysed its safety management of 50,000 visitors amongst the relatively restricted streets of Pinner town. The hazards identified included

overcrowding during the fair and the presence of crowds during erection and dismantling activities.

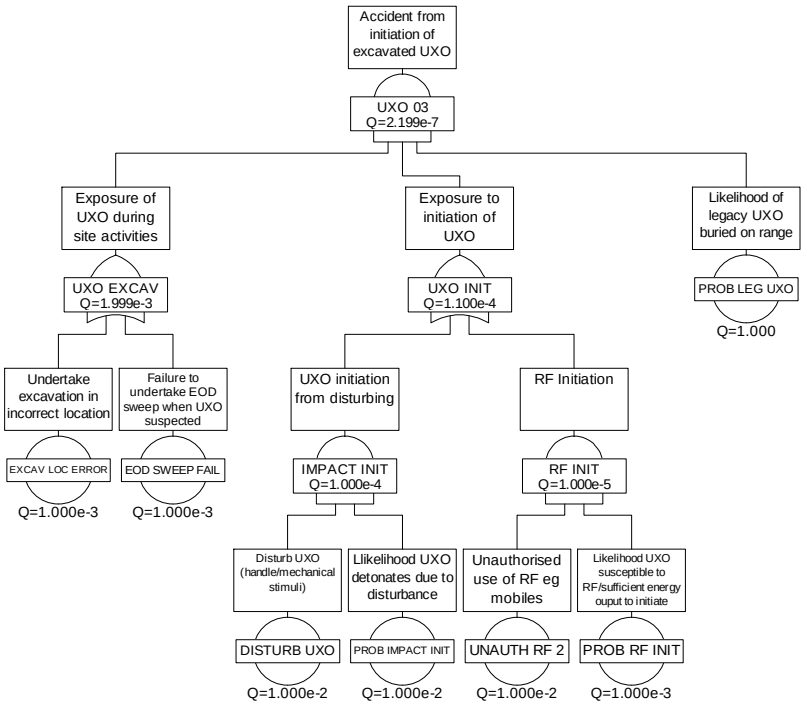


Figure 4.6 - Example of Fault Tree Analysis (FTA), (Garman, 2006).

By drawing comparisons with established codes of practice and guidance documents and by listening to the views of local residents, local authorities and the police a qualitative view of the whole event was created. By this method, established experts in safety management were able to show how some straightforward changes in the event's organisation and layout could eliminate some hazards and substantially reduce the risks from others (HSE, 2001a). As an aid to establishing priorities the improvements were ranked qualitatively using a five point scale from '*very low*' to '*very high*'.

The findings of this qualitative risk assessment were discussed with several interested parties, including the local authority, the emergency services and the Showmen's Guild of

Great Britain leading to an aligned adoption of improvement measures targeted towards crowd safety. A further follow up review of the fair was conducted the following year which highlighted some significant improvements.

One of the underpinning and crucial factors of any qualitative risk assessment is that the determination of the likelihood and severity of any identified risk is a matter of judgement. Within the author's highly regulated working environment access to both learned and experienced individuals, to conduct appropriate judgements, is relatively easy though it can be appreciated how such an approach to assessing risk can quickly degenerate into a diluted and even farcical affair in lesser environments. More specific guidance is offered by the HSE upon the use of qualitative risk assessment.

The following text and tables demonstrate how the author's environment manages the concept of qualitative risk assessments within the environment of T&E, specifically within the safe management of trial activities on the Ranges. The first steps of such an approach is to determine the likelihood that a hazard will cause an incident and, then, to determine the probable outcome of the incident.

Accident Frequency	**Occurrence of Event**	**Time based Frequency for single event**	**Hour based frequency (approximate)**	**Event based Frequency for single event**
Most Likely	Will occur often during the trial activity.	Up to 1 per 3 months, or, 4 times per year.	Up to 3.5×10^{-4}	Up to 1 per 100
Likely	Will occur several times during the trial activity.	Between 3 months and 3 years.	Between 3.5×10^{-4} and 3.5×10^{-5}	Between 1 per 100 and 1 per 1,000
Unlikely	Will occur some time during the trial activity.	Between 1 per 3 years and 1 per 30 years.	Between 3.5×10^{-5} and 3.5×10^{-6}	Between 1 per 1,000 and 1 per 10,000
Most Unlikely	Will occur possibly during the trial activity.	Less than 1 per 30 years.	Less than 3.5×10^{-6}	Less than 1 per 10,000

Table 4.5 - Risk Likelihood Categories, (HSE, 2001a).

Tables 4.5 and 4.6 identify the criteria for qualitatively categorising both likelihood and severity respectively. Again, the author caveats this approach with the requirement to use experienced and varied judgement for this activity. It should be noted that if any doubt is raised as to which category a hazard falls within then the highest of the likelihood and/or severity ratings should be chosen. Having established the likelihood and severity of the hazard its overall risk classification must be determined. This is done by cross referencing the likelihood with the severity (the shaded columns); this is further illustrated in Table 4.7.

Severity of Outcome	Definition of Personal Injury	Definition of Environmental Damage	Definition of Damage to Valuable Asset
Death	Death	Severe national or minor international environmental damage	Loss of asset and put Company's future at risk ≈ £100M
Serious or Chronic Injury	Single or multiple major trauma injuries or multiple severe occupational illness	Severe regional or minor national environmental damage	Loss of asset costing > £10M
Slight Injury	Single/multiple 3-day accidents or single/multiple occupational illnesses	Severe Range-based or minor regional environmental damage	Loss of asset costing > £1M
Trivial	Single/multiple minor or trivial injury or multiple minor occupational illness; or no measurable effects	Minor Range-based environmental damage or no measurable effect	Loss of asset absorbed within project budget or no measurable effect

Table 4.6 - Risk Severity Categories, (HSE, 2001a).

Additional information may be included during this activity such as applying weighting figures to assist in the identification of, or delineation between, certain specific risk boundaries. Such an approach may be used as default conditions by which certain risks are raised to more senior management for consideration.

	Death	Serious/Chronic Injury	Slight Injury	Trivial
Most Likely	A	A	B	C
Likely	A	B	C	C
Unlikely	B	C	C	D
Most Unlikely	C	C	D	D

Table 4.7 - Risk Classification Table, (HSE, 2001a).

The final classification of risks identified within Table 4.7 may be correlated and sentenced with the business' daily operations according to the entries in Table 4.8. When all of the risks resulting from the identified hazards have been classified the information should be formally documented within the system's Hazard Log together with all of the expected outcomes. As previously stated, any risks classified in the Trivial or Broadly Acceptable region (Class D) need not require any further in-depth analysis.

Risk Classification	Operational Risk Classification
A	High Risk Stop work activities and improve and/or increase controls immediately
B	Medium Risk Improve or increase control measures
C	Low Risk Monitor control measures for continued effectiveness
D	Trivial / Broadly Acceptable Risk Light Monitoring / No Further Action Required

Table 4.8 - Operational Risk Classification Table, (HSE, 2001a).

All risks identified as high (Class A) must be reduced; this entails identifying additional risk reduction measures and a further iteration of hazard identification, hazard analysis and risk classification Such a complete and holistic iteration is required to guard against any new hazards which may be inadvertently introduced by the revised risk reduction measures. It should be noted, that for *most* industries and/or businesses that a task (risk) which cannot be down graded from a Class A to a Class B, or lower, cannot be executed. Once all

remaining risks are reduced to a Class B or lower it is necessary to determine if all of these risks have been reduced to As Low As Reasonably Practicable (ALARP).

Formatted: Bullets and Numbering

4.12.2.5 The ALARP and Disproportionality Argument.

The As Low As Reasonably Practicable (ALARP) concept is based upon the weighing of risk against the trouble, time and money needed to control it (HSE, 2008a). Thus, the ALARP principle describes the level to which we expect to see a workplace risk being controlled (HSE, 2008a). The HSE effectively describes ALARP by means of a diagram (Figure 4.5) whereby risks falling within the Tolerable Region (Class B and Class C risks) may be tolerated provided that they are aligned to the ALARP principle. Having identified, analysed and estimated the risk present in a system using some of the previously discussed methods there is a need to demonstrate that the residual risks to individuals, both for workers within the environment and the general public, have been reduced to the lowest level that is reasonably practicable (the ALARP demonstration) (MoD, 2004).

The application of 'reasonably practicable' can be quite an onerous task, especially when dealing with individuals who have peripheral knowledge of the principle. From the author's own experiences, many individuals try to use the ALARP argument in an inappropriate way, predominantly to underpin investment cases where the initial business case has been challenged or rejected.

The test for risk reduction being in accordance with the concept of ALARP is determined to occur when the cost of any further risk reduction is not grossly disproportionate to the benefits accrued from the reduction (HSE, 2001a). One of the fundamental issues with this concept is to establish a common metric to measure benefit in the same units as the cost of further risk reduction. Within the context of the author's working environment, Defence Standard 00-56 introduces the concept of undertaking a cost benefit analysis when deciding if risks have been mitigated to a level which can be justified as ALARP. In the case of this project the use of relevant Joint Services Publications (JSPs), in particular JSP 553 (Military Airworthiness Regulations), and JSP 403 (Handbook of Defence Land Ranges Safety) will be used in any safety argument. Further guidance from the Civil Air

Publications (CAP) 670 and 722 will also be considered when developing any ALARP argument.

When there are several risks which interact then there is a requirement to balance the controls to achieve the best overall solution. It should be noted that HSE guidance suggests that the ALARP case must be fit for purpose, i.e. if the risks are high then a more rigorous demonstration of ALARP is required. This degree of rigour must also depend upon the consequence level whilst further thought should be given to any assumptions or conclusions drawn from uncertain sources such as modelling. In the absence of similar technical papers within the Range's environment the author has drawn much from the demonstration of ALARP from the Nuclear Safety Directorate (Vaughan, 2005) as well as other industries.

It is normally considered appropriate, and aligned with 'reasonably practicable', to spend up to the value of the benefit delivered, at the Tolerable/Broadly Acceptable boundary. At the Intolerable/Tolerable boundary it may be appropriate to spend many times more than the value of the benefit delivered (HSE, 2001a). In any ALARP driven calculations, the cost of the whole life expectancy of the item generating the hazard should be considered. When contemplating the aforementioned in any business calculation for an operational year the argument must consider the likelihood that an accident will occur in that year. Correspondingly, the spend is reduced as the likelihood of an accident reduces. From a more holistic perspective, there are other peripheral business benefits from spending and therefore reducing residual risks such as higher staff morale, minimised lost time due to accidents and even lower staff turnover. Many of these peripheral benefits are linked to the social and cultural aspects of a safety climate; these are discussed at length in chapter six of this thesis.

It should be noted that before any prolonged discussion is commenced on the concept of applying an ALARP argument to any situation it is presumed that the essential demands of the TOR and any Cost Benefit Analysis (CBA) frameworks have been met. This means that suitable and appropriate safety measures are in place to ensure that no person is at an intolerable level of individual risk, and that all safety measures have been implemented for

which the safety benefits (B) are greater than or equal to the costs (C), estimated using the current values of preventing fatalities and injuries (Evans, 2005). Whilst the application of a simple CBA to identify the criteria for suitable safety measures may seem wholly sensible, i.e. safety measures should be implemented if $B \geq C$, there are situations where such an approach may not be appropriate. Such situations may arise if the hazard is linked to industries where accidents may result in multiple deaths or wide reaching environmental damage. Other elements which may affect the use of a simple CBA evaluation for risk control may include societal pressure or even international ruling on certain industries. Such industries include, but are not limited to, defence, aerospace, nuclear power generation and the rail industry. To take the TOR and CBA frameworks further and to introduce additional constraints on any reluctance to spend to avert death or injury a disproportional factor (D) may be applied to the cost analysis; safety measures should therefore be implemented if $DB \geq C$, where D is greater than 1.

The adoption of a disproportion factor may or may not be a legal requirement and conceptually it is not really required given the current western world's valuations to prevent fatalities (Evans, 2005, p20). Today's 'willingness to pay' attitude of society is reflected in the following valuations for preventing fatalities. Typical values (normalised for 2003) for the transport industry (Roads) are shown in Table 4.9, they clearly show how road valuations of preventing fatalities have increased over the past five decades (Evans, 2005). The table is very useful in illustrating how the "value" of life can change as a function of societal opinion and/or culture.

Year	Value at Original Prices	Value at 2003 Prices
1952	£2,000	£36,380
1963	£7,880	£104,360
1971	£18,420	£164,760
1978	£89,300	£323,800
1987	£500,000	£889,600
2003	£1,312,260	£1,312,260

Table 4.9 - Road Valuations of Preventing Fatalities for Selected Years.

The figures used for road appraisal in the 1950s were not based upon public perceptions and willingness to pay; they were much lower, in real terms, than today's values. In a similar manner, the awarding of compensation payable to dependants for accidental death at that time was also, and still remains, lower than the 'willingness to pay' based valuations to prevent fatalities (Evans, 2005). Based upon the aforementioned, it may be argued that there was a clear need to introduce the disproportionality factor given the low valuations for preventing fatalities which were being applied in 1949 when the term was introduced. Given today's higher valuations for preventing fatalities the need to apply the factor outside the more specialised, high risk - high consequence, industries is minimal.

Current guidance offered by the HSE (Nuclear Directorate) offers some advice on the application of gross disproportionality and the probability of seeking its application in the courts (HSE, 2009a). Part four of its Technical Assessment Guide (TAG) to provide nuclear directorate inspectors with guidance states that "*the law does not recognise an acceptable region other than when ALARP has been met*". It also clearly states that "*there is no precise legal factor or HSE algorithm for gross disproportion*". The TAG suggests that the evidence delivered by John Locke, the then Director General of the HSE, at the Public Inquiry of the Sizewell B incident should be used as a foundation for any application for disproportion. Whilst this approach may be considered as quite dated there has been no other event or inquiry since that time which has provided any alternative options or opposition. Locke suggested that a disproportion factor of up to three should be used for workers whilst a variable factor should be used for the general public which depended upon the level of risk that they were exposed to. For activities where the risks are relatively low the factor applied should be around two; as the consequence and/or likelihood rises then the disproportion factor will gradually increase towards ten.

Further guidance on the application of a disproportion factor is given in Annex 1 of the HSE's guidance document for ALARP decisions in the Control Of Major Accident Hazards (COMAH) (HSE, 2009b). The document suggests that "*The necessary degree of disproportion is generally considered to be low near the negligible criterion, rising to in effect infinity at the maximum tolerable criterion*".

Basically what this points to is that within the tolerable region of the TOR framework (the inverted triangle) the degree of disproportion applied is inversely proportional to the level of relevant good practice and risk reduction measures that have been applied as the ALARP justification. A convincing and clearly demonstrable ALARP argument would be favourably received by the courts, resulting in a lower disproportion factor being applied.

In summary the HSE may apply the concept of gross disproportionality to the justifiable costs of reducing a risk; this requires that for higher risks they shall only be considered to be aligned with ALARP if the cost of further risk reduction is grossly disproportionate to the improvement gained. At the lower end of the ALARP region (just above the broadly acceptable region) the gross disproportion factor, shall be 1. At the top of the region (just below the intolerable region) the factor shall be a figure much greater than 1, usually determined by a weak ALARP argument and even some degree of societal perspective.

The actual level of gross disproportionality can be calculated as;

$$D = [\,[\,(X - A) \,/\, (I - A)\,] \times 9\,] + 1$$

Where; D = Gross Disproportionality Factor
X = Annual Risk of Fatality
A = Broadly Acceptable Accident Rate
I = Intolerable Accident Frequency

The factor, D, can then be used to decide the practicable level of ALARP spend that could reasonably be expected to reduce the overall risk to the broadly acceptable level, this is shown by;

$$S = X \times V \times D$$

Where; S = Reasonably practicable ALARP spend
V = Value of prevented fatality (VPF)

As each Class B and Class C risk is considered in turn to determine if any further risk reduction measures are feasible within the ALARP budget then an appropriate entry should be made in the Hazard Log and any Risk Assessment database. During such an exercise it is important to include a review team who are experienced and from a varied background to avoid inappropriate sentencing and the use of unconscious assumptions. The area of greatest concern is at the Intolerable/Tolerable boundary where societal views, often founded upon superstition and/or ignorance, may affect sentencing.

Formatted: Bullets and Numbering

4.12.2.6 Reducing the Risk and Accepting it.

Many techniques are available to help reduce risk; the most important and most desirable are quite often relatively rudimentary in nature (HSE, 2006a). The four most common approaches are listed in Table 4.10.

Risk Reduction Method	Effect Upon Hazard
Hazard Elimination.	Complete removal of hazard thus eliminating any associated risk.
Hazard Reduction.	Reduction of a hazard occurrence. This may be achieved by minimising the number of occasions when a condition could lead to a hazard occurring.
Hazard Control.	Reducing the likelihood that a hazard will lead to an accident. This may be achieved by reducing the time duration for which a hazard is present or by minimising exposure to the hazard.
Damage Minimisation.	The consequences of an accident are reduced; its severity is reduced.

Table 4.10 - Risk Reduction Methods.

In reality, the risk reduction techniques identified within Table 4.10 may be used singularly, or as combinations, to achieve the desired effect of risk reduction. The author offers a relatively simple example from his working environment to illustrate risk reduction in the real world. When launching a surface to air weapon system the launch area (danger area) will be controlled to minimise exposure to people. Additionally, any workers actively involved in the activity, such as arming, will be under cover during the actual launch so that in the unlikely event of, for example, a premature explosion they will be protected from

blast and fragmentation effects. Any instrumentation deployed on the trial will either be outside the weapon's potential debris boundary or be contained appropriately to reduce damage.

With any application of risk reduction due diligence should be carried out on any adopted techniques, especially when applied after a lengthy analysis, to ensure that none of the employed methods have inadvertently introduced new risks. Any risk reduction employed must be appropriately documented in the system's Hazard Log.

Having conducted all of the preceding activities to identify any residual risks within the system they must be accepted by a body or individual as being appropriate for the business or environment. The risk acceptance process demands that the residual risk afforded by a system is compared with an agreed level of tolerability. Final and formal acceptance of the residual risks will be conducted by a person, or persons, defined within the system's Safety Management Plan. In general, this will be conducted by independent review within the company and by agreement with a Duty Holder within the customer's organisation. Some projects and systems, especially within the author's working environment, will require review by an Independent Safety assessor (ISA) prior to formal sign-off.

Formatted: Bullets and Numbering

4.13 Limitations of Current Conventions.

The benefits offered by the application of a structured and formal safety case are numerous; they provide not only an improved understanding of the hazards and risks involved in a system but an enhanced knowledge base of the technical and managerial controls required to manage them (Wilkinson, 2002). By adopting such a structured approach they allow ISAs and regulators with a better oversight that the system or operation, as a whole, is effectively and appropriately managed. When applied in a consolidated form they should lead to the principal goal of reducing the numbers of, and consequences of, all major accidents.

The HSE and the industries which it regulates have experienced a number of difficulties in the application of safety cases including their sheer size and quite often, their complexity (Wilkinson, 2002). Of note are occurrences where safety cases have been created which

lack any usefulness to the workforce's operations or the 'stretching' of probabilistic figures (QRA applications) beyond any reasonable usefulness (Wilkinson, 2002). In certain circumstances the HSE have found it difficult to explain to the public how these safety cases were accepted.

The ultimate test for the success, or failure, of an approach which utilises safety cases is whether or not the frequency of major accidents is reduced or not. Fortunately within a modern and developed society occurrences in the latter are relatively rare. Does such an observation indicate that safety cases are improving our safety management process or has our socio-technical evolution taken us away from many of the more basic and riskier activities? More time is probably required to allow this question to be answered; the HSE is only just starting to receive safety data produced from the Control Of Major Accidents and Hazards (COMAH) legislation (Wilkinson, 2002).

Wilkinson (2002) states that "*the near universal opinion of managers and most of the workforce at hazardous installations is that safety cases have been very successful.*" Whilst this statement is relatively general in its approach, Wilkinson does offer a supporting view from the HSE's office. The HSE, from its experiences within the nuclear, onshore (major hazard), offshore (oil and gas) and rail industries heavily endorses the safety case regime; the inquiry into the Paddington train crash (Ladbroke Grove rail crash) in 1999 can be cited as an example endorsement. Aberdeen University conducted a study to assess the costs and benefits from offshore safety cases which was published in 1995 (Aberdeen, 1995). The study highlighted both the problems and the benefits of safety case applications. In its conclusion it states that the Safety Case Regulations have had "*a positive impact on safety in the offshore oil and gas industry, particularly…a heightened awareness of and more focussed attention on risk, improvements in the management of safety and the better targeting of safety related expenditure.*" A further follow-up paper was published in 1999 detailing the successes and failures from a more experienced perspective; this paper further corroborates the initial positive view of the application of safety cases (HSE, 2005).

One of the major problems that the author has encountered with the majority of safety cases is that of sheer size. As technology advances and systems (and systems of systems) become

larger then so the level of complexity increases to the point that safety cases can become onerous to the point of undermining the top level argument. One of the fundamental tenets of a safety case is that of maintaining an overall picture of the system's safety; in many cases, the sheer number of low level analytical threads combined with large amounts of supporting evidence can threaten clarity.

Most safety cases are produced as a logical, systematic and linear piece of work where arguments and evidence must be cross-linked across various boundaries to ensure consistency and completeness. This is an extremely difficult task which is worsened by the need to use various qualitative and quantitative tools, to engage proficiently with various stakeholders and to ensure clarity when crossing various disciplines.

Irrespective of any tool or process which is adopted to help manage the construction or maintenance of a safety case, it is predominantly people who hold the entity together. From the construction of a safety management system, through the various hazard identification processes to the effective safe operation of a completed system, the whole process is reliant upon key individuals. These individuals use their knowledge, their professional experiences and quite often their personal experiences to conduct design decisions throughout a system's life. Not many safety cases document the assumptions and justifications in sufficient detail to allow an independent third party to understand the mindset and thought processes followed in creating some of the fundamental arguments which underpin a system's safety. The author has experiences where he has strongly requested that additional contextual information is documented within both newly created, and extant safety cases, to ensure that the conditions of mind are recorded to allow subsequent analysis and understanding of the boundary conditions by an independent third party.

The significant contribution of human error to operational safety within systems has been recognised for some time (NATS, 2008). Critical systems such as air traffic management must pay appropriate attention to the human element if safety assurance is to be maintained. National Air Traffic Services (NATS) provides the air traffic management service within the 'controlled' en-route airspace in the UK and at many of the UK's largest airports (NATS, 2008). The organisation also provides air traffic management in the eastern

oceanic region of the North Atlantic and some flight information services to pilots flying outside controlled airspace. Being cognisant of the human error component to ongoing operational safety, NATS have been applying formalised and structured techniques for the analysis of human error. A relatively recent example of one of the techniques used is the human error reduction technique for evaluating systems (HERTES), which was applied to the recent implementation of a new control tower at London's Heathrow airport.

However it is also recognised that whilst human error assessment is a necessary component of human factors assurance, to use it in isolation is not appropriate. Human factors assurance is key to providing a holistic safety argument to any complex, human interactive, system. NATS are amongst a handful of large organisations who are now striding forward in the safety critical environment and incorporating human assurance techniques as part of the overarching system safety case.

In addition to the aforementioned observations raised by the author, Kelly (2008) suggests that there are seven types of 'traps' that should be avoided when creating a safety case for a system or activity. These are;

- *The "Apologetic Safety Case"*; which avoids the uncomfortable truths which may be economically and/or politically unacceptable.
- *The "Document-Centric View"*; which is wholly focussed upon the production of a document rather than a 'compelling safety argument'. Such a document often delivers no safety benefit.
- *The "Approximation to the Truth"*; such safety cases ignore the "*rough edges*" and often avoid fully sentencing all of the identified hazards.
- *The "Prescriptive Safety Cases"*; these are typically repetitive or routine tasks where a relatively high degree of detail is presented which appears on the surface to be convincing but does not deliver a compelling safety argument.
- *The "Shelf Ware"*; such safety cases are merely left to gather dust on the office shelf where they cannot support daily operations. They are also forgotten in any subsequent evolution or revision of the system.

- *An "Imbalance of Skills"*; Skills which are required to not only create the safety case but to effectively challenge the assumptions made.
- *The "Illusion by Pictures"*; The fact that people may be quickly "*dazzled*" by exciting and complex presentations using colour and even hyper-linked illustrations. The quality of the underlying argument is often hidden by stylish or fashionable presentations.

These observations are extremely lucid. The author both agrees with and has experiences of safety case related activities which corroborate Kelly's work. Haddon-Cave (2009, p538) strongly suggests (that) "*this article should be compulsory reading for many of the current purveyors of Safety Cases*."

One of the most difficult tasks when reflecting upon providing any additional contextual information is that of identifying any unconscious assumptions; though difficult to synthesise into a cognitive state it is these aspects which will provide a third party with a key to understanding how the safety case was assembled. A more detailed discussion on the limitations and problems faced within the application of safety cases, especially in relation to human interactions, is given by the author in chapter six of this thesis.

Formatted: Bullets and Numbering

4.14 The Maintenance of Safety Cases.

One of the crucial aspects of safety case management is that of maintaining the safety argument throughout its life (Kelly & McDermid, 2001). The justification of a safe system is a naturally iterative process requiring a part of the system to be developed, analysed, adjusted accordingly and then fed back into the development stage. The process of change therefore forms an integral part of the development and justification process. Once commissioned into operational use, it is highly probable that a system will be subjected to further changes as a function of maintenance and/or 'tweaks' to overcome issues such as performance degradation or component obsolescence. In order to maintain the system's safety argument or to improve its robustness such changes must be carefully fed back into the original safety case (Kelly and McDermid, 2001). In addition to the ever-changing requirements within the system's immediate operating environment there may be additional and/or different challenges that require the safety case to be maintained; typical examples

may include a change in the regulatory requirements or changes in technology. Such is the importance of maintaining a system's safety case after commissioning that many safety standards now formally include it as a safety requirement.

The concept of maintaining a safety case will not be discussed further within this thesis, the topic has been raised here to highlight to the reader that such a problem exists and that due diligence should be applied to any safety case throughout the life of its subject system.

Formatted: Bullets and Numbering

4.15 Future use of Safety Cases within Dependability Arguments.

Whilst a safety case addresses only one key system attribute (safety), there has been increasing interest in their application to address wider issues, predominantly in the field of dependability (Despotou and Kelly, 2004). Dependability is a system property which consists of many system attributes including safety, security, reliability and maintainability.

Whilst attempting to address all of the dependability issues could result in competing objectives there are opportunities to strike a balance between the dependability and safety elements. The idea of using a safety case to justify dependability is driven by the concept that providing an argument about a system's dependability can increase the assurances offered to the developers and users of the system. Though logical in nature, caution should be applied as the focus shifts from the single attribute of safety to attempting to address all of the attributes within dependability. The two main obstacles according to Despotou and Kelly (2004) are the evolution of the argument, and the resolution of conflicts between the evolving attribute objectives.

Whilst the idea of dependability cases is a relatively new and untested concept, the idea of developing such cases for system attributes, other than safety, is not new (Despotou and Kelly, 2004). The UK's Ministry of Defence has required maintainability cases for many of its equipments for some years (Defence Standard 00-40). It is clear that the ability to efficiently and effectively manage any trade-offs as well as maintain a degree of practicality is key to taking such an holistic and multi-attributed case forward. Having already raised the issue of large and impractical safety cases in a previous discussion the author suggests that the ability to satisfy so many stakeholders with so many conflicting

agendas is going to be a large task to complete. Despite such a view, much work remains ongoing in trying to establish a development framework for dependability cases (Despotou and Kelly, 2004).

Formatted: Bullets and Numbering

4.16 Summary.

This chapter has reviewed the background, creation and development of safety cases from many literature sources. By reviewing safety standards and published extant safety case practices the author has uncovered that there is a general lack of a published, formalised and specific structure for safety case creation and development.

The author has experience of reviewing many safety arguments and safety cases in his core role within the T&E environment. It was observed that the majority of safety cases reviewed were presented in a rigid format resembling a scientific or engineering report style. Though this format of presenting the argument has its benefits (document structure, good referencing, demonstration of a logical order to maturity), there is often a disconnect within the structure. Many such safety cases fall foul of poor expression and unclear language as well as an inappropriate and excessive use of quantitative analysis in pursuit of a final deliverable.

Of note for this paper is that the use of GSN and BBN techniques are being investigated by the Rail Safety & Standards Board (RSSB) with an aim to improve the overall efficiency of safety case development within the railway industry (Zhou & Weaver, 2003). Attendance at a workshop by railway safety stakeholders identified the following benefits and limitations offered by each method:

- GSN – To be used in the presentation and development of large scale projects as it is easy to understand and allows for the early identification of objectives and requirements whilst being useful for capturing successful argument approaches. Limitations were seen to include concerns with methodology, argument understanding and general usage.
- BBN – It was suggested that BBN was used to focus upon a specific obstacle within the safety case and to help identify the best solution. Limitations in its application

included issues with its development, predominantly with the use of Conditional Probability Tables (BBN model basis) and usage.

Reviewed papers on UAVS concentrated on large systems which require great decomposition and by default are onerous and daunting. There is a clear need to develop a smaller scale approach for sub-systems or imports of such which plug into existing safety cases; examples include small scale UAVs which require an overall safety figure to effectively 'plug' into extant Range Safety Cases.

Many of the safety cases reviewed suffered from limited resources (manpower, money, time etc) whilst there was a noticeable lack of contextual information to allow effective independent review and challenge. It was also observed that there was a need to strengthen the link between the technical attributes of the system with the 'softer' human factors element. Little, if any, reference was made to individual competency and training whilst no mention was made of the reliance upon the people side of the operation (the safety climate and safety culture). Though highlighted as being instrumental in delivering a safe operation they were not formally recorded as the basis of any argument. An in-depth review of safety culture is recorded in chapter six of this thesis.

The research objective of creating a limited (short) form safety case for smaller and simpler activities seems to be well founded especially when human intervention and/or influence (e.g. operators, maintainers, fault rectification) are both critical and present for the duration of an operation.

CHAPTER 5

An Integrated Air Range Operation

5.1 Introduction.

This chapter describes the author's high level vision of how a centralised Air Range operation, based upon the new TCS investment at Aberporth, may be created. Whilst the project was formalised as a future business consideration by both MoD and QinetiQ within 2008, the author had been tasked to consider the concept informally by the former Air Ranges Manager, Mr Bob Burrows, in 2004/2005.

The following text describes how the author had envisaged the project would be considered; his approach considers all aspects of the requirement to command and control a major T&E capability from a remote site in a relatively simple but holistic manner. The initial text considers what the author believes are the five key components for such an operation. Whilst the first four components are only briefly described the final element, the preliminary safety case, is investigated in more detail. In addition to the technical and operational requirements of the project the author considers the economic benefits of minimising some of the costs which are so prevalent within the extant method of operation and may be minimised through an efficient centralised operation.

The safety case is initially discussed from the author's early perspective and also in the context of his current work with the assigned project team. The chapter concludes by introducing and discussing the pivotal role that human factors, predominantly organisational culture, plays in delivering compliance and the assurance of robustness within any processes which underpin a safety case.

5.2 The Author's Centralised Air Range Vision.

The idea of remotely controlling and commanding such a complex entity as a T&E Range capability naturally suggests that a 'systems' approach should be considered. The author's initial (and premature) thoughts on the breakdown of tasks was heavily biased towards the provision of an engineering solution; subsequent systems thinking and reflection with

regulators and safety practitioners shifted this viewpoint somewhat. To allow the project to be managed more effectively and to allow focus to be maintained upon essential regulatory compliances the author broke the overall requirement into five key components;

- The business rationale;
- The regulatory requirements for legal operations;
- The engineering solution;
- The security aspects of remote data transfer;
- The preliminary safety case for the engineering solution.

5.3 The Business Rationale.

The business strategy for this project can be split into three main components. The first identifies cost savings available by reducing campaigning costs such as the travel expenses of detaching Air Traffic Control (ATC) staff from site to site. The second offers an opportunity to deliver broader cost savings by reducing the number of operational trials teams across the major sites from two to one. Finally an opportunity is created to allow an aligned model of trials conduct to be developed between Aberporth and the Hebrides; this latter element, whilst important, will occur largely through default by controlling both major sites from a single control and command environment.

5.3.1 The Campaigning of Air Traffic Controllers.

The majority of trials conducted across the Air Ranges are supported by Air Traffic Control Officers (ATCOs) supplied, through contract, by National Air Traffic Services (NATS). Upon being initially supplied by NATS to operate from a central pool of controllers, geographically based at Aberporth, they are further trained over a typical nine month period to gain additional and bespoke competencies in Range (T&E) specific tasks. It is only upon completion of this training that they become certified as Range Air Controllers (RACs), a role which is co-regulated between the Civil Aviation Authority (CAA) and the MoD. It should be noted that the term RAC is used solely to describe the role of an ATCO when deployed within the UK Ranges environment. This descriptor helps to maintain the delineation between normal air traffic control competencies and the extended and more

specialised competencies that must be attained prior to being certified valid to operate upon the Ranges. Due to the bespoke nature of Range activities and the special tasks demanded of the RACs the MoD regulator acts as the single competent authority for certifying and licensing the RAC.

The RAC pool is based at Aberporth and that is regarded as their parent site; during periods of low demand and utilisation they are sited there by default. An RAC scheduling tool is used to manage the requirements from the appropriate Ranges. This tool reacts with the same degree of priority and commitment to all of the Ranges unless otherwise advised by the Ranges management team. It should be emphasised that all of the RAC requirements for any Aberporth specific tasks must be requested through the appropriate scheduler.

Whilst RACs are utilised across all four Air Range sites and support ad-hoc tasks at Shoeburyness from the London Air Control Centre (LACC) in Swanwick, this business rationale will focus specifically upon the predominant activities and detachments at Aberporth and the Hebrides.

RACs are deployed to the Hebrides to support with the technical planning (attending trials planning meetings) and for the execution of trials; travelling and accommodation whilst on detachment are respectively time consuming and expensive. Travelling time, by regulation, for RACs is considered as ‘duty time’ and therefore requires a greater number of individuals to be deployed per unit time, predominantly units of weeks rather than single days, to allow for any T&E activities to be completed. This relatively high demand on such an expensive and specialised human resource is often exacerbated by the fact that the weather at the Hebrides is so inclement and changeable (causing programme slippages) and that the Range requires additional air assets to be deployed to support many of the Deep Range operations.

Deep Range trials at the Hebrides include the higher energy activities which require the use of additional danger areas to the North, South and West of the Rangehead location on South Uist. The greater majority of Deep Range activities require support from bespoke and specialised third party assets. These assets may include an airborne sea surveillance

platform such as a Royal Air Force (RAF) *Nimrod* Maritime Patrol Aircraft (MPA) or a commercial platform which offers a suitable and comparable capability. Due to the geographic remoteness of the Range and the nature of T&E the majority of the activities require the attendance of air to air refuelling assets. The pressure on such assets within the current political environment, predominantly due to theatre operations, causes trial operations to be frequently postponed or delayed. Such operationally vagarious elements, when combined with the constraints of travelling and inclement weather, make the concept of a remotely controlled operation extremely attractive. Given all of the aforementioned potential for problems the ability of the business to schedule and conduct trials to an efficient and well planned schedule is extremely difficult. The problem is also magnified by today's cost-conscious business environment as effective cost gathering and financial forecasting, especially in response to early bid work, is very difficult to bound. For example, having deployed RACs to support a task based upon a bid which was constructed on the basis that two RACs would deploy for a fortnight the business may find itself extending the deployment period to six weeks and incur increased accommodation and travelling costs to the order of three times that identified within the original bid.

The Inner Range activities at the Hebrides require the use of its inner Danger Area (D701) which is utilised primarily by detachments of military units for live in-service practice of GBAD systems. This activity predominantly involves the engagement of *Falconet* and/or *Banshee* aerial targets by live *Rapier* missiles. Sea surveillance for these relatively low energy in-service activities is provided by Range owned, land based, maritime surveillance radars; there is no requirement for any third party support for these activities. Due to the relatively short ranges of these engagements and the use of a relatively small and slow aerial target combined with low altitude geometries there is no requirement for an RAC to be present. Whilst air surveillance radar systems are operated during such activities the task of monitoring the Danger Area for air intruders is carried out by Range staff with special licenses administered and controlled by the MoD regulator. These licences are predominantly based upon 'grandfather rights' predicated by the site's Royal Artillery history.

It could be argued that by basing a team of suitably competent RACs at the Hebrides the costs of deployments would be minimised and also provide additional flexibilities. Whilst this approach offers some superficial benefits it is undermined by the lack of operational utilisation at the site and therefore an inability to remain competent and current in accordance with the prescribed regulatory framework. It is formally accepted by the regulator and bound into the certification regime of the RACs that the extended variety and volume of activities carried out at Aberporth must be used to underpin the whole competency framework of RACs across all of the UK's T&E capabilities. By basing RACs at the Hebrides costs would be incurred, probably at a higher frequency, in deploying them back to Aberporth for currency and continuity training; neither currency nor full competency in all aspects of the RAC role may be attained whilst solely based at the Hebrides.

5.3.1.1 Reducing Campaign Costs.

The author tasked a member of his former operational management team at Aberporth to conduct a preliminary investigation into the additional costs incurred for RAC deployments during 2005 and 2006 (Richards, 2006). The following summarises the report;

Contracted cost of NATS staff	(Year 2004-05)	£635,000
Additional costs incurred	(Year 2004-05)	£79,000
Contracted cost of NATS staff	(Year 2005-06)	£661,000
Additional costs incurred	(Year 2005-06)	£105,000

**Note: Additional costs incurred include Car hire, Travel & Subsistence, Additional Hours (Overtime) and Additional Voluntary Attendance (Voluntary Non-rostered support).*

Another report (Harries, 2009) which provided a business argument for increasing the RAC pool of resources identified similar cost components for 2007, 2008 and the first quarter of 2009.

Contracted cost of NATS staff	(Year 2006-07)	£686,000
Additional costs incurred	(Year 2006-07)	£120,000

Contracted cost of NATS staff	(Year 2007-08)	£710,000
Additional costs incurred	(Year 2005-06)	£104,000
Contracted cost of NATS staff	(Year 2008-09)	£695,000
Additional costs incurred	(Year 2008-09)	£114,000

**Note: Additional costs incurred include the use of a semi-retired RAC to support operations at Aberporth whilst the core pool was deployed on other Ranges.*

Whilst these figures may not be directly comparable, due to slight variances in what the cost constituents are, they give a good indication of the order of magnitude. For the five year period highlighted, the annual average additional costs incurred, which can be apportioned to the Hebrides, may be considered as £100,000.

These aforementioned costs do not include the return airfare from/to a mainland airport (e.g. Bristol, Heathrow, etc.) to/from Benbecula, and an overnight stay in Glasgow. Due to the many variables which can affect trials conduct the RACs book 'fully flexible' tickets at an unit cost (2009 prices) of £650 per flight. Whilst the RACs are content to overnight in relatively cheap accommodation (e.g. Holiday Inn) at Glasgow airport, each nightly stay costs a typical £100.

The average number of RAC deployments to the Hebrides, per year, over the past 4 years may be considered as a conservative 25; this is a difficult figure to finalise given the nature of some of the trips and that a more efficient method of scheduling RACs has been adopted since 2008. For the purposes of this thesis the figure of 25 is fair and appropriate. It can therefore be seen that the typical annual costs of deploying RACs to support the Range activities at the Hebrides is made up from the following components costs;

(Annual average additional costs incurred excluding flights & hotel) + (Annual cost of flights & Hotel accommodation);

= (£100,000) + (£650 + £100)25
= (£100,000) + (£18,750) = £118,750.

If all of the T&E activities currently being carried out in the Hebrides could be conducted between the other three Ranges then some reduction in manpower could be made but this is impossible due to the requirement for its larger danger area to accommodate the higher energy T&E activities. Moving the activities currently carried out at Aberporth to the other three Ranges is also not a realistic option given that the majority of Aberporth trials cannot be physically executed (hazard area size) at Larkhill or West Freugh. To migrate the Aberporth activities to the Hebrides would be extremely difficult given the excessive depth of water and climatic conditions (predominantly sea-state) for mooring any surface targets in support of air to surface or surface to surface weapon activities. Additionally, the cost to the customer of deploying to the Hebrides would be simply too onerous for many low budget projects. The dependence upon so many mission critical third parties and the level of such inclement weather would also impact upon the viability of conducting many activities at the Hebrides.

An additional but very important intangible benefit of this review was to quantify the overall utilisation of such expensive assets as RACs. In investigating some of the RAC deployments to the Hebrides the author has identified that they are typically underutilised by circa 40%. This is largely due to the transit times, pre-trial preparatory periods and the slippages of trials activities due to inclement weather and/or third party support asset failures. In response to the RAF's growing demands to exercise more third generation weapons (e.g. *AMRAAM*) the average deployment to the Hebrides involves 50% of the NATS resource pool. The under utilisation of the RACs may therefore be calculated in financial terms as 20% of the overall contract cost (40% x 50%) which is in the order of £130,000. When combined with the previously identified annual costs of deploying the RACs to the Hebrides (£118,750) we start to gather a much more refined figure of how much the deployments are costing in real terms to the business; i.e. £250,000 per annum.

By transmitting the required data from the Hebrides to Aberporth a more cost effective and operationally dynamic method of Range management can be adopted. Any slippages in the ability to execute a trial at the Hebrides, either due to weather or un-serviceability of third party assets, can be met by a more tactical and flexible method of scheduling trials through the use of a common command & control system based at Aberporth.

5.3.1.2 Aberporth as the Command & Control Base.

Whilst the author has suggested that the location of the centralised system should be Aberporth this view is personal and wholly driven by the fact that the NATS resource pool is based at the site. From a 'people perspective' the author is aware that the NATS staff have settled their families within West Wales and are relatively content with their personal situations. No doubt there are opportunities, supported by sound business arguments, to locate the centralised system at another QinetiQ and/or MoD site within the UK. The author is cognisant of such thoughts and is supportive of them to some degree; however there are two prime issues which should be considered before taking any revised idea on relocating the command & control system forward.

The first issue is very simplistic and is based upon the realisable cost savings as identified in the preceding paragraphs. If the control & command centre is relocated away from where the air traffickers live then the cost saving opportunities will be greatly reduced as they will be required to travel again to another location. Whilst the costs may not be as substantial as they are currently the volume will be greater; that is, travel will be required for all trial activities rather than for the ad-hoc deployments to the Hebrides.

The second issue follows a more intangible and people-centric theme. The RACs hold very specialised competencies and are essential to the continued delivery of trials activities to the MoD in accordance with the LTPA contract. Whilst their service contract includes clauses to allow a professional handover to another supplier, the author believes that to lose their support would be detrimental to the competent delivery of trial activities. The world is currently struggling from a gross lack of air traffic controllers and in response to this demand their collective salaries have risen worldwide. The air traffickers employed on the Ranges are not paid as highly as those conducting mainstream civil air traffic duties but they remain relatively content to carry out Ranges activities due to its 'exciting', 'niche' and 'elite' job type. This contentment is galvanised by the lifestyle afforded by living in a rural environment, especially when infants and young children are part of the family. It is suggested by the author that any relocation of the control & command centre away from Aberporth may upset this status quo and initiate a team fragmentation where the NATS

team members may decide to rejoin mainstream air trafficking, with a corresponding substantial increase in salary.

These latter people issues are simply raised here to provide context to the whole operation, in a true 'systems' application; they will not be discussed any further within this thesis.

5.3.2 Broader Cost Savings.

The development of a centralised trials command & control system would allow a degree of staff integration and rationalisation to be realised across both of the Aberporth and Hebrides sites. Whilst the RAC team would remain relatively unchanged the QinetiQ team of operational delivery staff at both sites would require consolidation.

Though the aforementioned argument supports the need to locate the centralised system at Aberporth no inference should be taken that the operational staff at the Hebrides would be completely surplus to requirements. In any combined operation there are benefits to be gleaned from creating a new multi-skilled and multi-experienced team which would more effectively deal with any future customer requirements. The current operational delivery teams at both sites consist of typically a team of 20 individuals ranging from support staff all the way up to the Operations Controller. Due to the lack of restrictive caveats upon this thesis and the sensitivity of the topic the author provides a simplistic and generic business case for the additional cost savings, which could be delivered from a centralised system, in the following paragraph.

The typical salaries of the operational staff are circa £22,000 but the real costs to the company approach £40,000 due to the overheads incurred through the provision of employee support such as welfare support, training, pensions etc. Simple arithmetic quickly identifies the potential to save a further £800,000 per year by creating a centralised command and control system.

5.3.2.1 Typical Payback Timelines.

The overall financial opportunities and savings that may be realised, in a conservative application, appears to be in the order of £1M. This figure may be used to create a business

rationale for investment in a centralised and integrated trials command & control centre. Typical payback periods for similar technical investments within the company are five or ten years. Whilst the former does not offer significant opportunities for investment the latter suggests that ten million pounds may be available for the investment. Whilst such a large and complicated project demands a more elaborate cost benefit analysis before any commitment, the author has identified a Rough Order of Magnitude (ROM) which may serve as a catalyst for further investigation.

5.3.3 An Aligned Model Of Trials Conduct.

Most, if not arguably all business climates focus very much upon the financial elements of any changes to their operating environment; QinetiQ is no different nor worse than any of its peers. The creation of a centralised command & control facility will no doubt deliver real cost savings to both the company and MoD but, in the view of the author, there are probably much stronger and longer term benefits to be realised. The concept of operational synergy was raised in chapter two where the author described his involvement with the *Synergy* project.

Many of the issues raised and discussed during the *Synergy* project would be effectively and efficiently re-addressed if the centralised command & control project was realised. Having established a community which was capable of communicating, deliberating, challenging and changing within the *Synergy* project the author's single and most demanding irritation was that of members reverting to type as soon as they returned to their home site. Such actions were not predominantly the fault of the individual concerned but a function of the static and prevalent culture at the site.

"When I hear anyone talk of Culture, I reach for my revolver."

(Hermann Goering; 1893-1946)

The ultimate achievement of creating a centralised Air Range operation can only be achieved by creating a centralised command & control centre which is staffed and managed under a co-ordinated and fully synergised multi-skilled team. Achieving a technical

solution is a prime consideration but to combine it with an integrated team of personnel will give it additional depth, strength and resilience.

5.4 The Regulatory Requirements For Legal Operations.

All activities carried out upon the UK's T&E Range facilities are subject to regulatory compliance by one or more regulatory bodies; a non-exhaustive list of regulatory and statutory documentation for the T&E Air Range operations is included at Appendix C. The QinetiQ operated MoD Air Ranges are regulated through two primary bodies located at MoD Boscombe Down, Salisbury;

- The Trials Evaluation Services & Targets (TEST) Integrated Project Team (IPT) through the office of the Range's Safety Manager (RSM); and
- Test & Evaluation Support Division (TESD) through the office of TESD, Airfields & Ranges (A&R).

The RSM, as part of a management sub-set of the TEST IPT regulates all land based T&E activities executed on the Air Ranges. Compliance to the Handbook of Defence Land Ranges Safety, Joint Services Publication (JSP) 403 is mandatory. Authority to operate each individual Air Range site is at the discretion of the RSM and is achieved through the issue of a Range Certificate (MoD Form 904), on a tri-annual basis subject to a three day review of processes and inspection of facilities. Each site is visited and further inspected on an annual basis. However, these occasions are more cursory and advisory than regulatory.

TESD (A&R) forms part of a wider organisation within TESD which inspects and regulates all airfields and airports where MoD registered T&E aircraft are operated. This mandate covers rotary wing, fixed wing and UAVs. Their remit includes elements such as safety compliance, (including fire fighting equipment), airfield & aerodrome standards, aircraft engineering management and regulatory compliance. The predominant document set for such compliance is the Military Aviation Regulatory Group document set, (JSP 550).

TESD (A&R) has three distinct parts to his regulatory role. The first part is highlighted in the preceding paragraph and is basically a 'systems' compliancy regulator. The second part

of his role is that of co-regulating and licensing the Range's Air-traffic Controllers (RACs) and ensuring the safety assurance of technical systems such as surveillance radars and communication systems which support the task of controlling aircraft.

QinetiQ sub-contracts its Range ATC requirements to National Air Traffic Services (NATS). NATS is a commercial company who have their origins within the Civil Aviation Authority (CAA). The company's current major shareholder (49%) is the UK government. All NATS staff deployed upon the Ranges are inspected and regulated by both MoD and civil regulators. The former is carried out through TESD (A&R)'s office whilst the Safety Regulatory Group (SRG) part of the CAA carries out the latter. CAA recognises its own lack of expertise and experience in dealing with these matters and formally delegate any regulatory requirements to TESD (A&R).

The third part of the TESD (A&R) role requires the individual to act as the Ranges' airspace sponsor. The Air Ranges rely upon the use of segregated airspace to allow potentially dangerous activities such as UAV operations and/or weapon firings to take place in a carefully controlled and sanitised (to third parties) air environment.

The 21st century has experienced a global increase in air travel. The UK is seen very much as a major hub in air travel with many European countries as well as from further a field using its facilities as a staging post for trans-Atlantic and other international travel. This already large volume of usage is further worsened by the fact that many individuals in this current age rely upon domestic air travel to attend meetings and conferences on a daily or weekly basis. The result of so much air travel means that the availability of airspace is at a premium; every small piece of it must be bid for and managed effectively with as much due diligence as possible being applied to other potential user requirements.

Compounding this issue of airspace use and/or ownership is the fact that the current general culture of the UK's populous does not see the defence industry as sympathetically or as important as it did a few decades ago. MoD, like all other airspace users, must formally bid for, defend and manage its airspace requirements with a view that all flexibilities are afforded to other potential users. Large volumes of airspace required by MoD for the

conduct of T&E activities on Ranges such as Aberporth and the Hebrides are attracting increasingly larger interests and pressures from other airspace users, especially the civilian airline companies. It is within these forums that TESD (A&R) must defend the current air danger areas and bid for even larger volumes, if required, to accommodate the more energetic activities. TESD (A&R) directly represents the MoD's T&E interests, and therefore QinetiQ's business, on the Airspace Users Committee (AUC). Airspace within the UK is governed by the Director of Airspace Policy (DAP) who in turn has delegations directly from the Secretary of State for Transport.

To maintain primacy for the current danger areas utilised across the Ranges the operational managers for each site must report the utilisation of airspace annually to TESD (A&R)'s office. These figures are used to effectively demonstrate not only utilisation but the flexible and tactical method of airspace management exercised on the sites. The author has worked with both the regulator and DAP's office to create a model of best practice which is cited by DAP to other agencies when airspace 'ownership' is an issue.

The centralised Air Range project will continue to allow the airspace at the Hebrides to be managed tactically, efficiently and succinctly. Discussions with the Ranges' Senior Air Traffic Control Officer (SATCO) suggest that this project may offer further reduced timeframes in the tactical management of airspace at the Hebrides.

The author discussed the concept of a centralised and integrated Air Range capability with both regulators in 2006 and was given their full and collective support for the concept to be evolved. Final approval for such operational conduct must be given by both regulators.

5.5 The Engineering Solution.

The proposed engineering solution for the project in its most basic form simply enables the real time picture of the sea surface and of the air traffic environment at the Hebrides to be monitored by the relevant operational staff at Aberporth. The concept relies upon giving the operations facility at Aberporth full situational awareness of the remote environment.

5.5.1 Linking the Hebrides to Aberporth.

The engineering aspect of the project requires the application of an appropriate and robust conduit for conveying the required datasets between both sites. Due to the real-time functionality and interactive methodology utilised in the command and control of trial activities the data conduit requires a bidirectional capability; it should be noted that the level of data transmitted to the Hebrides is not as demanding in terms of bandwidth and propagation delays as that required for data transmitted from the Hebrides to Aberporth. The former predominantly requires voice transmissions and low data rates in support of simplistic commands such as those demanded for terminating erroneous missile and/or UAV flights. The latter requires a relatively higher conduit bandwidth to support the transmission of radar data (sea surveillance, air surveillance and tracking radar data streams) as well as a host of equipment mode and status information such as those to support Flight Termination Systems (FTS), telemetry, microwave link relay systems and UAV systems. By providing a multi-channelled and duplexed conduit within the solution a higher degree of reliability and robustness may be delivered thus minimising system outages and optimising any opportunities to conduct trial activities. Design concepts must take into account specific regulatory requirements, especially those mandated for communicating and controlling manned aircraft, such as access to 'hot standby' communication equipment.

5.5.2 Minimising costs - A 'fail-safe' approach.

The overall cost of the engineering solution may be minimised through the application of 'fail-safe' technical and operational systems; this technique is already applied to the majority of UAVs and missile systems operated on the Ranges whereby an FTS system is incorporated into the platform. Such systems rely upon the fitting of an independent Radio Frequency (RF) receiver within the platform which has the ability to curtail flight when a transmitted 'keep-alive' signal is lost; flight termination is typically achieved by either initiating a small explosive charge on-board or driving the control surfaces to a predetermined configuration which will destabilise flight. Other less destructive methods of recovery such as deploying a parachute recovery system may be considered on a case-by-case basis.

5.5.3 Connecting to the Link.

The TCS at Aberporth has already established a system for interfacing the Range's instrumentation (e.g. Tracking Radars, Electro Optical Tracking Instruments *etc*.) to the main TCS hub. This system of interfacing utilises a purpose built hardware/software interface that accepts the serial data stream from the instrumentation source and re-transmits the data in the required protocol onto a secure Local Area Network (LAN) connected to the main TCS hub. This interface unit has been termed as a Range Interface Unit (RIU) within the current TCS project and it is planned to utilise the same interfacing approach within this centralised Air Range project.

By connecting the Range instrumentation at the Hebrides into its own local hub, using similar RIUs and data protocols, it becomes apparent that, with the exception of distance and any propagation delays incurred, the Hebridean data hub is merely an extension of the Aberporth secure LAN and therefore easily accessible by the new Aberporth TCS hub. This concept would allow the LANs at each site to be connected up to a Wide Area Network (WAN) configured from either a bespoke information conduit or a capability supplied by an infrastructure provider. Whilst this approach may seem relatively basic, it can quickly be deduced that it is the link between the two sites, i.e. the conduit, which is critical to the concept. During the development of the final solution for data transfer the time delays incurred between both sites must be measured to allow a quantitative safety assessment to be carried out which would focus upon the inherent time delays. Such time delays, given the typical trial activities conducted at the Hebrides, must be quantified in terms of linear distance measurements to allow safety specialists to incorporate them within the appropriate trial safety boundaries.

Fisli, (2005) describes and compares various techniques for creating corporate WANs based on Virtual Private Network (VPN) technology. VPN technology is seen as the overarching term for the techniques and technologies that may be used to connect remote sites and users together. VPNs can be differentiated from actual private networks which are created by a system of owned or leased dedicated lines. VPN offers benefits over private networks by having reduced running costs over dedicated lines and allows for future

expansion/contraction without weakening security. Fisli identifies that a combination of VPN technologies when applied to create a bespoke system is often the best solution.

5.5.4 Air & Sea Surveillance Radar Data.

In addition to the transmission of instrumentation data to obtain real-time positional information of the trial assets at the Hebrides there is a need to transmit data from the marine and air surveillance radar systems. This data allows both situational and positional awareness of all participative and non-participative targets to be established; this is the primary method of identifying clear areas for the execution of potentially dangerous trials activities.

The marine radar systems are primary radar only; they are physically located at various sites on Benbecula and St Kilda and are wholly owned by QinetiQ. The air surveillance systems comprise of both Government Furnished Assets (GFA) and civilian National Air Traffic Systems (NATS) assets. The air surveillance radars provide both primary and secondary (transponder) air surveillance information to the RACs at the Ranges as well as any other third party air traffic units, both military and civilian, within the UK. The data outputs from such safety critical assets cannot be re-packeted without design authority (DA) approval. The transfer of air surveillance radar data across relatively long distances is not a new requirement; NATS and the military have extant systems and established data protocols for this application. The centralised Air Range project would look to use similar protocols to transmit surveillance radar data from the Hebrides. In a similar manner sea surveillance radar data is also transmitted from remote sites, in support of port and harbour operations, though the problems of data pack speed is much less due to the inherently lower speeds of the targets being tracked.

5.5.5 Voice Communication.

Of great importance to the interactive method of command and control are the voice communications links. Access to the operational Range intercom facility at the Hebrides requires the application of a full duplex link. To allow effective use of the RF Radio Telecommunication (RT) systems on the Hebrides the application may use either Duplex or

bi-directional Simplex systems. The final decision on what type of system is to be used may be taken after calculating the total bandwidth requirements from all data transmissions.

Due to the nature of the activities conducted on the Ranges, predominantly manned aircraft operations, the overall voice communication solution must consider the appropriate safety and regulatory issues contained within the relevant Joint Service Publications (JSPs).

5.5.6 Link Options.

Investigations into the most appropriate conduit of data between both sites has identified two options; microwave data links and national private circuit links. Both types of data transmission systems are currently operated across the sites in support of varying requirements.

5.5.6.1 Microwave Links.

The microwave link option allows QinetiQ staff to control the serviceability and therefore the operational availability of the system from 'in-house' with minimal reliance upon third party support. This option also allows QinetiQ to capitalise upon its current technical competence and experience in the use of microwave link data transfer. This option was removed as a possible solution due to the distances, topography and costs of multi-linking (multi-hopping) between both sites. An over-land path would have required about ten relay stations whilst an over-sea path would have required some six relay stations. This latter option may not have delivered the operational resilience required due to both clement (multi-path effects leading to signal cancellation) and inclement (obscuration and fade due to high precipitation) weather behaviour. Each relay station would have required a main and standby system with 'hot' (real-time) changeover configuration. A similar type of system (though with a greatly reduced bandwidth) procured for the communications facility at MoD Aberporth in 2007 cost around £90,000. It should also be noted that the system was procured as a standard COTS system with no capability for intra-link handshaking. For a multi-hop facility from the Hebrides to Aberporth a number of geographical sites would have to be identified and either bought or leased to support such an operation. Due to the varied complexities of such a proposal a ROM cost was not identified by the author though

it is imagined that it would be well in excess of any cost benefits that the project would hope to deliver.

5.5.6.2 National Private Circuit Links.

The national private circuit link is a concept already used by both sites. The idea has been in existence since the early days of the General Post Office (GPO) and was part of a safety critical UAV operation since the 1960s at MoD Aberporth and MoD Llanbedr (*Jindivik* UAV Operations). As technology has advanced then so the data circuits have migrated from copper to fibre-optic. National private circuit links support both local area and wide area networks, internet access, video transmission and telephony requirements. They may carry any form of digital transmissions at data rates ranging from 64 $kbits^{-1}$ to 622 $Mbits^{-1}$. For higher bandwidths the use of more specialised circuits allows transmission rates of up to 10 $Gbits^{-1}$ to be achieved (Cable & Wireless, 2006a). Consumer and technical information from a suitable service provider (such as *Cable & Wireless*) suggests that a mean annual circuit availability figure of 99.87% and 99.3% is available for the 622 $Mbits^{-1}$ and 10 $Gbits^{-1}$ circuits respectively (Cable & Wireless, 2006b).

The use of national private circuits also provide a degree of security; once allocated and initiated the user of such a circuit has sole use of it and no data may be transmitted through any other organisation's facilities. Additionally, by the use of constant intrusion monitoring any disturbances can be detected immediately. Such systems are currently utilised within the police and criminal justice organisations for secure, quick and cost effective data exchange.

5.6 The Security Aspects Of Remote Data Transfer.

Due to the sensitive nature of the data being captured during the conduct of Range activities all information must be appropriately managed and safeguarded from disclosure without lawful authority. Under the Official Secrets Act (OSA) of 1989 it is an offence to disclose official information in six specified categories if the disclosure is damaging to the national interest. Government contractors, such as QinetiQ, in addition to crown servants, must comply with the requirements of the OSA.

5.6.1 List ‘X’ Company Status.

Due to QinetiQ’s position as a prime partner with the UK MoD it has sites which are identified as list ‘X’. List ‘X’ status applies to commercial companies, on UK soil, which are approved to hold UK government protectively marked information at ‘Confidential’ classification and above; it applies to a site and not to a company.

5.6.2 The Official Secrets Act.

All trials related information generated and handled within the Ranges environment is subject to the terms of the OSA (1989) under which it is an offence to disclose to unauthorised persons any official information. A breach of security could cause harm to the interests of the nation and have consequences far more serious than can be envisaged by those immediately or partly responsible for a breach of security. This can be through the result of carelessness or even the lack of discretion as well as by a deliberate act. Staff are liable for disciplinary action and/or prosecution if there is a breach of the legislation. In additional to matters of national security, staff must safeguard records arising where there is a commercial information content.

MoD currently classifies its data in the following classifications. They relate to information and material whose unauthorised disclosure of which would, for:

- Restricted - be undesirable in the interests of the nation;
- Confidential - be prejudicial to the interests of the nation;
- Secret - cause serious injury to the interests of the nation;
- Top Secret - cause exceptionally grave damage to the nation.

5.6.3 Compliance with MoD’s Security Requirements.

The transmission of data from one MoD site to another must be in accordance with published MoD security guidelines. Consultation with the Aberporth site security manager together with peripheral discussions with other individuals involved with the transmission of MoD data has confirmed that the centralised Air Range project would need to satisfy JSP 440, the MoD’s Defence Manual of Security; and JSP 480, the Defence Co-ordinating

Installation Design Authority Manual of Regulations for Installation of Information Systems. These standards are a minimum and may be augmented and/or supported by other company and MoD policies and standards.

The overall strategy adopted by the author for this project is to minimise the transmission of any secure data and thus lower the security restrictions that must be applied to the data link. By inference, this suggests that the requirement for robust data encryption applications is minimised or even discarded.

5.6.4 Data Encryption.

Data encryption techniques employ the use of data receivers, predominantly digital registers which act as incoming data buffers; these are in turn accessed by a processor and the data are manipulated according to the encryption techniques utilised. Having been processed and manipulated by the central processor the data is forwarded to yet another stage of registers which act as outgoing data buffers, to await further interrogation and onward transmission to the final recipient. Note that this process is executed both at the data source (encryption) prior to path transmission and again at the data destination point (decryption). Data quality and integrity checking at both ends of the transmission path may be utilised; examples include bit parity checking and secure confirmation handshakes. A number of systems will strip out discrete packets of received data and retransmit them back to the origin to be used as a source code for subsequent data streams.

Such complicated methods of data handling invariably adds time to the data transmission process. Data which is not encrypted to a high degree of security classification may be transferred within timeframes which may be measured in tens of milliseconds. Highly encrypted data may suffer from a latency approaching two seconds. Though this timeframe may appear somewhat inconsequential, in the T&E environment it can cause problems, predominantly within the safety argument. For example, consider an air to air trial activity at the Hebrides. To meet a test parameter an aircraft is instructed to fire a missile whilst it is flying at a speed of Mach 1.5 at a prescribed altitude; for the engagement the UAV target is to accelerate and achieve Mach 2. For a frontal hemisphere (head-on) and co-altitude attack profile the closing speeds are at Mach 3.5. Using simple mathematical calculations and

applying a figure of $300ms^{-1}$ as the speed of sound one can deduce that the closing distance covered every second is just over one kilometre. Furthermore, from this example when utilising a transmission method which has a data transfer latency of two seconds the positional real-time track data (provided by Range tracking radars) shown at the destination control & command consoles may indicate that the assets are circa 2½ km out of position. In reality the assets may not be out of position but it is the latency of the data link which is creating the false real-time image. For engagements where operators must intervene in real time to destroy missiles as they approach a boundary the problem caused by latency is magnified especially when such weapons can achieve higher speeds and turn rates during the initial phases of flight.

From a safety perspective the latency of a link may be overcome by increasing the hazard area of the activity (safety trace energy boundary) by a factor which corresponds to the latency of the link. Given the physical size of the Hebridean Danger Area and the dimensions of typical weapon safety traces operated there, an additional 2½ or even 5km will not limit any activity in the horizontal plane. In the vertical plane, the Range Danger Area may be further extended by increasing its height; again commensurate with the link latency.

It should be noted that specialist data encryptors can also be very time consuming as far as management time is concerned. Prior to being operational such systems often require a setting-up period such as the synchronisation of security keys. The use of such encryptors on a daily and often tactically driven activity would be extremely onerous upon the operational teams at both the Hebrides and Aberporth sites. Thus the author's overall strategy of minimising the transmission of secure data will deliver operational benefits in addition to minimising data link latency.

5.6.5 TSPI Data Classification.

Communications with the MoD's security advisor during 2005 established that the raw Time, Space & Positional Information (TSPI) data derived from Range instrumentation tracking radars is graded *Unclassified*. This is the prime source of data utilised by the

operational teams for real-time command and control. The marine and air surveillance data streams are not classified and therefore do not constitute any security issues for the project.

All voice communications via RT on the Ranges is minimal and codified through the use of a brevity code; e.g. *playmate knock-on* may be interpreted as the UAV has been damaged. All non RT communications traffic in the majority utilises plain English with some use of key brevity codes; the content of code utilised is largely driven by the classification of the trial activity in progress. To conform to the MoD's security requirements and to allow this project to become tangible there is no reason why a more rigid brevity code could not be utilised for non-RT operational communications.

Predominantly the most sensitive part of any data parameter displayed and utilised in real-time within the T&E environment is that data pertaining to a weapon's energetic capabilities. This is primarily information which demonstrates the weapon's limits of capability such as its Maximum Energy Boundary (MEB), its maximum useful range to target or its manoeuvring abilities. This data may include aerodynamic and/or ordnance (explosive warhead) energetic performances. Such sensitive information when combined with the basic laws of propulsion and aerodynamics may allow hostile forces to determine the engagement profile and tactics to be used when engaging such weapons. Subsequently, the development of defensive manoeuvres to combat such systems may also be determined.

This type of information is generically termed a 'safety trace' (or part thereof) within the T&E environment. During a typical trial activity the operational team must have the real-time positional information of the trials platforms, in particular the launch platform and elected target, superimposed within the Range boundary for control and command purposes. Current in-service second and third generation weapons (e.g. *Sidewinder AiM 9L* and *ASRAAM* respectively) have safety traces which are classified as *Secret*. The author believes that by loading, storing and displaying the relevant safety trace parameters and Hebrides Range boundary data in the Aberporth TCS that the security level of the data link could be kept at a minimum. By adopting this approach the requirement to transmit highly sensitive data from one site to another is minimised.

Though the T&E Ranges handle data up to a classification of Secret, the majority of data is classified Restricted and/or Confidential. The author believes that the data required to be transmitted across the data link would remain as Unclassified and that the link itself only requires basic system integrity to accomplish business resilience, ensure business continuity and maintain reliability on a mission critical basis. The latter is extremely important given the cost and lead times of all deployed assets which must be in place prior to the commencement of any deep-range activity at the Hebrides. The fragility of the final ensemble of operational, specialised and mission critical assets serves only to reinforce the need for a reliable data link.

5.7 A Preliminary Safety Case for the Proposed Engineering Solution.

The intent of this part of the thesis is not to demonstrate the author's ability to construct a preliminary hazard assessment and safety argument for the proposed engineering solution but to communicate to the reader how such arguments are composed at an early stage. Of greatest note is the demonstration to comply with standards which are wholly driven by a quantitative approach and therefore demonstrating compliance with the ALARP argument as communicated by the H&SE.

The information recorded here includes the results of activities which have been carried out by the author as a facilitator and/or as a participant in safety workshops. The text is designed to introduce the reader to the early stages of a safety argument and to convey the rigidity of the quantitative approach currently demanded by the MoD within the author's current working environment. Some discussion is entered into at the closing stages of this work which relates to the qualitative aspects of arguing safety.

It should be duly noted that, within the context of this thesis, the safety argument for any UAV system will be completely independent of the remote command safety case. It is suffice to say that, given the regulatory requirements for UAV operations, combined with the Ranges' safety integrity requirements, that the safety argument for any UAV will be virtually identical at each site; any deviations from such a single model of safety would be a function of population density variations or local climatic extremities. The design of an UAV, and its operational safety case, would be virtually the same at each site.

5.7.1 Defining the Safety Criteria.

The safety argument for the integrated command link between Aberporth and the Hebrides must not grossly undermine the extant safety arguments formally recorded in each Range's extant operational Safety Case. Therefore, the accident severity categories, probability categories, equivalent numerical probabilities and accident risk classifications used for the proposed centralised Air Range operation must remain aligned with those specified for both Range Safety Cases (Rowley, 2008 & Warner, 2009).

The main safety related function of the centralised Air Range operation is the provision of displays which show the positions of trials participative assets, non-participative vessels and/or aircraft in conjunction with safety boundaries in real-time during a trial activity. These displays may be located at Aberporth and will facilitate complete situational awareness of the Hebrides' Range environment in real-time to allow RACs and Trials Conducting Officers (TCOs), located at Aberporth, to conduct activities in a safe manner.

As the extant Aberporth TCS has no direct input or exhibits no direct control over either the participative or non-participative assets displayed to the Range's operational teams the system is considered to have a secondary function in the context of determining a software Safety Integrity Level (SIL). Though the TCS handles and displays information of a safety-critical nature, it is the operators (human intervention), using multiple solutions, which make the final decisions such as terminating the flight of a weapon or UAV. This secondary function consideration aligns with the strategies and policies adhered to in the Range Safety Cases at both sites. Whilst the core component of the centralised Air Range operation is that of providing a suitable data link, it is important for the system engineers employed to be aware of the software SIL level of the TCS system which it will be linked into. Any additional software requirements demanded by the centralised project must demonstrated cognisance of the extant system's SIL level requirements.

The top-level safety requirement stated within the Range Safety Cases for Aberporth and the Hebrides demand the principle of ALARP to be followed. This requires all risks to be reduced to an acceptable level and that risk reduction (mitigation) is applied as far as

reasonably practicable. To enable the risks from the planned centralisation to be effectively identified, logged and sentenced an appropriate SMS should be applied.

5.7.2 Safety Management System.

The author suggests, that in accordance with the MoD's guidance, the SMS should clearly identify the following elements to enable efficient and consolidated control of the project to be exercised.

A clear project safety organisation should be created which identifies the responsibilities of all key individuals and the roles that they hold within the organisation; the safety organisation must also clearly and unambiguously identify the reporting lines of responsibility within the project team. The author recommends that the project safety organisation should be based upon the following roles;

- Centralised Air Range Project Manager - An individual who is responsible for ensuring the development and deployment of a safe system, including the identification and mitigation of safety issues. S/he must also ensure that all safety related activities are identified and carried out by the appropriate personnel as well as giving final approval for the project's safety related tasks.
- Centralised Air Range Project Safety Engineer - An individual who acts as the focal point for all safety related issues and has responsibility for planning and conducting safety engineering activities within the project. These activities may include maintaining and controlling all project safety related documentation and ensuring compliance to all safety standards. One of the key roles for this individual will be to advise the design authorities on any safety related issues and to provide technical assurance on all outputs.
- System Design Authority - The Authority has responsibility for ensuring that any potential hazards and risks have been identified and have been formally recorded within the system hazard log. It must also ensure that all essential and appropriate actions are taken to reduce each hazard log entry to an acceptable level. In the identification and management of risks the System Design Authority must ensure that all relevant documentation (e.g. instructions, procedures and drawings) is

appropriately annotated with the relevant safety related information. During any application of subsequent system changes the System Design Authority must ensure that such changes do not undermine any of the extant in-built system safety configurations.

- Independent Safety Advisor - The Independent Safety Assessor (ISA) must conduct technical reviews and audits throughout the life of the project. Any views, observations or findings must be reported to the project's safety committee as appropriate. The ISA may provide independent advice as necessary and produce a final report at the end of the project.
- Project Safety Committee - There is a need to establish a Project Safety Committee (PSC) which has the responsibility of reviewing and endorsing all outputs of the project's safety related processes. Any safety related issues identified must be raised formally within the PSC to allow any corrective action, as appropriate, to be identified and to be assigned to individuals for implementation. The PSC offers an opportunity for all hazards to be constantly peer reviewed as the project matures. The PSC will include projects members such as the Project Manager, ISA, System Design Authority, Project Safety Engineer and any other individuals who have a safety related role or may offer information which may affect the safety of the project. The author would consider that in the context of a Centralised Air Ranges Project that the Trials Safety Managers (TSM) from both the Aberporth and Hebrides sites should be members of the PSC. The TSMs are the principal authors of the Ranges' Safety Cases and will ensure that the project's safety goals are aligned with those of the Ranges.
- As the project matures then additional working groups and committees may be created to tackle bespoke tasks; their outputs may be fed into the prime and project core committees identified above.

The aforementioned is the author's view of how the project's safety management organisation should be configured based upon his experiences of working within many project teams over the past two decades. The fact that the options for a centralised approach to Air Range operations is currently with MoD was raised earlier within this thesis; despite the need for MoD to authorise project execution there was a need to conduct a feasibility

study and therefore to review the preliminary hazards and obtain a deeper understanding and help quantify some of the problems.

Whilst the project may not achieve realisation due to funding and pay-back timelines the author co-facilitated the first workshop on identifying the preliminary hazards and technical issues which need to be managed for the project to succeed. The following text explains how the initial qualitative approach quickly ran into the extant base requirements that the Ranges demand; i.e. a quantitative approach which would require an estimated three to five man years of activity to effectively determine an output which satisfies the Ranges' requirements.

5.7.3 A Preliminary Hazard Assessment.

The author co-facilitated the first workshop to discuss the possibility of controlling the Hebrides from Aberporth during 2008. The initial activity of scoping the problem was led using both informal causal route diagrams and HAZOP approaches. The former was used to support the capture of logical thoughts and to bind the ideas into more well-defined routes. The latter was used to provoke questions within the team and to explore as many areas as possible, including peripheral areas, which may be affected by the concept of remote operation.

Whilst the project in itself may be considered as a standalone technical entity, in true 'systems engineering' terms it must take account of the wider environment and its need to interface with the Ranges. The over-riding requirement was therefore to create a 'system' which, when realised, would become a sub-system component within a much larger, integrated and centralised Air Ranges trials execution system. To deliver a realistic, efficient and practical solution, in holistic terms, would require an intimate level of meshing.

5.8 The Extant Range Safety Cases.

The Ranges' safety cases consist of a body of evidence, written in free text and supported by fault tree analysis, which justify the safety claims made by QinetiQ in respect of their

management of the MoD Ranges and facilities. The safety cases are deemed to be a core requirement by the MoD in their application of due diligence and compliance to the HSE's legislation on safety management systems.

The safety cases provide evidence and logical arguments that all hazards have been identified, attended to and that any residual risks have been reduced to a level commensurate with the ALARP principle. Additionally the safety cases provide a degree of verification that the level of safe operation can be both met and perpetuated. The expression for delivering the evidence and arguments is almost exclusively carried out by the use of fault tree analysis with supporting explanations written in free text. The overall structure and approach for the creation of Range safety cases is based upon a framework contained within Defence Standard 00-56 (MoD, 2004).

The following information on the specific safety cases at Aberporth and the Hebrides is intended to convey to the reader how intensive the MoD's safety case requirements are and how they are almost wholly based upon a quantitative approach. It is quickly seen how such an approach may be suitable for a major capability such as a T&E Range facility or even a large military UAV but seem inappropriate for use in assessing the risks inherent within a relatively small and light UAV system which is the basis of this thesis. Of note, and what is quite obscure and perverse, is the fact that some of the foundational information from which to build the fault trees from is based upon an expert qualitative understanding of the hazards and risks such as the reliance upon individuals being competent and applying professional due diligence during hazardous activities. These latter thoughts will again be discussed in more detail in chapter seven.

5.8.1 The Extant Aberporth Range Safety Case.

Whilst the Aberporth Range safety case identifies the Range's safety management system in detail using free text (e.g. Command Structure, Responsibilities of Staff, Safety Committees, etc.) the defining and underpinning information is based upon quantitative figures derived from a fault tree analysis. The residual risks to various parties are identified within numerous categories; the author has selected two pertinent examples to convey the heavy application of quantitative analysis to the reader.

5.8.1.1 Annual Individual Risk Exposure to Activity Participants.

These individuals are considered as participants in the activity of delivering a hazardous activity and/or service in direct support of a trial activity. This group of individuals consists of staff who are directly involved in preparing aerial targets (e.g. fuelling, fitting & arming of pyrotechnics and Jet Assisted Take-Off (JATO) motors); preparing, fitting and arming weapon systems (e.g. Loading of stores on to helicopters, interfacing the Range instrumentation to ground launched stores); and the recovery of articles, including unspent ordnance, munitions & explosives from the land and sea danger areas. Having identified all of the hazards present within the operating environment of these trials participants the risks were calculated, by the application of quantitative techniques, and assembled to give an overall figure of risk by the use of fault tree analysis. The fault tree top level events for this class of participant is shown at Table 5.1.

Safety Case Fault Trees	Probability per Single Event	Number of Events Planned per Annum	Annual Risk per Individual (Based on team of 4)
FTR 04 (Storage, Transportation & Preparation)	$2.47 * 10^{-08}$	234	$5.52 * 10^{-06}$
FTR 05 (Gun Firing)	$8.11 * 10^{-13}$	100	$8.11 * 10^{-11}$
FTR 06 (Sighter Rocket Firing)	$2.07 * 10^{-09}$	100	$2.07 * 10^{-07}$
FTR 07 (*Sea-Skua* missile loading)	$1.53 * 10^{-08}$	20	$3.05 * 10^{-07}$
FTR 08 (Disposal of unspent OME)	$1.77 * 10^{-07}$	4	$7.08 * 10^{-07}$
Total Annual Risk to Activity Participants :			**$6.74 * 10^{-06}$**

Table 5.1 - Fault Tree Top Events for Activity Participants (Rowley, 2008).

Note: As the Range's explosives team consists of four individuals and that the expectation is that no one individual will participate in every hazardous activity it is deemed appropriate to consider that each explosive worker will be subject to 50% of the annual

hazard budget. With this in mind the total annual risk to a single participant falls to 3.37 $x10^{-06}$ per annum. Whilst this level of risk exposure is marginally greater then the HSE's Broadly Acceptable boundary it is considered ALARP and mitigated by the Range due to the rigorous training, inspecting and peer reviewing regime which is applied within the environment. As with all safety management tools, the Range's safety case is subject to annual review; these risk exposure levels to participants will be again checked and peer reviewed. The fault tree logic which supports the top level events shown at Table 5.1 is shown in Appendices D, E, F, G and H. These again serve to illustrate the considerable level of quantitative measures taken to support the safety case argument.

5.8.1.2 Annual Individual Risk Exposure to Military and Civilian Light Aircraft.

This group includes individuals and third parties aboard aircraft who may be in innocent passage outside the Range's Air Danger Area and/or stray into the Danger Area and become intruders. The Range's geographical position (Appendix A) places it within a complex network of national and international civil air routes and various military low flying areas. Due to the very highly structured network of air routes and procedures used by civil airlines the Range considers, from both expert opinion and experience, that the overwhelming majority of Danger Area airspace intrusions are caused by military fast jets and civil light aircraft. With these suppositions in mind, the Range considers that the hazard presented should be considered within the context of a military aircraft and/or a civil light aircraft carrying a maximum of ten persons aboard. The relevant fault tree top level events which support these deliberations is shown at Table 5.2.

The fault tree logic which supports the top level events shown at Table 5.2 is shown in Appendices I, J, K, L, M, N, O, P and Q. These again serve to illustrate the considerable level of quantitative measures taken to support the Range's safety case argument.

5.8.2 The Extant Hebrides Range Safety Case.

To further illustrate the very high reliance upon a quantitative approach for the creation of Range safety cases the author includes the following high level event from the Hebrides Range safety case. Rather than reviewing a similar event to the Aberporth Range safety

case the author has selected a different trials related event. This enables the reader to further understand the complexity and the effort required to create and maintain such an entity. In a similar manner to the Aberporth Range safety case, the Hebrides use a degree of free text to explain and qualify the capability though it is the fault tree analysis which underpins the whole safety argument.

Safety Case Fault Trees	**Probability per Single Event**	**Number of Incursions Considered per Annum**	**Annual Risk per Aircraft**
FT 01 (ASRAAM OM / *Sidewinder* AIM 9 strike)	$1.91 * 10^{-09}$	81	$1.54 * 10^{-07}$
FT 05 (ASRAAM TOM strike)	$5.74 * 10^{-09}$	20	$1.15 * 10^{-07}$
FT 08 (Non-participative aircraft collision)	$1.95 * 10^{-10}$	500	$9.75 * 10^{-08}$
FT 09 (LGB / JDAM strike)	$3.41 * 10^{-12}$	200	$6.82 * 10^{-10}$
FT 12 (Non-guided store strike)	$3.41 * 10^{-12}$	100	$3.41 * 10^{-10}$
FT15 (*Maverick / Sea Skua* strike)	$3.41 * 10^{-11}$	60	$2.05 * 10^{-09}$
FT 18 (Rangehead Gun Firing) (AS90 strike)	$3.48 * 10^{-13}$	100	$3.48 * 10^{-11}$
FT 21 (Sighter Rocket strike)	$3.48 * 10^{-13}$	100	$3.48 * 10^{-11}$
FT 26 (*Mirach* UAV strike)	$2.83 * 10^{-11}$	100	$2.83 * 10^{-09}$
Total Annual Risk to Military Aircraft & Civilian Light Aircraft :			**$3.73 * 10^{-07}$**

Table 5.2 - Fault Tree Top Events for Activity Non-Participants (Rowley, 2008).

5.8.2.1 Per Event Risk of a Store Breaching the Weapon Operating Area.

The Range considers that for any store to breach the Weapon Operating Area (WOA) it must either have an errant trajectory, the Range may have applied an inappropriate safety trace or the data displayed to the trials conducting personnel is incorrect. Procedural and operational mitigations are emplaced within the capability to minimise such occurrences though the risk is still present.

The fault tree logic which supports this top level event is shown in Appendix R; again it serves to illustrate the level of quantitative approach determined by Defence Standard 00-56 (MoD, 2004), which is prevalent within the T&E environment.

5.8.3 Concluding remarks on the Extant Range Safety Cases.

The various fault trees discussed in the preceding paragraphs and illustrated within the relevant appendices are meant to convey to the reader how focussed the current methodology within the T&E environment is upon a quantitative approach. Each one of the Range safety cases reviewed by the author has over 700 individual fault tree components and has taken over one man year, per Range, to create.

From experience the author believes that here is an opportunity to create a relatively robust safety case, especially for smaller systems, using a more qualitative approach. Whilst a heavily quantitative approach is fundamental for some high risk industries such as nuclear power and/or aerospace activities, there is an argument to be made, for lower risk industries, especially when dealing with smaller and simpler systems, for a less onerous and straightforward approach to safety management. Whilst a completely qualitative approach may seem too much of a step away from the established norm, the author suggests that a safety case could be created, for a suitably appropriate system, using a predominantly qualitative argument supported by a few key quantitative components such as fault tree analysis.

A typical and simple example to illustrate this revised concept would be the activity of allowing a young child to ride a motor-powered vehicle, such as a tricycle, for the first time. Seating the child astride the tricycle whilst it is static and explaining the controls

(brake, steering, accelerator) could be considered as a qualitative component of safety management; additionally, checking the integrity of the boots, helmet and chinstrap would also be considered as a similarly qualitative aspect of the safety management. The qualitative aspects will have been peer reviewed subjectively for suitability and appropriateness by 'subject matter experts' in the field of trike riding (e.g. sales staff) and child care (e.g. parents and other responsible adults).

Having gone through the whole qualitative aspects of the planned activity a quantitative based approach could be considered for any underpinning safety control mechanism, i.e. the long length of rope held by the supervisor and connected to the vehicle's 'kill switch'. The quantitative approach for this element of the activity would consider the length of string and its ability to withstand the tension incurred to bring the vehicle to a safe stop. This latter 'safety critical' aspect could be investigated and recorded using a quantitative tool such as a fault tree analysis and/or even a simple spreadsheet mapping the length of rope and speed of tricycle against the mass and height of the child. This approach is already carried out in some environments, for example when there is a need to alter suspension settings for a bespoke activity (e.g. touring, racing, etc.).

This example brings into focus the fact that certain individuals, such as parents or sales staff, are important to some of the safety related decisions in our daily lives. Their inputs are clearly subjective and qualitative; whilst they may use an instruction manual to obtain a few basic quantitative bits of information, their inputs are almost wholly qualitative. Whilst the example above relates to the risks involved in allowing a child to ride a tricycle there are numerous other everyday activities where qualitative approaches are used to manage the safety of subjects which are more emotive, closer to our personal beliefs and probably more intimate and important to us in our own lives. General Practitioners (GPs) apply very much a qualitative approach to diagnosis; initial engagements with patients rely very much upon a qualitative approach by asking questions on where something hurts or how long they have had the symptoms. For most patients this first stage of qualitative assessment is sufficient, however, further investigations may require a degree of quantitative assessment through the application of more specialised techniques such as blood pressure measurements and blood analysis. Dispensing chemists engage in a subjective dialogue and

use a qualitative approach in issuing some drugs to customers. From the author's experience of vehicles, the approach taken in garages which conduct 'Ministry of Transport' (MoT) roadworthiness tests may be relatively objective and quantitative in some aspects (e.g. tyre tread depth, brake efficiency, etc.) though the detection of rusting framework and its correction (e.g. the welding of strengthening plates) is very qualitative and subjective, and relies greatly upon the personal integrity and experience of those individuals engaged within the process. With these observations in mind the author further investigates the concept of a qualitative approach to safety cases and safety management within chapter seven where the concept of a qualitative approach to safety, especially for light UAV systems, is further developed.

The term personal integrity and its importance to a safe system of diagnosis, control and execution was raised in the preceding paragraphs. Whilst it may not appear at first glance to be important the author suggests that it is fundamental to a safe system of operating. When the author uses the term personal integrity he is trying to encapsulate the requirement of an individual to act professionally within the confines of their discipline with a relatively high degree of moral principle. Effectively the individual is exhibiting a high degree of consistency and displays a distinct lack of corruption. Clearly, if a more qualitative approach to safety management is to be credibly considered then an in-depth review needs to be conducted of those aspects which constitute how an individual, or a group, may operate from a moral behaviour perspective. Whilst this thesis has discussed engineering and safety from a predominantly quantitative and somewhat events-based viewpoint so far, it now needs to look in more depth at the human components of the system under scrutiny.

5.9 The Human Component of a System.

The development of a safe system relies very much upon the integration of a multitude of different engineering skills. As briefly introduced in chapter one, modern systems are becoming more complex through not only advancements in technology but in their increasing interfacing and coupling with humans; this is especially important when considering semi-automated and fully-automated applications.

The majority of engineering integration is carried out by engineers who are well practised in the more 'traditional' engineering disciplines such as software engineering, electronic engineering and mechanical engineering, to name but a few. Of note though is that these traditional engineers are not well practised in the understanding, and application, of human factors engineering within systems (Sandom, 2002). Perrow (1984) characterised complex and interactive systems as those which support dynamic processes which involve hardware, software and human elements that interact in many different ways; examples include Air Traffic Control towers and nuclear power generation plants. Some complex and interactive systems are safety-critical and rely heavily upon human intervention in real-time as well as equipment and procedures to maintain a safe operational environment. Such systems rely heavily upon the human interfacing aspects; this includes taking cognisance of the human aspects, including the social and organisational structures, when making claims about the system's safety integrity levels.

Despite the aforementioned, safety cases are predominantly focussed, as highlighted within chapter four, upon the technical and engineering components of the system. Such approaches typically address the hazards arising through technical failures alone despite the fact that human error is repeatedly cited as a major contributing factor and/or the direct cause of many incidents. The human component of the majority of safety-critical systems is rarely considered in the same depth as the technical components of the system; this is obvious from the distinct lack of human focussed hazard analysis and risk assessment tools which are applied in the process of creating most safety arguments. The predominant 'tool' for assessing the human component within the author's environment is based wholly upon an individual's training record, certificate of competency and log book of currency. This approach is merely a review of attendance at training courses and a subjective, and somewhat cursory, view of the demonstrable paper chain to fulfil a management system requirement. True due diligence is simply not applied.

5.10 Minimising Human Errors.

One of the foundational methods used by organisations to minimise the opportunity for human error to occur is to promote a 'safety culture'. Many organisations monitor the safety culture within the organisation by use of tools such as questionnaires which are

completed by the staff. The responses offered by the staff are assumed to be a measure of the 'safety culture' within the organisation due to the fact that the questions are based upon certain key definitions of what constitutes a safety culture. In simple terms, the organisation trusts the staff to answer the questions in a truthful manner to reveal the 'community's' safety perspectives and measure how 'good' or how 'bad' it is. Whilst this may sound simplistic and easily achievable at first glance, a further in-depth review reveals a whole host of complicated aspects and issues which should be carefully considered and reviewed before drawing any conclusions.

The following chapter introduces, discusses and reviews safety culture in the context of applying it as a tool to monitor the extant safety values and underlying operation of an organisation as well as using it as a leading indicator to provide an insight into potential sources of safety concern in the near future.

Note: The proposal to control and command the Hebrides remotely, which has been discussed in this chapter, is the author's own concept for realistically delivering an aligned operation whilst realising a degree of cost saving. The prime driver is the delivery of a Range service which is seen to be consistent from the customer's perspective for T&E operations at both sites. QinetiQ, during the period of this doctoral study, has taken the integrated operation concept much further and tasked a relatively large team to devise a plan for delivering such a project. This plan was effectively delivered to the MoD for ratification during early 2009. Whilst the details of the plan remain Commercial-in-Confidence it proposed that around £45M was invested to facilitate the *remoting* of the whole T&E operation at the Hebrides, allowing control to be exercised from Aberporth. The plan included, but was not limited to, the full remoting of all functions at Benbecula, its peripheral radar sites, and the outlying and instrumented island of St Kilda. The plan identified that 125 jobs would be lost from the Hebridean site and that the permanent presence of staff on St Kilda would be removed.

On the 15th of September 2009 the Scottish Secretary announced that the plan put forward by QinetiQ to remotely control the operation at the Hebrides, was to be

completely abandoned. The decision taken by the government was based primarily upon the ultimate cost to the islands, the islands' families and their economies.

Whilst the author's plan, as discussed within this chapter, highlighted a degree of cost saving, it primarily focussed upon the realistic delivery of an aligned T&E operation to the benefit of the customer/Range user. The impact of implementing such a modest plan could have been met through staff natural wastage and would have allowed a stronger and richer operational team to have been created. By attempting to deliver the 'Big-Bang' solution, the company created, and magnified, many issues which included technical, economical and political elements.

Whilst the decision to take the plan forward was based upon the fact that a sound safety argument could be delivered for the remoting operation and that it was economically sensible for QinetiQ to do so, the fact remains, that the decision would have eroded the economy within the wider environment. The Scottish islands have been suffering greatly from economic decline for many years and this proposal would have probably dealt a lethal blow to the remaining threads of island life. Whilst the economic view from within QinetiQ made business sense the wider ramifications did not. The author suggests that the decision taken by the government aligns with the view expressed in this thesis that many important decisions must rely upon qualitative data as well as the hard evidence offered by quantitative data alone. In this instance the quantitative facts (cost reductions) aligned with the requirements of the business drivers yet the decision to abandon the concept was wholly based upon the qualitative, subjective and emotive elements of island life, culture, heritage and politics.

A more detailed account of the decision is available on the internet; the following BBC News website may be found to be useful and accurate at http://newsvote.bbc.co.uk /mpapps/print/news.bbc.co.uk/1/hi/scotland/highlands_and_islands; accessed 25th September 2009.

This page left intentionally blank.

CHAPTER 6

Safety Culture - A Literature Review

Formatted: Bullets and Numbering

6.1 Introduction.

It is suggested that we cannot hope to understand the attitudes of either management or workers until we have seen them from an historical context (Brown, 1980, p276) and that much of what we currently define as part of 'human nature' is, in fact, the output of its particular culture at a specific point in time. The opinion that work is an unsavoury necessity, that the worker is self-interested, lazy and competitive and that society consists of a plethora of unruly individuals and that the fear of starvation is the prime negative incentive whilst money is the main positive one is an image of society taken at a certain point within its development. These beliefs align with no known fundamental human characteristics; they simply reflect, when applicable, a very small minority of members within the industrial environment. It is regrettable that these assumptions were assimilated, over time, to form the basis, not only of management practice but also the majority of the early work within the field of industrial psychology. From Taylor (1919) and Gilbreth (1911), the catalysts of industrial efficiency, as well as Műnsterberg (1913) and Myers (1909, 1921), the early industrial psychologists, the overall approach was a completely "*atomistic and mechanistic one*" (Brown, 1980, p276). Such an approach took no view of psychological drivers or even any social elements. Balchin (1947) suggested that though the struggle for survival in the early days of industrialism was extremely hard, the worker did in fact experience a manner of "*grim satisfaction with his lot*". Within such a struggle to obtain, by some considerable effort, a meagre living from society the individual gained some basic reward through the taking on of something immensely powerful, not giving in to it and in fact winning small battles against it daily. The underpinning strength for this type of behaviour is not fair play, justice or equality but pride and satisfaction that come more or less instinctively from the process of survival; and this in an age when it was not easy. Another important and fundamental facet of life during this age was that of religious belief; seen as a relatively short preparatory phase for an eternal life of true happiness, the meagre existence served only as a casual expenditure of time until death. Happiness was not about to arrive tomorrow or next week but was to come upon leaving the current life.

Through the process of time and by the application of management learning more modern working conditions were introduced; through such changes the irrational satisfaction of existing within such a hostile environment was removed (Brown, 1980, p277; Maslow, 1943). Slowly, working life became more palatable, but with it came the slow erosion of the survivability ethos and the gradual crumbling of the worker's religious convictions. Happiness, reward and pleasure were items that the worker now desired in this life, rather than in the next; the incentive to work is not pure survival in this new regime but that of a new kitchen, another holiday or even a financial bonus. Suddenly (relatively) the whip wielding ogre of a boss becomes a modern businessman, hours of attendance are forty hours per week and workers are paid for absences of sickness and even holidays.

Subsequently, psychologists, human factors engineers and other learned individuals set about measuring and distilling every component which could have limited the worker's ability to achieve continuous high output. Everything, including temperature, lighting, humidity and even noise was monitored and dissected to optimise throughput; everything that is, except people. The result was a body of misaligned papers which could not have possibly led to a model of good working conditions. Balchin (1947), observed a factory where five hundred women, most of them under the age of thirty, operated under "*perfect working conditions*" but within "*appalling living conditions*" (Brown, 1980, p276). Outside this sterile and monotonous work environment the women lived a life "*for colour and excitement and drama and change – for emotion*". All that interested them or that they really cared for was left outside the working environment.

Hopefully, it has been demonstrated that the physical conditions of the working environment has a direct influence on the worker, but to focus solely upon these elements can lead to a systematic failure in understanding of how an individual may give an optimal output. More importantly for highly commercial and certainly for safety related organisations is the fact that the psychological, (relating to, or arising in the mind) (Oxford, 1995), predominantly that of the cultural (of or relating to the cultivation of the mind or manners) (Oxford 1995), facet of working life must be understood to allow a more complete and systematic entity to be created and managed.

Psychology, in a similar manner to other sciences, has a prime objective to try to foretell the future behaviour in any system under observation (Brown, 1980, p287). The fact that it currently cannot predict accurately should be unrelated to any argument for its abstention from an application; moreover, any extant information, such as trends and biases should be taken as a positive and constructive advancement. Cognisance should be taken of such behaviours shown in our daily lives; examples include the economics of a country (bank interest rate control of economic growth) and even market spending fluctuations which are dependent upon the weather (overcoat and umbrella sales). Each day we conduct business which is predominantly based upon our assumptions of what others will do or require in a more or less predictable way (Brown, 1980, p285).

Over a relatively short period of time, safety research has tended to focus upon counting and analysing adverse incidents in order to try and stop them from recurring. However, in recent times a growing perception has developed which recognises that there are broader dimensions involved with safety incidents. Initially the legal emphasis on safety was focussed upon engineering; for example, the fitting of guards to dangerous machinery (e.g. agricultural machines, pulleys, drive belts etc.) and the use of load indicators on lifting equipment. Whilst this approach resulted in a significant drop in the overall accident rate there were still opportunities for further improvements. Having invested quite considerable resources into the application of engineering solutions to the safety issues it was identified that if there was no effective management control of risk then accidents would continue to occur as a result of omissions in, for example, improvements, usage, maintenance etc. Organisations which had effectively applied safety engineering concepts and created a robust safety management system conceded that there had been a drastic downturn in accidents but found that there were still some residual occurrences. Such events were identified as being related to behaviours. The majority of accidents can be linked to a failure of a person, or group of persons, somewhere within the chain of events. The first two methods of minimising accidents involved approaches which applied restrictions or requirements upon individuals; i.e. they are done *to* people rather than *embracing* them as part of the process. The third approach which is now being adopted builds upon the engineering and management approaches; it includes and involves all individuals within an organisation. By working as one entity, both managers and workers are required to

collectively identify and eliminate unsafe behaviour with a goal of creating a positive safety culture through the changing of attitudes.

Hollnagel (2004, p45) also suggests that trends in attributed accident causes have changed over time; though they commenced by focusing upon equipment in the 1960's, re-focussed upon human error in the 1990's, they are now turning their attention to organisational causation. Figure 6.1 provides an useful illustration of the evolutionary change in accident causation.

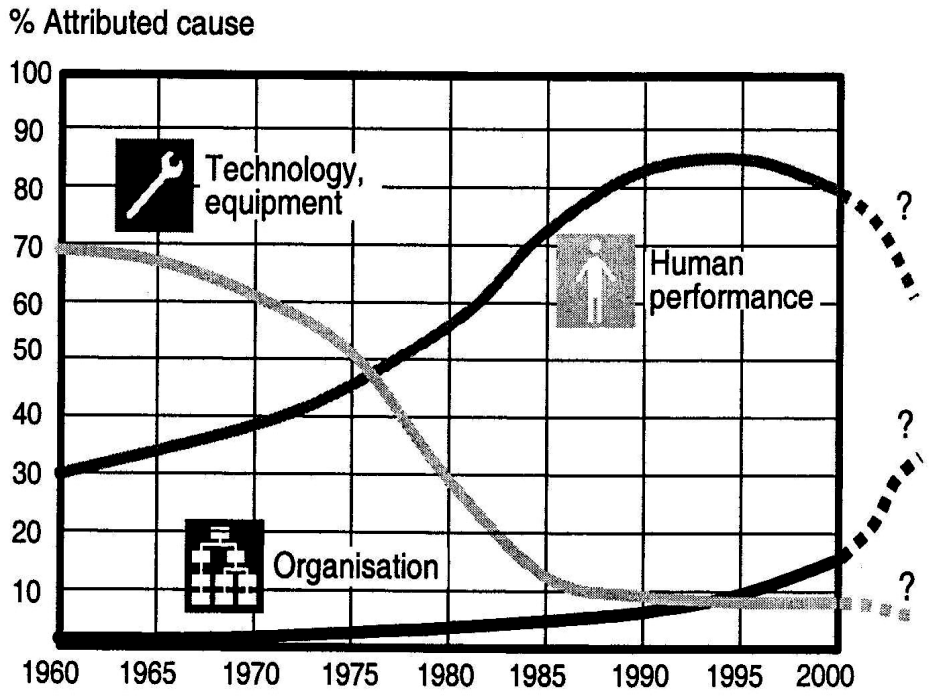


Figure 6.1 - Trends in attributed accident causes (Hollnagel, 2004).

Over the past decade it has been widely accepted that examining the organisational culture of an organisation is imperative if achieving sustainable improvement in the safety domain is to be realistically delivered. Most large organisations now accept that there is a need to understand the common attitudes, beliefs, values and assumptions that influence people's perceptions and actions when dealing with safety related issues linked to their organisations

(Kirk, 2005). These shared components of our safety related lives are more commonly referred to as a 'safety culture'. Current research into safety culture owes a great deal to studies on organisational culture and the common components of shared beliefs, norms and values of people who work within an organisation. It is thought that the actions and communication patterns within an organisation may be influenced by the organisational culture (Kirk, 2005); however, it should be noted that organisational culture is not considered to be a single entity but a collective of various sub-cultures operated and commanded by various professional groups, departments and teams.

An organisation's safety culture was not deliberately created but in fact developed naturally in response to the specific needs of institutions where there was a potential risk to the workers or the general public. It can therefore be deduced that the safety culture of an organisation is but a single component part of the greater organisational culture which focuses upon improving, augmenting and reinforcing the use of safe policies and practices. It should be stated that one of the most important but difficult to measure aspects of both organisational and safety culture is that of the qualitative and the intangible. Personal attributes such as attitudes, beliefs, responsibility, confidence (non-exhaustive) as well as the more abstract ones such as an individual's perception of risk or their acceptance of an open reporting regime (non-exhaustive) are extremely difficult to bound and measure.

Formatted: Bullets and Numbering

6.2 Background.

The idea that an organisation could be influenced and controlled by underlying events and processes was first tabled during the 1970's (Guldenmund, 2000) but it was only later in the 1980's that the concept started to be referred to as organisational culture. Guldenmund (2000) further identified that the term culture was occasionally replaced by the term climate as the concept began growing in application. His work also identified that the original concept and the use of the term climate related more specifically to its global definition; whereas, the modern definition for it now is organisational culture. Furthermore, the term organisational climate is now seen as a demonstration (or manifestation) of organisational culture.

The fact that theorists in management practices are appearing to replace the term 'organisational climate' with the term 'organisational culture' was identified by Hale (2000). It seems that the term 'culture' is now firmly identified and utilised as the modern substitute for 'climate' in organisational safety behaviour work (Cooper & Phillips, 2004; Cooper, 1998, p1).

Formatted: Bullets and Numbering

6.3 Separating Culture And Climate.

Within the safety behavioural environment the definitions of culture are very similar to that of climate; though the term safety culture is generally seen as a more rounded and comprehensive term than that of climate. The term culture is generally seen to be intertwined within the life of an organisation and/or bound within its institution, whilst the term climate suggests a state which is influenced by an external force such as social trends (Oxford, 1995, and Glendon & McKenna, 1995). Cooper (2000) does in fact put forward a theory for the interrelated aspects of safety culture as an embodiment of three elements;

- Psychological aspects (often referred to as 'safety climate),
- Behavioural aspects (or 'organisational') aspects,
- Situational (or 'corporate') aspects.

Glendon & McKenna (1995) described safety culture as "the embodiment of a set of principles which loosely define what an organisation is like in terms of health & safety" or "the way that we do things around here" (CBI, 1990). Though individuals within different parts of an organisation will be dictated to by the same procedures and instructions, their view of the environment will differ by a smaller or greater degree depending upon their relative positions. It is these underlying beliefs and persuasions that the worker has which is seen to be more aptly reflected within the term culture (Guldenmund, 2000 and Payne, 1996). Such variances in safety views within an organisation are predominantly caused by the various levels of local practices and customs which have evolved over time and have been allowed to flourish under local management; the creation of local citadels. This level of variance is further exacerbated by the variations in risk levels across and within the organisation. By consolidating these issues an increasing influence is uncovered which greatly affects compliance with an organisation's inherent safety management system. In a

nutshell, the safety climate is viewed as a barometer for gauging an organisations safety culture from the viewpoint of the employee at a point in time (Cox & Flin, 1998).

The author within his own experiences of T&E management has been guilty of misusing and incorrectly interchanging the terms safety climate and safety culture; in reality, these terms and their definitions are not clearly distinguished.

Formatted: Bullets and Numbering

6.4 An Overview Of Safety Culture.

Over the past few years the outputs of various boards of enquiries into major disasters has highlighted the fundamental importance of a proactive strategy to safety management within organisations. Such outputs have driven many companies to give safety management a higher order of importance within the organisation; it has also engendered a realisation that the organisation's safety culture probably needs to be improved (Cooper, 1998, p225). At first sight the aforementioned seems to be a straightforward issue, but, scientific modelling of human behaviour suggests that prior cognisance should be taken of the interactive relationships between people's behaviours, attitudes, perceptions and their environment if any attempts are to be made to improve an organisation's safety culture. By ignoring or overlooking such important relationships many initiatives to change culture, such as Total Quality Management (TQM), have failed (Cooper, 1998, p1, 14,). The author's work on '*Synergy*' during 2006/7 relied heavily on an understanding of each of the four Air Range's local management systems; the effective delivery of an aligned system of operating could only have been achieved through co-operation and a broad understanding of local cultures, attitudes and perceptions.

An efficient safety management system, as it matures and develops, will enhance organisational control, communication and co-operation within the organisation though cognisance must be taken of the requirement to invest and develop the underpinning competencies which are essential for success. Such an approach requires the management team to effectively understand what the staff's perceptions and attitudes are towards safety thereby enabling a more focussed approach to any change requirements. Such changes should not be considered as superficial but should be seen as a wholesome commodity fully woven into the fabric of the organisation. In a similar way, the management team should

consider their motivational strategies (Cooper, 1998, p24, 44, 89, 214) so that the staff readily and consistently, behave in a safe manner. For such changes to be effectively delivered within an organisation the senior management team must show strong leadership and commitment throughout the implementation and maturation phases; to be fully effective the whole organisation must appear to be fully aligned and permeated by a genuine wanting to be safe. From a purely business perspective the rewards to the organisation in terms of competitive advantage, quality, reliability and profitability can be massive (Cooper, 1998, p2, 214).

Formatted: Bullets and Numbering

6.5 A Definition For Safety Culture.

The use of the term safety culture began in the atomic energy industry following the International Atomic Energy Agency's (IAEA) initial investigation into the nuclear reactor accident at Chernobyl, USSR (Lee, 1998). Further investigations into the incidents at Clapham Junction, Kings Cross and Piper Alpha suggested, quite strongly, that the safety systems had in fact broken down. This occurred not because of the processes and procedures that were in place but because of the safety climate and safety culture within the organisations. Though a number of definitions have been used since these incidents it is the Advisory Committee on the Safety of Nuclear Installations' (ACSNI) definition which is the most widely accepted and used (HSE 1993);

"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."

Though other definitions are available which try to further break down or distil that which has been articulated in the preceding text, the general agreement is that safety culture is ultimately a proactive perspective towards safety.

6.6 Linkages To The Causes Of Accidents.

Formatted: Bullets and Numbering

Established praxis on endeavours to improve safety within the workplace have predominantly concentrated on the technical problems encountered and/or any identifiable human failings. It was not until the occurrence of relatively recent major incidents such as Chernobyl, the train crash at Clapham Junction, the fires at Kings Cross and Piper Alpha, that the role of organisational policies and procedures were seen as contributors to such occurrences. Desmond Fennell QC, during the Kings Cross Inquiry, stated that "…a cultural change in management is required throughout the organisation" (Fennell, 1988).

Following on from Fennell's observations, Lord Cullen held similar views during his investigation into the Piper Alpha incident. During the investigation Lord Cullen reported that, "it is essential to create a corporate atmosphere or culture in which safety is understood to be and is accepted as, the number one priority" (Cullen, 1990). In more recent times Lord Cullen has focussed greatly on the role of safety management systems and the safety culture within the rail industry as a whole. The judge's inquiry into the Ladbroke Grove incident in 1999 has pointed to evidence which suggests that a large proportion of accidents, incidents and near miss occurrences may be caused (both directly and indirectly) from unsafe acts that are a result of fundamental or latent deficiencies in the system's safety management regime (Cullen, 2001). During the inquiry Lord Cullen highlighted the relationship between "good safety and good business" and went on to establish the importance of leadership to a positive and successful safety culture. One of the key revealing pieces of information put forward to the inquiry was the lack of clear safety leadership within the industry; caused primarily by the government's privatisation strategy which resulted in a largely fragmented environment. Cullen emphasised the importance of senior management's commitment to safe operations and that this should be seen at all times by the "front-line" workers. The inquiry also pressed home the need for effective safety communications within the industry and that safety targets and goals should be given as much importance as the financial aspects of both strategic and daily operations.

6.7 A Growth Of Knowledge.

Formatted: Bullets and Numbering

As with most occurrences in life, with each new event, a finite amount of new understanding is uncovered; constantly with each incident that occurs our knowledge of

causal factors which make systems vulnerable to failures grows correspondingly. It has transpired through time and experience that these vulnerabilities are not simply driven by pure human error, probabilistic chance and/or engineering failures alone but are rooted in the protocols and policies of the offending organisation. Such weaknesses have been identified and highlighted many times during these relatively recent incidents where they have been shown to be present for a substantial period of time prior to the final incident. Such a vulgar statement in itself highlights how weak and inappropriate the policies were if they did not stop the incident in the first instance. As a clear example, the Clapham Junction train crash occurred as a result of both individual and corporate safety failures; predominantly caused by inappropriate attitudes towards safety and incongruous policies relating to safety management. It is from such observations and new understanding that current Health and Safety practitioners focus upon organisational concepts and values that may augment an organisation's safety management and performance during periods of hazardous and/or complicated operations.

6.8 The Scope of Safety Culture.

Whilst research evidence suggests that a positive safety culture will improve an organisation's safety performance, there is not much guidance on how organisations might achieve such improvements through cultural changes (Clarke, 1999). Weick (1987) suggested that highly reliable performance can be achieved through the development of an organisational culture which encourages 'interpretation, improvisation and unique action'. For such a culture to exist, there has to be trust, openness and mutual understanding, on the part of the workers, their managers and the wider community of operation. Such qualities of culture are cited in the HSE's description of a positive safety culture, which should be characterised by 'communications founded on mutual trust, by shared perceptions of the importance of safety, and by confidence in the efficacy of preventive measures' (HSE, 1999). The ultimate viability of a complete safety culture must therefore depend on a number of disparate, yet critical elements, including staff-management communications, inter-company communications and, especially within the defence industry, the regulatory and inspecting bodies. Within the context of this thesis the author suggests that for a full and positive safety culture to be present across the Air Ranges, the MoD, QinetiQ and all of

the regulatory bodies (e.g. DOSG, TESD, etc.) must be fully aligned and bought-in to the safety culture regime.

Through personal experience, and from observation (Haddon-Cave, 2009), the author can appreciate how the demands of an operation can tangibly and directly affect its safety related focus. At the lower and daily working levels there may be a decent and positive safety culture both within an organisation and across the wider field of partner organisations involved in the operation. At this level the individual may be sparingly cognisant of project cost pressures, or pressing timescales, but the overall personal attitude of individuals is still predominantly focussed on accomplishing the daily task in a safe and competent manner (e.g. welding, fabricating, testing, etc.). As an individual's position within an organisation rises then so the balance between the daily task and the more strategic organisational issues shifts. Project costs and/or timescales become much more important to middle and senior managers, especially when organisations are driven by commercial elements; as the level rises within the organisation then so the target of making money increases and the focus upon delivering a daily task becomes diluted. It is this dilution of safety in ascent within organisations, especially at the most senior levels, that should be noted; it may also be exacerbated when many large organisations are operating together or within a single environment.

The author reiterates that creating a positive culture within one organisation may not ultimately deliver a completely safe operation; the author cites the recent Haddon-Cave inquiry into the loss of an RAF Nimrod aircraft in theatre as a tangible example (Haddon-Cave, 2009). In the case of the Nimrod incident the inquiry found that both defence contractors (QinetiQ and BAE Systems) had failed, in varying degrees, to apply appropriate due diligence to the safety systems. Additionally, but probably more importantly, the MoD, as the owner of the operating domain, was found to be wanting in its management of the whole environment, especially that of safety and technical management.

A positive safety culture can make a substantial contribution to the principle of 'defence-in-depth' (Barraclough & Carnino, 1998). It can promote the vigilance needed to recognise actual or potential safety problems and to communicate the need to address them. In

addition to the safety culture within an organisation, the use of peer reviews, especially externally driven ones from the regulatory regime, can help immensely. Whilst regulatory inspection and enforcement are essential tools for monitoring safety, the attitude of the regulators towards inspection and/or enforcement, can help or hinder the safety culture (Barraclough & Carnino, 1998).

Formatted: Bullets and Numbering

6.9 Attributes Of A Good Safety Culture.

It is argued (Pidgeon & O'Leary, 2000) that a good safety culture may be reflected and further promoted by four factors;

- Commitment to safety by senior management,
- Realistic and flexible policies and practices for handling both well-defined and weakly-defined hazards,
- Feedback, monitoring and analysis of information offers opportunities for continuous organisational learning,
- The whole workforce needs to share and own the concerns for all hazards within the organisation.

By surveying the attitudes of workers towards safety and their perceptions of hazards within the work environment senior management may be given a measure of the organisation's safety climate and essentially its underlying safety culture. A great deal of research has been carried out on the link between safety climate as an indicator for an organisation's safety culture (Guldenmund, 2000 and Flin *et al*, 2000). Cheyne *et al*, (1998) suggest that employee attitudes are one of the key elements in determining a safety climate; this is due predominantly to its multi-faceted dependence upon many constituents from the working environment. They submit a view that attitude towards safety is a fundamental component of any safety culture. Further work by Williamson *et al* (1997) suggests that any safety procedures or actions that are put in place may be inadequate if the attitudes of the employees and their perceptions of hazards are not taken into account.

In more recent times the independent review into the Nimrod XV230 loss in Afghanistan (Haddon-Cave, 2009, p261) has reiterated how important it is to have an adequate and/or

effective safety culture present within an organisation. In his report Mr Haddon-Cave QC states that responsibility for a culture which is committed to a safe and ethical operation lies with the leadership of the organisation (Haddon-Cave, 2009, p261).

Formatted: Bullets and Numbering

6.10 Focussing On The Safety Climate.

Cooper (2000) suggests that safety culture itself can be distilled into three prime components; psychological, situational and behavioural. Measurement and analysis of these components can be carried out by utilising many qualitative and quantitative methods. The situational aspect of a safety culture is often observed in the structure of organisations such as their protocols, policies, work schemes, management systems etc. The psychological element is often analysed through the use of safety climate surveys created to interrogate an individual's perception of safety by focussing questions upon their values, norms, dispositions and attitudes. Behavioural components are often measured by (external) workforce observation or self-feedback (internal) through further surveys and questionnaires. Though much work has been conducted over many years to try to develop surveys which focus upon understanding the core constituents of a safety climate (Zohar, 1980, and Lee, 1998) the results often reflect the safety climate of individuals, which are erroneously reported through amalgamation, as that of the whole organisation. It seems that the topic of safety climate measurement has been considerably investigated over many decades and is now inclined to be used as a substitute metric of safety culture.

The re-awakening of interest within the topic of safety culture since the turn of the millennium is attributed predominantly to the requirement to truly understand the causal factors of major events such as Piper Alpha, King's Cross and Clapham Junction. This has injected further energy and vigour into the topic; a recent review by Flin *et al* (2000) has highlighted the fact that there are many assessment tools, including survey techniques, now available to support safety climate interrogation. Such assessment tools usually rely upon a core model which is specially adapted and/or re-engineered for use within a particular industry; examples include the power industry, general manufacturing, the health industry and aerospace. Flin *et al* (2000) specifically investigated nineteen studies and concluded that sixteen had been derived from pure literature reviews of preceding safety research; six of the studies utilised qualitative methods such as discussion (focus) groups and/or

interviews whilst three used extant questionnaires. Established factor analysis was used to derive and highlight common threads; in this instance the number of threads (elements) identified ranged from a simplistic two to a more complicated nineteen. It is clearly seen from such work that this qualitative approach to safety climate measurement allows a great deal of dimensional variation in terms of subjectivity and therefore makes comparative measurements (between studies) much more difficult.

Further investigation into other safety climate measurements uncovers additional problems, predominantly with that of consistency. Glendon & Litherland (2001) uncovered the fact that when the same questionnaire was used on two completely separate occasions the results varied considerably. Zohar (1980) established that there were eight safety climate elements present in his work with Israeli production workers whilst Brown & Holmes (1986, cited in Glendon & Litherland, 2001), using the same questionnaire, found that there were only three safety climate elements present in a sample of American production workers. Glendon & Litherland (2001) further cite the work of Coyle *et al*, (1995) where they subjected two similar organisations to a common safety climate questionnaire; the results again uncovered inconsistencies. One organisation revealed seven safety climate elements present whilst the other reported only three.

Formatted: Bullets and Numbering

6.11 Developing Patterns Of A Safety Climate.

As highlighted in the preceding text, one of the main problems that the concept of safety climate brings is that of specifics; safety climate covers such an array of factors both by default and by design. Combined with this is the inconsistency of the results which, when coupled to misaligned outputs from surveys and questionnaires, leads to an inability to identify common elements within the work of various researchers.

Of some importance in the interpretation of common elements within the research of safety climate is the work of Cox & Flin (1998), where they identified five common elements from their collected data;

- '*management commitment to safety*',
- '*personal responsibility*',

- *'attitudes to hazards'*,
- *'compliance with the rules'*,
- *'workplace conditions'*.

Further work by Flin *et al* (2000) and Guldenmund (2000) gravitates towards three prime elements as a common metric for analysing (the presence of) a safety climate;

- *'management'*,
- *'risk'* and
- *'safety arrangements'*.

In support of these prime elements is the presence, occasionally, of secondary elements;

- *'work pressure'*,
- *'competence'* and
- *'procedures'*.

The following text attempts to corroborate the presence of these six primary and secondary elements.

Formatted: Bullets and Numbering

6.11.1 Management.

The element of management, (specifically management commitment and/or supervisory related), was found to be predominant within the reviews carried out by Dedobbeleer & Beland (1998) and Flin *et al* (2000). Particularly included within this management element was that of the perception of attitudes and behaviours in terms of safety and organisational output; these were included in the reviews as were other components such as recruitment selection and discipline. An observation raised by both reviews was that the term *management* was used in slightly different ways thus making it difficult to ascertain and therefore define what level of management was being reported upon. Such an observation should be carefully examined as organisations have various levels of management conducting specific roles within its operation and the perception(s) from the workforce will

alter sympathetically (Brown, 1980, p282). From the author's work within his host organisation principal managers are seen to support safety activities by creating and issuing policies and procedures. At an intermediate level, middle managers and team leaders form an important conduit between the principals and the 'coalface' workers active within the organisation. The importance of these middle managers should not be underestimated as they not only manage and monitor the daily operational activities but provide continuity and ownership through essential bilateral feed back.

During the Ladbroke Grove train crash inquiry Lord Cullen (Cullen, 2001) suggested that there was "no substitute for personal contacts" and that all senior managers within a large organisation should communicate and engage with 'coal face' (frontline) workers, especially on the topic of safety. A further suggestion offered by Lord Cullen was that senior managers explicitly schedule a minimum of one hour per week into their diaries to focus upon employee safety; additionally he suggested that middle management schedule one hour per day for such work whilst first line managers apportion 30% of their total time to safety. These suggestions were raised by the fact that the frontline workers had reported that they did not see their senior managers during daily operational activities; it was apparent that they merely saw them during special (VIP) visits. Linked to these observations of Lord Cullen's are the observations cited within Flin *et al* (2000) where a number of managers from various oil companies were questioned. The output of the survey suggested that the managers felt so weighed down by the organisation's administrative arrangement and/or by the corporately driven initiatives that they felt unable to offer sufficient time to manage safety appropriately. They did themselves acknowledge the fact that they needed to be seen amongst the workers and to be involved with the daily activities to ensure continuous safe operations. Of particular interest here is the observation made by Collinson (1999) in a case study of an offshore operation. He found that senior managers based onshore (London and Aberdeen) had quite a skewed view of the safety culture offshore. Despite advocating and driving forward a very strong and positive safety culture onto their workers Collinson found evidence of "accident concealment" on board the offshore platforms. The study pointed out how senior managers can be "hierarchically, geographically and culturally separated from local practices".

Much of the literature reviewed for this paper has shown that management commitment greatly influences the success of any safety initiatives. What is certainly in need of clarification though is the form of discrimination between the term management, often part of a more hands-off executive, and supervisors, who are predominantly seen as having their presence felt at the 'coalface' during daily operations. Thompson *et al* (1998) observed that managers and supervisors would often bias the organisation's safety culture in differing ways; he found that managers predominantly affected safety through communication and reporting whilst supervisors affected it through the level of fairness that they applied to the workers. One particular study (Simard & Marchard, 1994) did in fact try to uncover what behaviours and traits a supervisor displayed which supported accident prevention. The study looked at two circumstances; the first (participatory involvement) where the supervisor worked alongside the subordinate in any safety activities, and secondly, (hierarchical involvement) where the supervisor conducted any safety related activities without the involvement of subordinates. Though the participatory approach was deemed to be more effective at minimising lost-time accident rates the supervisor's ability to deliver such an effect was not completely independent; it was ascertained that the supervisor's results were linked to the organisation's safety activities across the whole site. The study suggested that a well developed safety regime can be positively correlated with a participatory form of supervision but, that it is difficult to examine the supervisor's role in isolation as his output will be affected by the safety culture within the greater organisation.

No review of management commitment to an organisation's safety culture would be complete without some words on corporate reputation and/or profits. A poor health and safety record has the potential to seriously damage a company's image by forcing one or more of its stakeholders to view the organisation with some disdain. Research by Smallman and John in 2001 uncovered some evidence that senior managers at board level were in fact taking the importance of a good health and safety record seriously. On a slightly different angle though was the thought that a good health and safety record did not necessarily augment the corporate image; i.e. a balance had to be struck between the cost of implementing and maintaining a health and safety regime (e.g. training, equipment,) and the possible cost of an incident. This research also highlighted how isolated the senior managers were from the costs involved. Further research identified that it was the fear of

losing its corporate image which drove a company to invest within the health and safety domain. Additional research by Peterson (1993) suggested that the lack of management buy-in was in fact more of a perception rather than a reality. Peterson went on to suggest that senior managers are in fact committed to safety and it is the barrier(s) erected by the middle tier of management which often causes issues to arise. Though middle management are often briefed by senior managers upon the importance of health and safety their daily perceptions may be obscured by other more topical or pressing topics such as budgeting, productivity or even rationalisation. Peterson (1993) therefore believes that to achieve a good safety culture within an organisation the senior managers must be seen to be supportive; the middle managers should be actively involved and the supervisors must be accountable for all daily activities. Clarke (1998) augments this view by suggesting that a positive safety culture within an organisation is provided through a systematic approach, by approaching the organisation's culture as a whole and not as a series of smaller discrete packets. Most of the literature reviewed suggests, both implicitly and explicitly, that management has a strong impact upon an organisation's safety culture. It was observed though that the various layers of management within an organisation affect the safety culture in sympathetically different ways; of importance was the observation that Collinson (1999) made that if the senior managers of an organisation are geographically remote from the workers (and the hazardous activities) then the safety policies and procedures fall into disrepute. Taking this point further, large organisations will be reliant upon local (sub-ordinate) site managers to influence the safety climate by being both operational and strategic; such an approach will occur naturally for smaller organisations where the top level managers are usually resident (by default) at the operational site.

Formatted: Bullets and Numbering

6.11.2 Risk.

Research into risk has shown that workers both within the same organisation and job-set will have varying levels of risk perception. Cox & Cheyne (2000) observed that oil and gas offshore platform workers had a greater awareness of risk and the need for safe operations than other members of staff within the same organisation. What they also found was that the drill workers had a significantly lower perception of the risks involved in the task than the management team. It was suggested in their study that this may have been due to the fact that the drillers consisted of a specialised team which was imported on a sub-contract

basis to carry out the drilling activities and that they were part of their parent company's safety culture. However this does not explain why their perception of risk was so different. Earlier work by Rundmo (1995) found that offshore workers perceived their working environment to be much safer in 1994 than in a previous period (1990). This perception included both the low end risks (e.g. slips, trips and falls) as well as the more serious risks which had the potential of being catastrophic (e.g. fire, explosion,) and could have been associated with the improvements that had been instigated since the Piper Alpha catastrophe of 1988. It would seem that if the chances (probability) of an accident occurring diminishes then the perception of risk would also diminish. Other work by Rundmo (1995, 1996, and 2000) suggests that risk perception and related behaviours are associated with the attitudes towards safety and the safety climate although the causal path of interrelationships between them is unclear.

Though the concept of risk is frequently reported within safety climate surveys (questionnaires) a clear definition for its meaning is not quite as easy to obtain; the term can include not only specific task related (often specialised) activities but those which include a more indefinite view of risk such as corporate or even business risks. Cox & Cheyne (2000) also found out that the way that workers view the risk associated with their activities, as well as their need to feel safe, as an effective measure within their safety climate assessments.

Formatted: Bullets and Numbering

6.11.3 Safety Arrangements.

The term *safety arrangements* as used by Flin *et al* (2000) is a relatively extensive term used to encapsulate the tools and methods used by various organisations conducting a host of activities in many industries. The term was devised to include constituents such as (non-exhaustively);

- Management safety committees,
- Site safety plans,
- Emergency plans,
- Crash exercise plans,
- Safety management systems,

- Safety equipment / Personal Protective Equipment (PPE),
- Health & safety representatives / managers/ advisors.

It was found that the status of the safety advisor (or manager) and the safety committee affected the worker's view of the safety climate (Zohar, 1980). We have already reviewed what role management plays in establishing and maintaining a positive safety culture and this is further corroborated by the work of Cooper (1998, p25, 175) where he suggests that the safety manager should reside within the organisation's senior management team. Such an appointment clearly demonstrates to both internal and external parties that the company is wholly committed to a safe and proper operation. It should be noted that within the author's own host organisation the role of safety, both in terms of general Health, Safety & Environment (HSE) as well as Trials Safety is represented at both divisional and corporate management boards.

Safety committees in general are formed by management teams to ensure that the workers and managers meet to align the whole process of safety. Cooper (1998, p25, 205, 212) suggested that the creation and operation of such committees could be viewed as a measure of management's commitment to communicating its safety policies to the workers. Additionally, the content of the related meetings indicate the flow and direction of safety related information between workers and management. It is broadly accepted within industry that those organisations with an effective safety committee are much more likely to take safety more seriously and to make improvements than organisations without. Such committees are often scored on their ability to influence and even promote safety within an organisation. Correlations have been identified between good safety attitudes within the workforce and the inclusion of safety topics within team briefings (Lee & Harrison, 2000). Reinforcing this view is the work of Rundmo *et al* (1998) where a link was established between poor worker management and the lack of interest exhibited by workers in safety related improvements; consequently it was suggested that poor management could lead to a reduction in safety standards. Cooper (1998, p25, 161, 191) also identified that whilst safety committees are predominantly measured upon their impact within an organisation by their ability to lever and/or support Health & Safety (in general terms) it is the time line afforded for implementation which is of greatest importance. The committee will be seen as

credible, productive and competent if its recommendations are executed promptly and advertised appropriately to the whole workforce.

Formatted: Bullets and Numbering

6.11.4 Work Pressure.

The difference between work-related stress and pressure is often not clearly defined. All individuals experience pressure daily; it is a motivator and also, for the majority of individuals, a catalyst for high performance. It is when individuals experience high levels of pressure for extended periods of time without any opportunity for recovery that stress is experienced. The HSE defines stress as "*the adverse reaction a person has to excessive pressure or other types of demand placed upon them*" (HSE, 2004b). Flin *et al* (2000) considered the pace of work and its burden collectively as work pressure. Their work suggested that establishing an equipoise between the operational pressure to deliver a task and overall safety within the environment was important; this relationship was also identified as a key element of safety culture by the Advisory Committee on the Safety of Nuclear Installations (ACSNI) in their report of 1993 (HSE, 1993). Though the perceptions of offshore workers to their management's commitment to safety were established as largely positive in a survey by Mearns *et al* (2001), it was found that the majority surveyed believed that production would not be stopped due to safety concerns if profit was at risk. In a similar survey of safety within the nuclear power industry (Lee & Harrison, 2000) it was highlighted that the workers perceived that management would put pressure upon production before safety. This primacy of production ahead of safety was perceived to be wholly driven by management and not by safety representatives or co-workers.

Another important element of safety management is that of the work pressure exerted upon managers. The Nuclear Installations Inspectorate (NII) established that excessive workloads applied to managers affected their proficiency to effectively manage and supervise safety. Such an impairment manifested itself operationally through an inability to conduct preventative and elementary safety management tasks such as investigating occurrences or the checking of logbooks (Dyer, 2000).

6.11.5 Competence.

Formatted: Bullets and Numbering

Competence is defined by the Institution of Engineering and Technology (IET) as "*the ability to perform activities to the standards required in employment using an appropriate mix of knowledge, skill and attitude*" (IET, 2008b). A further definition, albeit in holistic terms, is offered by Lindsay & Stuart (1997); "*integrated sets of behaviour which can be directed towards successful goal achievement within contribution domains*". From the author's experience of management and the application of competency frameworks within the T&E industry the term competency is predominantly used to encapsulate elements such as formal qualifications, subject matter knowledge and personal skill sets.

One of the major weaknesses with competency measurement is that of a need for continuous appraisal to ensure that what is formally recorded accurately represents the individual's extant level of competency and that all lapses, if any, are identified and managed accordingly. The NII's report on Sellafield (Dyer, 2000) identified such failings within the site's safety management regime. Their methodology for managing competency and training was seen to be defective in that records of competence were either out of date and/or were unclear on what the competencies were. Recommendations from the report included a need to apply a consistent, robust and effective method of managing staff to include human resource elements such as training, skills analysis and continuous competency assessment.

Competence and ignorance were highlighted in the report into the broader issues surrounding the loss of the Nimrod aircraft XV230 (Haddon-Cave, 2009, p262) as a fundamental weakness in the ability of QinetiQ to fulfil its role in providing independent advice on the aircraft's safety case. These issues, as well as heavy work pressures and high work loads, were was also raised against the MoD's IPT and BAE Systems; this lacking of competence in BAES led to the initial identification of 1,300 'hazards' and demonstrated a lack of competence and fundamental understanding of what was required of them within their role (Haddon-Cave, 2009, p270).

Formal training in general health and safety can be very weak in some organisations though the author must state that it is extremely good in his host organisation. The ACSNI report

of 1993 raised comments regarding the lack of health and safety training within management training courses whilst there was a distinct absence of safety related information within the majority of business related texts. Pearson (1999) highlighted that only 7% of senior executives held a National Examination Board in Occupational Safety and Health (NEBOSH) Certificate and that only 4% held the Diploma.

Formatted: Bullets and Numbering

6.11.6 Procedures.

Monitoring is not appropriate if suitable procedures are absent or cannot be devised. In a similar way, monitoring is not necessary where another method of evaluation is used that demonstrates that the control measures in place are adequately controlling exposure. Procedures must be written and reviewed by those who have both an understanding of the real practices conducted by those staff who will use them and of any safety related requirements demanded by the organisation.

Once written, and used for a relatively short span of time, any newly-created procedures must be carefully reviewed and altered (evolved) to ensure that all sub-activities are effectively encapsulated and duly risk assessed. The opportunity for local equipment managers to discuss any changes required of any procedure should be seen as an important prerequisite for effective organisational safety management.

Formatted: Bullets and Numbering

6.12 The Existence Of Sub-Cultures Within Organisations.

Many of the definitions and constituents of culture have been included previously in this chapter. Most of these definitions may be encompassed in a general statement of workers holding shared values, tenets and beliefs (even morals) regarding safety. Such a view appears logical and fits in with the majority of literature reviewed by the author. One of the main issues for larger organisations (the author's host organisation is included here) is the management of sub-teams and their *de-facto* sub-cultures. The existence (and presence) of sub-cultures within larger organisations suggests that the business is not a fully holistic entity. The work of Pidgeon (1998) questioned if a culture change or culture management initiative could be designed for a large organisation without due cognisance to any sub-cultures which may exist. Such sub-cultures will no doubt have their own hierarchical order

where relationships and interactions will differ both within the sub-team and across to other sub-teams.

Mearns *et al* (1998), during their survey of offshore platforms, found evidence of safety sub-cultures operating with different perspectives and views of safety within the industry. Such sub-cultures manifested themselves through variations in age, work pattern, appointment and even rank. A further component which affected the creation of a safety culture was that of accident involvement; i.e. a greater diligence to safety was applied when a member of the sub-team had been involved in an accident. These findings were supported by further research into the roadways construction industry (Glendon & Litherland, 2001) where distinct differences were seen in the safety culture across relevant sub-teams.

The lack of effective and continuous communication between the day and night shifts that led to the Piper Alpha incident, in spite of the presence of safety management systems (e.g. shift hand-over systems) (Mearns *et al,* 2001), was indicative of the presence of safety sub-cultures and that they can, at times, lead to variances, incompatibilities and even conflicts. Collinson (1999) suggests, somewhat negatively, that sub-teams tend to assess safety from their own localised position rather than buying into the wider organisational perspective. From a different standpoint, Mearns *et al* (2001) suggest that these variations in risk perception should be aggregated to form a richer and deeper knowledge pool thereby offering wider boundaries to the identification, assessment and management of risk. For this type of approach to be successful the focus of management should be upon effective communications and conduits to enable the various safety sub-cultures to exchange views and any subsequent deliberations. Another catalyst for the creation of sub-cultures is the use of different terms of employment for workers within the same organisation. Collinson (1999) found that sub-contractors operating amongst the most dangerous and demanding tasks without paid leave (sick and/or holiday) became isolated from the owning company and its management system. Safety management was seen as something which was second in priority to continued production output; subsequently, and quite understandably, their accident record was greater than that of the owning company.

Research into the cultures operating within the nuclear power industry uncovered evidence of a dichotomy; the presence of a management safety culture in addition to a 'worker' safety culture. The former included technically competent staff whilst the latter included industrial staff (Harvey *et al*, 1999). Though they identified that the existence of two sub-cultures could cause problems in areas such as communications or even actions they did not conclude that it was detrimental to the operation. It was suggested by them that through the use of effective communications the divisions between the two parties could be minimised.

Though the extensive number of reports researched here offers information and views on the safety climate of an organisation they do not however identify any donations to the overall safety management offered by any sub-cultures. As well as the safety sub-cultures which may occur within the sub-teams of large organisations there would be instances where other sub-teams were created by the business during its daily operations. Such instances would occur when (for example) external agencies such as contractors were employed to conduct specific tasks. The author has experience of competing agendas within his own host organisation, typically when third party contractors were employed on civil or building works, where some (minor) safety requirements were breached in their hastiness to complete a time constrained task. Though initially reported as a sub-team (contractor management) failing, the incident would be investigated and corrective action applied if appropriate; but, it typifies the lack of distillation and cognisance that could be applied to gain a deeper understanding of safety sub-cultures (in general) within the larger organisation. Note that this example is typical of all major organisations and should not be read as a specific negative against the author's host organisation.

Formatted: Bullets and Numbering

6.13 Effective Communications Within Organisations.

The topic of communication, especially effective communication has been discussed both directly and indirectly in much of the previous text. Communication in its base form can be defined as *(1) the act of imparting, especially news. (2) a means of connecting different places. (3) social intercourse. (4) the science and practice of transmitting information. (5) the means of transport between a base and the front (military). (6) a paper read to a learned society.*(Oxford, 1995).

It was suggested earlier within this paper that the presence of an effective communications element within an organisation aligned well with the presence of a positive safety culture. The presence of effective communications allows for the sharing of ideas, views, concepts and in fact risk; safety is therefore deemed to be of importance to all employees and not the millstone strung upon one individual such as the HSE adviser. As these shared beliefs expand the level of mutual trust across the organization grows and with it a level of confidence in the mitigations which must be maintained for a safe working environment. The Health & Safety Executive have issued many papers and articles relating the importance of effective communication to a positive safety culture; HS(G) 48 (HSE, 1999) outlines how managers can communicate effectively with their employees in a number of ways. The three key methods are;

- By the use of visible behaviour managers may communicate to employees the importance of health and safety within the work domain. This concept relies upon the sub-ordinate monitoring and adapting its behaviours to align with that of the supervisor. Management commitment to the safety ethos may be conveyed through participation in site safety inspections, attending safety meetings and by active participation in accident investigations. One caveat to be applied is that any management negativity can undermine the whole process of developing and/or sustaining a positive safety culture.
- Through the use of written communication such as health and safety (corporate) policy statements, minutes of formal meetings, company performance, results of audits (internal & external) and notice board newsletters *et al.* This latter form of communication, though one-way, conveys the same information (and therefore, image) to all parts of the organization and is important in creating a single and aligned safety culture. It also acts as a catalyst for discussion and debate between workers and management.
- Face to face meetings between workers and management which allow healthy discussions and therefore personal ownership of issues to be developed. From a human behaviour perspective such engagements allow the workers to feel as if they are personally contributing to the development of a safe working environment. Face to face meetings need not be solely confined to the ritual and formal site meeting

agendas but should be promoted within the more informal briefings as well as any site walk-around tours. By discussing safety in the periphery of other discussions it moves from being a bolt-on topic to being a fully infused part of the daily operation; a tool to help and support daily operations rather than being viewed as a bug-bear or a limitation on any process.

Communication (specifically the lack of it) was clearly identified as a weakness within the rail industry (Cullen, 2001) where its level and quality varied considerably. Lord Cullen emphasized that effective communication is paramount to maintaining a safe operation and that it involves all parties engaging in listening and discussion. The inquiry also identified that workers feel more valued, respected and demonstrate a belief within the host organisation when engaged in effective communication.

Formatted: Bullets and Numbering

6.14 Collecting, Measuring and Analysing Safety Related Information.

Companies are strongly recommended to record and analyse their safety performance in order to either maintain or improve their operational health and safety performance. These recommendations are reiterated in the HSE's publication, HS(G) 65 (HSE, 2000). The safety performance of an organisation may be measured and analysed by proactive, active or reactive methods. One concept in the application of a proactive approach is that of deploying lead indicators within the organisation which tries to forecast trends within an organisation's safety performance. The active method relies upon the organisation actively putting in place facilities such as environmental monitoring, worker health surveillance & screening regimes, plant (equipment) inspections, site inspections and audits. The reactive approach is usually initiated by an occurrence or an incident (including a near miss) where the event is identified, reported, investigated and lessons learnt (if any) are realised. Typically within this type of approach to an occurrence, local boards of enquiry as well as independent and external review may form part of the overall investigation. Virtually any industry and any organisation has a host of both qualitative and quantitative tools available which may be used to measure and analyse its extant safety management system and/or its safety climate.

6.14.1 Qualitative Approach.

Formatted: Bullets and Numbering

Qualitative approaches try to identify and analyse elements of the safety management system which may have an effect upon the overall system risk (Kennedy & Kirwan, 1998). Though they often qualify the quality of a particular element of a safety system they will not give a numerical output of the predicted risk level within it. Despite such limitations the qualitative approach is very useful in understanding an organisation's safety culture from a 'systems' or 'holistic' perspective. By utilising assessors with a varied background and skill set a combined judgement may be offered of the organisation under scrutiny. The combinational effects of the various inputs (e.g. from questionnaires, interviews, audits, etc.) may be interpreted giving a 'gestalt' view of the organisation's safety culture (Kennedy & Kirwan, 1998). One of the limitations of such an approach is that the indicators chosen (questions) need to be sufficiently accurate, realistic and comprehensive to include all of the issues which need to be analysed. Some of the tools used for qualitative appraisals include analysis frameworks such as Operant Supervisory Taxonomy Index (OSTI) and the Nuclear Organisation and Management Analysis Concept (NOMAC). Other methods include audit tools such as the International Safety Rating System (ISRS); the Management Oversight and Risk Tree (MORT); the Complete Health and Safety Evaluation (CHASE); the Five Star System (FSS); the Professional Rating of Implemented Safety Management (PRISM) and the Assessment of Safety Culture in Organisations Team (ASCOT) (Kennedy & Kirwan, 1998).

6.14.2 Quantitative Approach.

Formatted: Bullets and Numbering

Quantitative approaches to assessing a safety management system are generally based upon the use of Quantified Risk Assessments (QRA) or Probabilistic Safety Assessments (PSA). QRA uses numerical data from inventories of equipment and/or sub-components to make an overall quantitative assessment of the overall system under analysis; such an approach is predominantly (but not exclusively) used in the process industry. The tools used for assessing a safety management system within the QRA approach include MANagement Assessment Guidelines in the Evaluation of Risk (MANAGER) and the Process RIsk Management Audit (PRIMA).

The PSA approach has been developed from the high risk industries such nuclear energy plants where the need arose for a more holistic approach to risk management; it assesses the risk offered from virtually all types of failure including human, hardware, software and even the environment (Kennedy & Kirwan, 1998). PSA involves modelling the relationships and events (failures, interactions, etc.) within a system and determining quantitatively what the likelihood and consequences would be if an incident actually occurred. One of the more well known tools for a PSA approach is that of Work Process Analysis Modelling (WPAM).

For large and complex systems, quantitative analysis commences with the smaller sub-systems and is numerically 'aggregated' with other sub-systems to form an overall quantitative system risk. This final risk figure can then be compared with any regulatory or legal requirement that the organisation must comply with; for example the risk of a weapon excursing the boundary of a Test & Evaluation (T&E) Range facility must be lower than one event in one million ($1:10^{-6}$) (MoD, 2004).

In conclusion, it is accepted that the PSA approach allows the safety management process to be effectively modelled and therefore enables the failure events to be effectively traced from source to (possible) consequence. This approach is deemed appropriate not only in determining failure paths and causal chains but in the uncovering of failure combinations though some of the assumptions and extrapolations that may be required from information gained through audits and/or questionnaires may be quite large (Kennedy & Kirwan, 1998). Succinctly, PSA requires that the possible causes and failure mechanisms are specifically and comprehensively modelled whilst QRA requires either no modelling or a much lesser degree of modelling. Whilst the level of detail and depth applied to the modelling can seem onerous, the usefulness of such an explicit approach not only determines the level of risk but can form a useful guide in its reduction post initial identification and assessment.

Formatted: Bullets and Numbering

6.15 Incidents And Near Misses.

In researching this paper the author found it difficult to identify and qualify the safety climate results which are discussed in the various sources; this is due predominantly to the fact that safety behaviour relies upon self-reporting regimes. As in the author's host

company, the majority of information gleaned from near misses and actual occurrences comes from the 'coal-face' worker; this in itself subjects it to local interpretation and/or filtration before it is entered on the management's recording system. Actual incidents (relatively small) may be interpreted by workers as 'mishaps' or just 'mistakes' and may often be hidden or misreported to the organisation. Though isolated and local in nature (e.g. chemical spills, trip or fall) they may form part of a series of indicators of a much larger health and safety problem. Cooper (2000) suggests that one of the fundamental weaknesses with the self-reporting regime employed is that it is subject to "*social desirability biases*" where the workers feel compelled to behave as they *should* rather than as they actually *would*. Therefore it follows logically that measuring worker's beliefs and convictions may not predict how they would actually behave.

By investigating near misses an organisation gets access to both a good measure of extant health and safety performance as well as opportunities for learning from mistakes. Though very useful, applying diligence to near miss reporting usually occurs in only a few industries, predominantly those with the potential for major incidents and relatively large catastrophic consequences. Examples include the airline industry, the offshore (oil & gas) industries, the nuclear industry and aerospace (e.g. munitions & military aircraft operations). These industries have a well-founded and mature 'no-blame' culture in which reporting is acceptable to all.

Near miss reporting requires organisations to investigate occurrences which may have possibly led to an incident in order to try to minimise the chances of a similar occurrence and/or a more serious consequence from happening in the future. Pidgeon (1998) highlights how the monitoring of near misses is used to promote and engender safety management improvements within industries such as aviation. A key environmental component in the creation of a safety conscious culture and the reporting of near misses is that of a 'no-blame culture'. Various published papers discuss a 'no-blame culture' and whilst the theory is very acceptable and simplistic its application in the real world, especially within the more safety critical industries, brings with it some problems. Pidgeon (1998) suggests that the prime problem is that of the "*dilemma of blame*" where immediately after a serious incident there is a craving to not only understand what happened but also to identify an individual to

blame. This need to establish blame should not be dismissed without some further thought. From a positive perspective the presence of blame ensures that individuals with responsibilities within an organisation's safety management system must also carry the mantle of accountability; a burden that many managers find difficult to own when incidents occur. The greatest drawback from this approach is that individuals will tend to hide many safety related issues; a culture of blame evasion may develop which leads to a downward spiral. Pidgeon (1998) goes on to suggest that a 'no-blame' organisational culture is not the solution and that the issues should be sub-divided into "*culpable*" ("*deserving blame"*, Oxford, (1995)) and "*tolerable*" ("*able to be endured"*, Oxford, (1995)) errors.

The performance and behaviour of most organisations is largely measured against the results offered by accident and/or near miss reporting. Such metrics are termed as lag indicators of safety performance. The output of a report carried out on a wood processing company in Finland (Varonen & Mattila, 2000) identified that there were two dominant elements which correlated its accident statistics with its overall safety climate. Specifically these were (a) the level of training executed, and (b) the level of good 'housekeeping' demonstrated throughout the organisation. A higher score in safety climate aligned with an overall reduction in the accident rate. It should also be stated that safety improved when senior management demonstrated a positive attitude to safety and when the work environment was clean and uncluttered. Despite such findings it is suggested that the use of accident information for safety performance measurement is fraught with problems (Cooper, 2000). Such information does not take cognisance of the different risk exposure levels across the various operating environments; is often subjected to local interpretations on seriousness and/or magnitude; and ultimately different organisations (and sub-teams) may not report each and every occurrence. Another issue with that of using such information to measure the safety climate is that of the inherent timelines involved between the occurrence, the investigation and the feeding back of data to the management team. The information dataset is very much a lagging indicator and as such should be viewed as a measure of consequences rather than that of risk. Cooper (2000) suggests that a reduction in reported accidents may be due to a change in metric or a change in the business elsewhere rather than as a direct result of an organisation's safety culture; for example, some incidents

may not be reported as it may impact upon an individual's (or team's) financial bonus payments.

The monitoring of safety behaviour has been used in many organisations as a metric to identify or support overall safety performance; predominantly this focuses upon the random sampling of how workers go about some of their everyday tasks. Examples may include using independent and trained auditors to judge lifting techniques, the use of appropriate (and safe) practices or even disposal of hazardous waste. Cox & Cheyne (2000) used this type of behavioural evaluation and combined it with both employee attitude assessments and interviews to create their 'Safety Assessment Toolkit'. The report suggested that minor incidents and near misses may be identified through directly monitoring worker actions. These observations can then be tabulated to form a 'checklist' whereby the behaviour (and consequential actions) can be correlated against a particular form of accident avoidance. Cox & Cheyne (2000) further state that these behavioural elements may be used as indicators to help support the creation of a more holistic model of an organisation's predominant safety climate. This theory has some virtue but does not identify any empirical evidence between an organisation's safety climate and its employee's safety behaviours. In their research of the offshore industry, Mearns *et al* (2001) examined the relationship between worker's perceptions of risk, their behaviours and their attitudes across two years of data. They concluded that there was a great amount of correlation between what the worker thought of the management team's commitment to safety and the worker's consent to self-report any occurrences. It was also observed that the worker's perception of a manager's competence level within his field was important.

Formatted: Bullets and Numbering

6.16 Developments Within The Behavioural Aspects Of Safety Management.

Some organisations, in an effort to modify safety behaviours, have introduced a rewards based initiative where rewards are given for reductions in the number of accidents that occur within the organisation. Whilst well intended such an approach can often lead to the misreporting or none reporting of incidents which may lead to a false sense of security. Cooper (1998, p35, 112, 183) suggests that a complete lack of information on accidents and incidents, especially near misses, is a prime indicator of poor organisational culture. Other approaches which actively encourage the reporting of safe organisational behaviour such as

near misses, safety problems and possible improvements are deemed to be more effective and appropriate.

Behavioural based safety involves identifying, through direct observation, behaviours which are deemed to be safe and those which are not. Such an approach usually involves training of workers and/or the use of specialised observers to help create a baseline model for the extant organisation. By creating work teams, identifying targets and giving management encouragement, the workers focus upon raising the safety level of the environment above and beyond the baseline.

The use of behaviour based safety, though a useful tool to use within an organisation, is limited and can put the onus of safety behaviour completely upon the worker. During such occurrences management's level of ownership for the organisation's safety culture may be eroded somewhat. Atkinson (2000) suggests that although the worker has been trained in safe behaviours, (e.g. to call the engineer to unblock a mechanical machine), the safety culture of the organisation may still give primacy to production thereby pressurising the individual to quickly unblock the machine themselves.

Formatted: Bullets and Numbering

6.17 Summary.

Culture may be viewed as a notion which describes the collective values and opinions within an organisation; it is that which models and shapes the behaviours and attitudes of those individuals within it. The safety culture of an organisation is a component part of the overall organisational culture and may be viewed as an influencer in terms of the organisation's beliefs and behaviours towards safety related activities (Cooper, 2000). Though Flin *et al,* (2000) have tried to differentiate and clarify the differences between safety culture and safety climate, it remains very difficult to maintain the dichotomy when dealing with the reality of every day issues. It is due to this prime reason that the terms safety culture and safety climate are often swapped erroneously.

The research reviewed suggested that the worker's perceptions of management's attitude and conduct towards safety, operational planning and output was the most convenient method for measuring an organisation's safety climate. The research also suggested that

different levels of management within an organisation impacted upon the workers' perception of health and safety markedly; levels and type of communication as well as fairness in dealing with occurrences were important.

HS(G)65 (HSE, 2000) strongly advises that safety advisors within organisations should have sufficiently high enough status, training and relevant competencies to both advise management and to engender the correct attitudes within the workforce. Cooper (1998, p175, 205, 210) suggested that the overall status of safety advisors was perceived by the workforce as a reflection of management's devotion and buy-in to safer activities. If principal managers (predominantly senior executives) cannot perceive the importance of effective health and safety management then the safety advisors will not be appointed at any appropriate (and useful) level within the organisation. Safety committees are heavily reliant on senior management attendance and support to be effective; if managers view safety forums with disdain then worker attendance will dwindle and any outputs will be diluted and weak. Change management may suffer as a consequence.

Performance measurement is deemed to be important in so far that it allows the extant safety environment to be measured and used as a reference; as new initiatives are rolled out across the organisation then further data may be recorded to understand the effects, both positively and negatively. Performance may be measured using near miss reports, post accident data, behavioural methods, independent audits and even through self report questionnaires.

The use of bonus schemes to improve production output and/or to compensate for hazardous operations may lead to the development of unsafe practices through pressurising workers to work quicker, inducing risk taking and even not reporting accidents. The use of any bonus scheme must be carefully considered and rationalised against possible changes in worker behaviours before being implemented.

Whilst site safety audits and inspections may be used usefully and effectively to measure an organisation's safety environment they must be carefully administered and not confused with each other. It is suggested that effective audits should be conducted by suitably

competent, trained and independent individuals and/or teams. Again, it must be stressed that management commitment to the process is fundamental to an effective audit. By demonstrating support through the availability of time, resources and participation managers will communicate and engender the correct image to developing a more positive and healthy safety culture.

This page left intentionally blank.

Formatted: Bullets and Numbering

CHAPTER 7

A 'Systems' Approach To Safety Cases

7.1 Introduction.

The preceding chapter on safety culture identifies how organisations seek to construct defences to minimise the opportunity of human error creeping into their activities. One of tools used to monitor and feedback the 'climate' of safety attitude embedded within the organisation is that of the use of a questionnaire which is duly completed by the staff. By the use of established industry criteria and definitions the responses to these questions are presumed to allow a measurement to be made of the organisation's prevailing safety culture.

We currently live in a very highly technological era where most of our daily lives are controlled or influenced by high technology applications. Farmers gather crop yield data whilst harvesting which is loaded into a real-time processor aboard the harvester; the yield figures are also correlated with map co-ordinates fed from the on-board Global Positioning System (GPS) so that fertiliser and seed dispersal may be similarly controlled the following year to optimise returns. The same harvesting machine advises the local main dealer of its servicing and maintenance requirements via a satellite link; the farmer receives a telephone text and/or e-mail message to advise of the arrival of the engineer on site. The same satellite link will completely disable the harvester, when appropriately advised by the supplier, if hire purchase payments are defaulted; control of such activities are often executed from other countries and/or other continents.

Despite our current tendencies to over complicate our lives the fact remains that this was not always the case. Since we started to operate in higher risk environments, such as commercial explosive manufacture, and started using machinery to optimise outputs in other industries, many lives have been saved and/or made safer by the timely application of just plain, simplistic and often inspired technical arrangements. Examples which quickly spring to mind include Samuel Plimsoll's marking on the side of a ship to show its legal limit of submersion when loaded with cargo under various sea conditions. Mining in

general has been a greater beneficiary of risk mitigation due to its inherent dangers and lengthier history when compared with most other industries; mining for coal, ore, precious gems and building material range back to many centuries. The introduction of the miner's safety lamp and alternative routes for egress (The Hartley Colliery disaster, chapter four) are just two further examples of how similar incidents were averted by applying some quite simple and basic precautions.

Western society has done a huge amount over the past century to deal with some of the most obvious roots of accident causation; as far back as 1802 the welfare of children working in the textile industry was seen to be in need of a form of control (*Factory Act, Health and Morals of Apprentices Act*). Clearly it can be deduced that the most obvious and largest causes of risk are primarily seen and dealt with the quickest whilst those which are less obvious and do not carry high consequences take longer to become conspicuous and to be dealt with. What is apparent in today's society, as a function of the aforementioned progressive approach, is that causations will become less obvious and mitigations or controls will become more complex and involve a multitude of components, often from disparate areas. Such an evolution therefore suggests that a somewhat different and probably discerning method is required to effectively decompose, understand and manage the risks embedded within today's activities. When combined with the technologically varied, multi-disciplined and very complex systems operated within today's society the need for such a different approach to risk management is again magnified.

From a financial perspective, as the progressive approach to removing risks is applied, one can quickly identify how the risk mitigation returns get progressively smaller as the cost of any application rises. In real terms, as society gets safer and the level of accidents and fatalities subsides then the cost of providing a subsequent and higher degree of safety increases. Whilst another host of papers could be written for and against the morals of such an argument the reality is that we are probably approaching a point whereby the cost of the next safety mitigation may be too expensive to apply. The author would suggest that the practical implementation of the ALARP concept as applied by the H&SE may need to be re-visited in due course, especially in relation to what financial figure may be applied to avoid a fatality. It may be prudent to consider augmenting the ALARP principle by

assessing the overall net safety gain (or loss) after applying any mitigation whatever its financial cost.

Whilst the progressive approach to applying safety mitigation trundles forward many organisations are collecting a large amount of information relating to fields such as ‘near misses’, ‘incidents’, ‘fatalities’ and ‘safety culture’ to name but a few. Though such activities demonstrate a good proactive approach to safety management and the application of due diligence, the author, from his own experiences within his host organisation, suggests that the information gathered is not optimally used. A variety of regulatory, corporate, divisional and local forms and databases are used everyday in various organisations in various industries to record virtually everything pertaining to some event or other. How many true and meaningful lessons are learnt from these records? The author would suggest that the majority of information recorded is left in the archive until it is discarded in a number of years due to the need to ‘move on’ or to ‘streamline the company’. Any output gleaned from any such report predominantly manifests itself as a series of small internal recommendations, or at times, a knee-jerk reaction to an incident which had an increased profile within the organisation. Quite often the recommendations do not identify or address the real underlying causal factors which may have been hidden by complicated structures such as internal political ‘wars’, organisational pressures or socio-technical issues, implanted, surreptitiously, many years ago. From experience, the author would suggest that the degree of focus and energy applied to the reporting of an incident within his own organisation is often determined by the perception and personal judgements of those managers directly involved in managing the area of incident. Consequently the delineation of what is reported as a near-miss, or an incident, is biased to a degree by subjective decision making; in a similar manner, the degree of investigation is also driven by subjectivism. Of note is the fact that many of the ‘lessons learnt’ which are published by organisations are not identified because of their clear and strong importance but as a direct function of the fact that the incident had been treated more importantly and that more time and energy had been given to exploring the causations. The author suggests that in a similar manner many large accidents may appear much more complicated than a ‘near miss’ whilst in reality the latter may have been equal or greater in complexity, but due to the lower level of scrutiny applied it is deemed to be less complex.

Of concern to the author and key to this thesis is the systematic refusal by many managers, including safety managers, to actually recognise the information gathered in reports, statements, interviews and recording media, in support of incident reviews and investigations. Such information is generally regarded as being too subjective though it probably contains many hidden truths which could enable a better judgement to be made and therefore better identify the true causal routes of an incident. The author strongly believes that this subjective information is key to learning about the truth behind an incident; currently the trend within organisations is to avoid subjective information and focus predominantly upon collecting objective data sets. In simple terms we need to understand not only what has been said (or written) but also how it was said (or written).

The aforementioned is probably exaggerated by an organisation's operating ethos. Managers, and supervisors to some degree, rely very much upon being fed 'objective' and somewhat 'filtered' data sets within reports which have been created in accordance with local business requirements; collected data is usually rather succinct due to the limitations of the fields within the corporate form combined with the time pressures to sentence causation and move on to the next task.

7.2 Integrated Air Range Safety Case.

Quite clearly the high level safety case for the integrated Air Range project discussed in chapter five is wholly focussed towards providing the regulators of safety (both internal and external to the organisation) with a quantitative figure of risk. Whilst each of the T&E safety engineers involved with the preliminary safety assessment had in excess of 20 years of experience within the industry their well honed, wide-ranging and qualitative skills were not effectively utilised.

The whole experience of creating a preliminary safety argument was governed by the constraint of an established quantitative approach in the guise of a Range Safety Case. Though a qualitative and somewhat subjective approach was allowed to occur in the creation of a HAZOP analysis; this was probably the only real identifiable occasion for using a qualitative approach. Whilst the HAZOP analysis allows some degree of freedom of thought, the exercise, as with others that the author has been involved with, becomes

very quickly focussed and reliant upon the HAZOP codeword cues. One of the dangers with the code words, especially when they are applied repetitively to one activity after another is that the thought process driving the objectivity becomes 'flavoured' or 'skewed' by a former activity which was discussed at length. In simplistic terms, if one of the earlier activities which were 'HAZOP-ed' led to a somewhat specialised discussion (possibly leading down a 'rabbit hole') then there is a danger that any subsequent analysis of other activities may be similarly affected. Linked to this issue with the use of HAZOP codewords is the underlying reliance upon the codeword list as the 'holy grail' of catalysts for hazard identification, discussion and sentencing.

One of the impediments of using a HAZOP approach is that of the limitations of the panel of assembled engineers. To allow a reasonable degree of hazard scrutiny to occur during the exercise there is a need to have both a relatively large number of engineers and experts present in relation to the size of task and the team must also encompass many disciplines. From the author's experience it is suggested that some of the disciplines which need to be employed for an effective hazard analysis may seem peripheral or even obscure to the project team. The value of non-specialists must not be ignored; the opportunity to ask simplistic and 'dumb' questions often leads to an enlightenment, especially when dealing with large and complex systems. At first sight an engineering project may seem relatively straightforward and to the un-initiated may demand the attention of a project team consisting of hardware and software specialists; upon further investigation there may, for example, be a need for a Human-Machine Interface (HMI) specialist, an ergonomics specialist, a psychologist, a thermodynamicist or even a ballistician to be present for the decomposition and analysis of hazards. This type of approach is acceptable and realisable both in time and cost terms for relatively large projects but has severe limitations for projects which are relatively small or cost sensitive.

As stated earlier, the creation of the preliminary safety argument was completely driven by the need to ultimately identify both systems and sub-systems which could be assigned a quantitative figure of risk and which ultimately would support the extant safety cases of the two sites. The extant site safety cases are underpinned by hazard logs which were populated through the use of similar HAZOP exercises complemented by periodical peer review by

Range Subject Matter Experts (SME). The quantitative aspects of the site safety cases are analysed using Boolean algebra and displayed using fault tree analysis; such an approach displays a logical sequence of events leading progressively to an overall quantitative figure of risk for both the sub-systems and the complete system under scrutiny. What is certainly prevalent within the author's environment is the focus upon achieving or calculating a risk figure which is acceptable to the corporate model of risk management; as reviewed within chapter four the acceptability of risk within the organisation is driven by the HSE's risk tolerability model. Calculations to support the quantitative (FTA) models at the sites are almost wholly focussed on the engineering and functional failures of components and sub-systems; the only qualitative aspects which are taken into account are the subjective use of historical data on archaic systems to develop 'proven by usage' arguments and/or to assign simplistic and generalist human error figures for equipment operators. Very little attention is paid to the competency and skills element of any operator despite the presence of robust real-time monitoring and multiple peer reviewing of actions combined with a good incident reporting system. Discussions with the Aberporth Trial Safety Manager (TSM) during 2009 suggest that the inherent engineering systems and processes employed at the site give the required level of risk mitigation; there is little need to analyse the more subjective and qualitative aspects of the system. This suggests to the author that a degree of valid qualitative data may be being ignored systematically within some large organisations.

Whilst quantitative data has been selected as a prime source historically to best argue the risks and consequences of safety related activities the author suggests that much important information relating to context and perspective may have been filtered or even disposed of through ignoring the qualitative data. It may be argued that those individuals who are tasked with managing and/or reviewing safety arguments should use all of the available, relevant, dependable and authentic data in the quest for an optimal safe solution.

7.3 A Subjective View of Safety.

From experience and from communications with other safety managers, the author offers the view that the extant safety management regime, certainly within the T&E environment, is predominantly focussed on objectivity and a quantitative approach. Notwithstanding this last statement the author suggests that there is more to be learnt from the subjective and

contextual information which surrounds any incident. This thought strongly supports the work of Davies *et al* (2003, p16) who state that; "*the whole area of risk and safety is grounded in individual differences and subjectivity; that such subjectivity is a useful source of information*;…".

Whilst subjective and qualitative data may be rich in explanatory and contextual terms its manipulation and measurement is very difficult to manage. Questions arise as to what metrics may be used to indicate the importance or strength of a certain key item of information whilst another may be related to how we ensure that one individual's perception of importance or insignificance aligns broadly with another? Whilst it may sound difficult to answer these questions there are methods available which may be used to help identify an aligned approach. It has already been stated that quite often a simple and relatively cheap human factors application will minimise risk before the need arises to devise and employ a complicated and expensive technical solution. One of the basic and earliest pieces of advice that the author was taught during his formative years in T&E safety was to ensure that any weapon was pointing in the right direction, i.e. in a safe direction, and that all personnel and equipment were located behind a large lump of reinforced concrete! Risk mitigation at its cheapest and simplest state.

Wilde (1994) reviewed a number of studies of car drivers which provides supporting evidence to the aforementioned. His conclusions included the observation that an increase in future public safety would unlikely be found in a 'technological fix' due to the way that people respond to such 'fixes'. Alternatively he suggests that the future of increased safety lies within the human being rather than within the machine or environment created by the human. Whilst some aspects of this approach seem rather absurd (clearly there is a desire and a need for some technological fixes) Wilde does recognise that the human interfaces and aspects of safety are quite often ignored in instances where there is a clear opportunity to use a simplistic and cheap approach. This approach, if directed at the human component, may deliver a relatively better solution than an alternative which demands complex technology and probably more expense. In conclusion, there is a need to develop a method of recording, measuring and acting upon people's free text and speech so that safety

managers may enhance their own abilities to better understand the foundational problems often encountered in wide reaching and often complicated systems.

Risk and people's individual perceptions of risk have already been discussed in previous chapters and is known to be varied and a function of local attitudes, beliefs and even social cultures. These variances in risk perception, including what they perceive as being personally important or not, when combined would provide the safety community with a much greater degree of understanding to allow the management of risk to be taken in new directions.

7.4 Quantitative and Qualitative Safety.

The majority, if not all of the methods identified for managing risk seem to be based upon the same theoretical approaches and appear to be commonly driven by a deterministic view of life; the author is conscious that he has little experience of safety management processes outside of the Western world and therefore caveats the aforementioned statement. With this in mind the author would certainly advocate future studies to research how safety is managed, even in general and less formal environments, outside the developed Western world. There may be opportunities to learn how other cultures view and value subjectivity.

Whilst the application of common sense relates well to the aforementioned observation to apply simple and cheap control measures before any expensive and complicated technological 'fix' there is a need to create or to adapt a new approach to handling and processing qualitative and subjective information. Davies, *et al* (2003, p18) identify this as a problem area and raise the issue of;

"*the lack of rigorous methodology for dealing with 'subjective' reports concerning accidents, their causes and their consequences, where the choice appears to be between, on the one hand, a loose and undisciplined qualitative approach, in which extracts from reports are selected apparently whimsically by a third person as being particularly salient on the basis of criteria which remain unspecified and unknown, and on the other an approach which seeks to demonstrate its 'scientific rigour' by simply refusing to accept*

that such subjective reports might constitute useful data in any form, or even be amenable to principled and replicable analysis."

Modern science itself is caught up somewhat in differing paradigms of determinism, probability and even a half way house such as chaos theory; the latter being based upon a deterministic approach but never having sufficient information at hand to qualify or accurately forecast the output of a non-linear system (Crystal, 1990, p240). What is common though to all of these paradigms is the human element; it is the human who either observes, investigates or postulates a theory. Surely in light of such a common denominator in virtually all that underpins our quantitative and objective lives we should pay more attention to its interference, both constructively and destructively. Whilst the delineation between what is subjective or objective seems very distinct the determinant as to which side of the fence that it falls into is so ludicrously fickle that it approaches absurdity; if an observation such as a broken fence at a school playground is reported to a head teacher the fact that it has been reported by another party immediately sentences it to be classified as 'subjective'. If it had been observed first hand by the head teacher then it is classified as an 'objective' and real fact. By simply having the observation reported by another individual the fact is 'downgraded' as if it may be inaccurate, biased or even fabricated; and all of these presumptions may be applied despite the fact that the observation was reported by the deputy head teacher for the school! Verifying that there is in fact a broken fence can only really be done by going along and observing the fact for oneself; but surely we cannot demand this approach for all observations and issues raised by other parties or we would very quickly undermine one of the prime tenets of civilised society, trust. Additionally, we just wouldn't have the resources available to review every observation in person.

From a safety management perspective the safety manager and/or engineer relies upon third party reports, statements, interviews and even technical publications, often written many years ago, to create, understand and even make recommendations in support of risk management. From the author's experiences, organisations take time and incur relatively large costs to both train staff to report safety incidents and to put in place a system of reporting them including data bases, websites and forms; yet those organisations are not very well equipped to manage and interpret the gathered data. Within large organisations,

which are very hierarchical in composition, the author suggests that a great deal of important information may be lost during translation from tier to tier; this observation may also be not unique to safety management.

Safety reporting is motivated by individuals who want something to change or to inform the organisation that something nearly 'caught us/me out'; this therefore suggests that there are morals and passion contained within the reporting event. Whilst some individuals will write a better or worse report the fact remains that there is a degree of subjectivity to the recorded data. The majority of the safety information recorded is from other people's reports and reported probably with varying levels of subjectivity and selectivity and also from personal perspectives of varying understanding, skills and interpretations. Despite the vagaries of such reporting the value of what is contained within the reports remains important; not only to the recipient (i.e. the organisation) but also to the originator of the report.

A great amount of work has been carried out in the field of interpreting free text information to create a more clearly bounded objective model from such qualitative data. Whilst the Newtonian perspective of determinism relies on a model of an universe which is populated with many objective and ordered facts, more recent work by Groenweg (1996) and Carver & Scheier (1998), who have looked at applying theories such as chaos and/or catastrophe theory to the study of human behaviour, suggest that the ultimate truth (of the universe) may either be a delusion, be based upon misconceptions or deterministic in principle but pragmatically unknowable (Davies *et al*, 2003, p22). Of note though, is that relativity, quantum mechanics and chaos theory are all dependent on the human as the 'observer' of what is uncovered. The human, and the techniques used, are all considered as an integral part of the system under scrutiny and are considered as having a direct influence upon the observation. On the other hand, the Newtonian deterministic perspective considers the human as independent of those elements which are being observed.

The author suggests that the whole process of collecting and analysing safety information in support of a safety argument should not be considered as a pure and formal scientific activity; it is suggested that the extant methodologies of obtaining objective information,

often clinically and quantitatively, for dissection by quantitative and objective experts should be reconsidered and replaced, to some extent, by a more subjective and 'wholesome' approach. It is suggested by the author that a higher degree of 'good' safety information, leading to a more complete understanding of a system under scrutiny, may be assembled if the assessment involved more social and qualitative processes to understand the underlying beliefs, culture and opinions. From experience, the author has observed how a relatively large, professionally assembled safety case, supported by a team of well trained and experienced engineers, has failed operationally due to an eventual breakdown in the 'soft' (human/culture) aspects of its construct.

7.5 Applying Qualitative Data.

This chapter has proposed and recommended that qualitative data, predominantly in the form of free text, should be used more to support safety arguments. The underpinning argument for this approach is that it befalls upon safety managers to learn the truth about a safety incident; correspondingly the safety manager should ensure that as much information as possible is made available to him/her of a proposed safety related activity so that a more systematic, insightful and 'truthful' safety decision may be made ahead of the activity.

Having established the constructive need to use qualitative data there is a requirement to understand how the qualitative information may be combined with the quantitative in a unified and coherent manner and ultimately create a synergistic output. By reviewing qualitative and subjective information along with the more well defined quantitative components the concept of true *systems engineering* is naturally approached.

7.5.1 Triangulation.

Triangulation is a term which was first used by Campbell and Fiske (1959) for describing elements of their work on psychological testing; specifically theoretical frameworks. The predominant method of triangulation used by safety managers for combining qualitative and quantitative data to create a more 'rounded' and 'complete' picture of an activity is that of complementary triangulation. Such an approach, often carried out unconsciously by managers, relies upon treating the qualitative and quantitative components of a safety

argument as predominantly separate and individual entities; they are then combined to provide a final output. Another form of triangulation which is advocated by many is that of validatory triangulation. For the provision of context and additional support to the qualitative importance of safety information within safety arguments they are both discussed below.

7.5.1.1 Complementary Triangulation.

Complementary triangulation emerges from the belief that qualitative information, often from interviews are 'just things people tell us', while 'official' statistics, as an example, are 'objectively true' (Davies *et al*, 2003, p71). Such an approach suggests that one source of information cannot be used to test or validate the other due to the consideration that they do not measure the same observation or object.

The complementary approach considers the use of qualitative information as providing additional information to both augment and test (challenge) the quantitative data which has been gathered. Supporters of the complementary approach denigrate any views that information sourced from qualitative and quantitative means may be consolidated and merged into a common entity. Fielding and Fielding (1986) claim that any merging hinges upon the false supposition that there is a common and valid theory between the information sources. One of the key observable issues with the complementary approach is the primacy given to quantitative data ahead of any qualitative data without any real strong and clear arguments.

The testing of a theory to demonstrate its validity is fundamental to its acceptance as a scientific principle or not. Any scientific theory must be capable of making predictions and such predictions being possible to be falsified. Theories that cannot produce predictions which are falsifiable may be valuable but cannot be described as scientific. It therefore also follows that no scientific theory can be shown to be true. Karl Popper introduced the concept of *falsification* to indicate his rejection of classical empiricism and the classical observationalist account of science which had evolved from it (Popper, 1963). Popper suggested that scientific theory, and human knowledge in general terms, is based predominantly upon conjecture and hypotheses, which have been generated by creative

imagination solely for the purpose of problem solving in specific environments. He postulated that no number of positive outcomes to challenges in experimental testing could confirm a scientific theory though a single counter-example may be accepted as a logical and decisive event of confirmation. Popper's description of the logical asymmetry between verification and falsifiability is core to his philosophy of science. His belief in this idea inspired him to apply falsifiability as a base criteria for identifying what is genuinely scientific and what is *pseudo-scientific* (Popper, 1963). A typical real world example, and application of the aforementioned (as pointed out by the author's supervisor), concerns the dynamics of a rugby ball and the application of Newtonian mechanics. When we deal with very small items then quantum mechanics must be applied; and when the items are very fast and very large then special relativity must be applied. Neither of the two need be applied to the rugby ball.

The reluctance to test and challenge theory is a weakness of many humans, including scientists. This weakness is both recorded and accepted by many institutions including the judicial system of England and Wales. A current Law Commission consultation paper (Emson, 2009) describes the process, and need, to test and challenge theories and expert judgements, especially in the context of forensic applications, in a competent and logical manner.

Robson (1993) and Breakwell *et al*, (1995) raise concerns with the complementary method of triangulation. Within the complementary approach, they raise the issue that researchers usually gather objective numerical data first and then *"pick and choose"* qualitative and diffused information to align with those numerical results. A typical example of such an approach would be for near miss incidents within an organisation to have risen from X to Y over a defined period of time. The complementary approach would be to ask simplistic questions to support the increase in this quantitative data set; most of the questioned would suggest answers which were plausible and which would tend to reinforce the numerical data set. In simple terms, the numerical data is accepted as real and true and that any qualitative data is seen to be merely for augmentation rather than as a tool for the testing of an hypothesis or the validation of a data set.

7.5.1.2 Validatory Triangulation.

This form of triangulation relies upon the belief that there is an amount of convergence or coincidence between the information sources. Many papers have been written which discuss the virtues of validatory triangulation and its ability to test theories by applying challenges from more than one data source as opposed to relying upon a single interrogation. Maxwell (1998) states that triangulation "*reduces the risk of systematic distortions inherent in the use of only one method*".

Given the degree of strong support for the complementary approach, and the lack of general interest in using qualitative data, one can quickly deduce that there is a need to change mindsets within the general safety community if validatory triangulation is to be seriously and consciously applied.

7.5.1.3 A Balanced Approach.

Whilst it is easy for the author to criticise the extant methodology of dealing with qualitative information, especially within his field of safety management, there are some benefits to the complementary triangulation approach. In the current world of safety management there is certainly a high degree of pressure, both in time and cost, applied to the overall topic of safety management. Managers are conscious of the need to deliver reports or investigations within tight timeframes and to a limited budget and therefore tend to follow the 'path of least resistance'. Whilst convenience and practicality are great facilitators and catalysts for a certain mechanism to be employed it falls upon those managers to use a tool which is effective and provides a truthful and complete answer. No tool should be employed simply due to its convenience.

Whilst the preceding text has identified how complementary triangulation has been used predominantly more often than validatory triangulation to support safety arguments, this preference has been driven almost wholly by the theory that quantitative and qualitative data are very distinct in content, the former being 'more objective' than the latter. It is recommended by the author that any data gathered is looked at as a source for determining the truth about a system and that whatever the format it should be used to its fullest

capacity. Both quantitative and qualitative data may be good or bad; the secret is in filtering out the bad from the good and not in pre-judging one form of data from another.

7.6 Verifying Qualitative Texts.

One of the key observations that the author has in terms of his own safety management environment is that almost all of the organisation's safety managers are sourced from engineering foundations. Whilst safety managers may head up a department, they will have been trained and evolved from an engineering background; the author himself was trained in electronic engineering and subsequently moved into weapon engineering.

A prime feature of using qualitative data is the fact that safety related information, whether in risk assessments, reports or even safety arguments should not be managed and disassembled into its component parts like a watch or radar system. Of consideration is the fact that descriptors and context for qualitative information is supplied using spoken or written words and not just numbers; we use a language. Of note is the fact that when a number is written down without any form of language to provide context (units) the number means nothing. Those who are singularly focussed upon the use of quantitative data must acknowledge the use of language in the form of prefixes, units of measure or even acronyms to convey any meaning at all.

One of the main issues with language is the fact that it is so varied, unstructured and open to so much interpretation that it is often very difficult to analyse efficiently and concisely. Quantitative data on the other hand is very easy to analyse using mathematical models or to translate into statistical reports and graphs; such information is also very quickly tested for patterns and underlying trends. Despite the vagaries of language, a transcript or few sentences written in the words of the interviewee is a more accurate method of capturing the required data and also easier to defend than a question within a quantitative questionnaire which uses someone else's words, often with a generalist approach. There is a tendency to use the 'best fit' answer to an imprecise or vague question.

Whilst language allows communication it also allows for miscommunication; both purposefully (e.g. lying) and accidentally (e.g. miss-learnt meanings for words). This

immediately raises questions relating to the true meaning of text; in simple terms, reading a text does not allow simple access to the minds of those who have spoken or written it. With this observation in mind there is the need to understand how such text may be interpreted and verified as correct, especially if it is to be used to both support and improve the safety argument or safety management of a system. In its basic form any text may be interpreted by simply engaging with the author or interviewee and simply asking them if the interpretation is correct. But if language is merely a form of spoken or written debate then the result of such another engagement would be even more debate and ambiguity.

One of the prime tools used to try to ensure that the correct interpretation of a text had been obtained in other environments has been the application of *hermeneutics*.

7.6.1 Hermeneutics.

Hermeneutics is concerned with the interpretation of text; predominantly that of the Bible and literary texts (Oxford, 1995). Its application started with the study of works such as the Bible or the Torah due to the way that such texts had been written; often they were complicated as they used parables and allegories to communicate (Wallace, *et al*, 2003). Reading and applying the 'correct' form of interpretation was one of the prime tasks of the priesthood within those early times. This requirement was therefore sub-divided into two prime areas; the first involved analysing the texts in a manner which looked beyond the superficial statements whilst the second involved the verification of what had been interpreted. In a similar manner, these two requirements are fundamental to the use and application of qualitative information to support safety management.

The first version of hermeneutics was developed by the philosopher Wilhelm Dilthey (1833 - 1911) in a bid to defend the social sciences from the analytical technique which was prevalent within the natural sciences. Throughout the twentieth century hermeneutics were wrapped up in debates over whether the approach was based upon an 'individualistic' approach or a 'positivist' approach.

Martin Heidegger (1962) offered a major and complex piece of work in 1926 (re-issued in 1962) where he raised two important issues. The first identifies that an individual's

empathetic interpretation is often 'coloured' by previous texts and interpretations in terms of our presumptions, prejudices and conjecture. Whilst this may appear as a limiting function of such an approach it is quickly seen that by reading subsequent texts the former readings may be re-interpreted again and again as part of an iterative process to achieve a more refined and (hopefully) truthful result.

The second issue raised by Heidegger relates to a paradox called the hermeneutic circle. During the act of reading the human mind breaks the text down into its component parts (sentences and words) but must reassemble those discrete components to recognise and discern what is being communicated. According to Heidegger there is a continual dialogue and reasoning (dialectical processing) being applied during an act of reading between the concepts of reductionism and holism. This behaviour manifests itself in two distinct areas; the first is a paradox in that we cannot ever understand a text without breaking it down but we must analyse it as a whole before understanding the component parts. This is classical 'chicken and egg' with each step of understanding relying logically on the state of the other. Interpretative reading may be considered therefore as a paradoxical action; to break out of the paradox there is a need for the reader to take a somewhat irrational 'leap' of subjective faith 'into' the text. Once 'within' the text, the reader, through an iterative dialectic process, may disassemble and reassemble the text until its meaning becomes more lucid and unambiguous.

Further work which built upon Heidegger's principles of applied hermeneutics were carried out by Hans-Georg Gadamer in the 1960's and Paul Ricoeur in the 1980's. Furthermore, hermeneutics were further developed and applied between 1999 and 2001 by the University of Strathclyde in its qualitative methodology for Confidential Incident Reporting and Analysis System (CIRAS), (Wallace, *et al,* 2003). The project involved qualitative safety data being decomposed and stored within a central data base; by applying a new 'Applied Hermeneutic Methodology' it was able to provide a method of reliably analysing interpretations between different interpreters. Due to the method of classifying which was used, and that textual elements were represented using numeric formations, it is suggested that the application crossed the 'qualitative - quantitative divide' (Wallace, *et al,* 2003).

Whilst this brief introduction into the subject does not delve deeply into some of the theories which are applied, it is designed to communicate to the reader, especially those who are 'hardened' quantitative safety practitioners that 'objective' outputs may be generated by applying a process, such as hermeneutics, to qualitative information. Hermeneutic methodologies may not be a complete answer to the qualitative aspects of safety information but could be used, like any other tool, to help provide a more truthful and wholesome level of safety management.

7.7 Concluding Remarks on a Qualitative Approach.

The author has tried to illustrate within this chapter how qualitative information may be used to not only augment any quantitative approach but that it should be used within its own right. The nature of the language that we use and the way that we use it not only reflect our view of the world but also give an insight into how we perceive it. Due to the personal and individualistic character of human beings we cannot yet perceive how words can ever provide the same meanings to any two individuals. This creates so many problems as can be seen in the way that safety management, both as individuals and teams, handle and manage incident reports, near misses and any other safety related text.

The predominant and extant method of learning from such reports and written words, certainly within the author's working environment, is to employ an expert such as a 'safety engineer' or 'safety manager' to decompose the material into a 'more understandable' and 'easily manipulated' format. Whilst this may seem a trivial matter on the surface, the author would suggest that there is a clue within the *more understandable* phrase; the underlying thought which is provoked here may be related to that of competence. Whilst the author is a professional engineer, trained in many fields, including safety, he struggled with the concepts of safety culture and a qualitative safety approach for many years before studying for this doctorate. A 'typical' safety engineer would probably read and decompose any text within an incident report and quickly assign causation through an engineering mindset, probably quite unconsciously. Given the pressures of cost and time such assignments are either classified relatively well within the specific areas of engineering discipline or classified as 'other' or 'human factors' if they appear to fall outside his specialised domain.

Safety experts are human; they suffer from the afflictions that normal individuals suffer from. They will not always agree with each other's views and interpretations and they will always be affected by subjective prejudices and distortions. This suggests that there is more to be learnt, possibly from the hermeneutic process, which has been adopted in other environments where the task of extracting a wholesome and 'truthful' message is judged to be important. What is becoming quite evident though as this discussion is advancing is that safety experts, both individuals and teams, predominantly from an engineering background, may need to understand not only the technical attributes of their operating environment but also grasp the implicit and explicit fundamentals of language and the culture of the operation under scrutiny.

Sentencing causation of an incident to 'human error' is not an explanation or conclusion in itself; it is merely the first step of a requirement to further investigate to another level of understanding. Such a vague and coarse descriptor conveys no message on how to stop the same incident from being repeated again; in a similar manner, the term 'mechanical failure' to explain a commercial airliner disaster does not offer any insight into how to avert another similar incident. In simple and everyday terms they can be identified as 'someone had blundered' or 'the kit broke'; neither really helps us to understand how to stop it happening again. From experience, what is quite unequivocal within the author's industry is that the safety experts will have distilled the mechanical failure down to the exact component and why it failed; the final report will often recommend improvements both at component and system levels in the absence of any such demands by the enquiring body. Again from experience, any sentencing of incidents to 'human error' will be largely left at that; there will be very little delving into more specific causes other than reviewing processes and any individual competency and training records. There is minimal use of all information, both qualitative and quantitative, at one time to produce a more complete, meaningful and 'truthful' conclusion.

7.8 A 'Systems' Overview.

As systems have become more technologically complicated and the problems within them, or the incidents which they are involved with, become more multi-disciplined then so the process of understanding becomes more difficult. Whilst such systems are being evolved

and created with a great amount of mature technical risk management, the causation of incidents is predominantly shifting towards how humans interface with them.

The term *systems engineering* deals with the orderly process of bringing a system into being and the subsequent effective and efficient operation and support of that system throughout its projected life cycle (Blanchard, 2008, p1). Systems engineering and the adoption of a 'systems' approach involves using an interdisciplinary approach and technique to allow for the creation and operation of an efficient and favourable system. A system consists of a complex combination of assets such as human beings, materials, equipment, facilities, services etc., which may be integrated in a way as to fulfil the requirements of a need. The prime objective behind applying a systems approach is to address the requirement within the context of a complete and whole entity rather than as a group of individual separate components. One of the more important views within the systems approach is the realisation that the final system performance is very much dependent not only upon the efficient and timely integration of all of the components but upon ensuring the correct and appropriate intra-relationships between them. Within the context of this thesis it may now become evident why the author considers the available qualitative information, predominantly that which concerns human interaction within a system, as being fundamental to its correct and safe functioning

Of the many disciplines considered important for the application of systems engineering is that of *human factors and safety engineering* where the human being is addressed as a major element of a system and its integration (Blanchard, 2008, p170). This discipline deals with the anthropometric (scientific study of the measurements & proportions of a human body), human sensory, physiological, and psychological factors within the system design. The safety engineering facet of the discipline considers if the system under design will be safe to operate, repair and maintain throughout its whole lifecycle. The safety design process, in a similar manner to the MoD's design cycle process discussed in chapter four, is an iterative process where various measurements (error rates, time between failures, etc.) are fed back into the design and provide a state of evolution.

7.9 Human Factors within System Safety.

It has already been established both within the preceding text of this chapter as well as within other chapters of this thesis that the development, delivery and management of a safe system relies upon integrating many and various engineering disciplines. It has also been claimed within this chapter that the topic of human factors is largely not well understood by the 'traditional' engineering practitioners. Perrow (1984) sums the interactive human interface with systems, in terms of human factors, as systems that support dynamic process involving large numbers of hardware, software and human elements that interact in many different ways. Examples of such interactive systems may be found within nuclear power generation sites, command & control centres (e.g. civilian emergency services, military operations, air traffic control centres etc.) and even in the remote controlling of UCAVs. Whilst some of these systems may be deemed as safety-critical, they rely upon the complete integration of humans, hardware, software and procedural control to deliver an efficient and safe activity. It is therefore relatively obvious, within the context of such a system, that human factors have been considered throughout the whole activity from the design phase through to the writing of operational and maintenance procedures. For such systems the overall safety integrity level which is claimed will include human factors as a component of both control and failure.

The human component was discussed in chapter six and whilst it is seen as a relatively important component of a system it is often either ignored, sentenced as 'too difficult to explore further' ('*someone blundered'*) or just left hanging in 'mid-air' under the broad and unhelpful banner of '*Human Factors*' on the occasion of an incident enquiry. Safety cases for complex systems which require a human operator predominantly consider safety from a technical perspective which is limited to addressing the hazards which could arise from technical failures alone; this is despite the fact that human error is alluded to frequently as a major contributory of accident causation within the safety case. The author considers the civil airline industry as a typical example of a highly disciplined and orderly industry with a 'good' safety record. It is only when published figures for human factor related incidents are reviewed that the enormity of the subject is fully unveiled; the CAA's Aircraft Proximity Reports for 1997 showed that 98% of incidents within UK's airspace for that year were attributable to human error (CAA, 1998).

The author would suggest, based upon his own experiences, that there is a degree of paradox present within the general safety related industries. Many incidents within the past three decades such as the '*Herald of Free Enterprise'*, '*Clapham Junction'* and '*Piper Alpha'* act as forbidding reminders of human failures within complex systems. Whilst identified as an important factor within safety critical systems, the human component is rarely considered as truly safety critical and therefore not subjected to the hazard identification, analysis and assessment regimes which prevail for the technical components.

7.10 A 'Systems' Approach for Light UAVs.

The author, upon reflecting on the preceding discussions on human factors and qualitative safety information, combined with the lack of regulatory guidance within the environment of civil light UAVs, proposes a revised safety approach which consolidates all of the components which should be addressed in the creation of a safety case for such platforms. From his experience, the author is relatively content that most, if not all, of the technical elements of an UAV platform are sufficiently explained and qualified within extant safety cases. Note that this observation is based upon the larger UAVs, almost exclusively military registered, which are operated within segregated airspace across the UK. Despite the fact that extant safety cases are technically sound the overall approach avoids the most important and fundamental component of safety, -the human component.

As stated elsewhere within this thesis, this revised approach to assembling a safety case for civil light UAVs does not tackle the most demanding of current UAV challenges which is that of 'sense and avoid'. The aim of this new type of safety case approach is to facilitate a more complete body of evidence so that safety engineers, safety managers (or regulators) may make a more accurate, relevant, and consolidated safety judgement of the whole system under scrutiny.

UAVs, in general terms, challenge many of the established methods of safety planning and safety management. It has already been established how minimal the regulatory regime is within the light civil UAV environment; combined with the fact that there is no pilot aboard, the thought processes for self preservation are possibly not vested as strongly or as emphatically as within a manned aircraft. When compared with the commercial airline and

light aircraft operating environments the level of procedural control is very much lower in the case of small and light civil UAVs. Figure 7.1 illustrates how the light civil UAV environment compares with other flying activities within the procedural and residual risk categories.

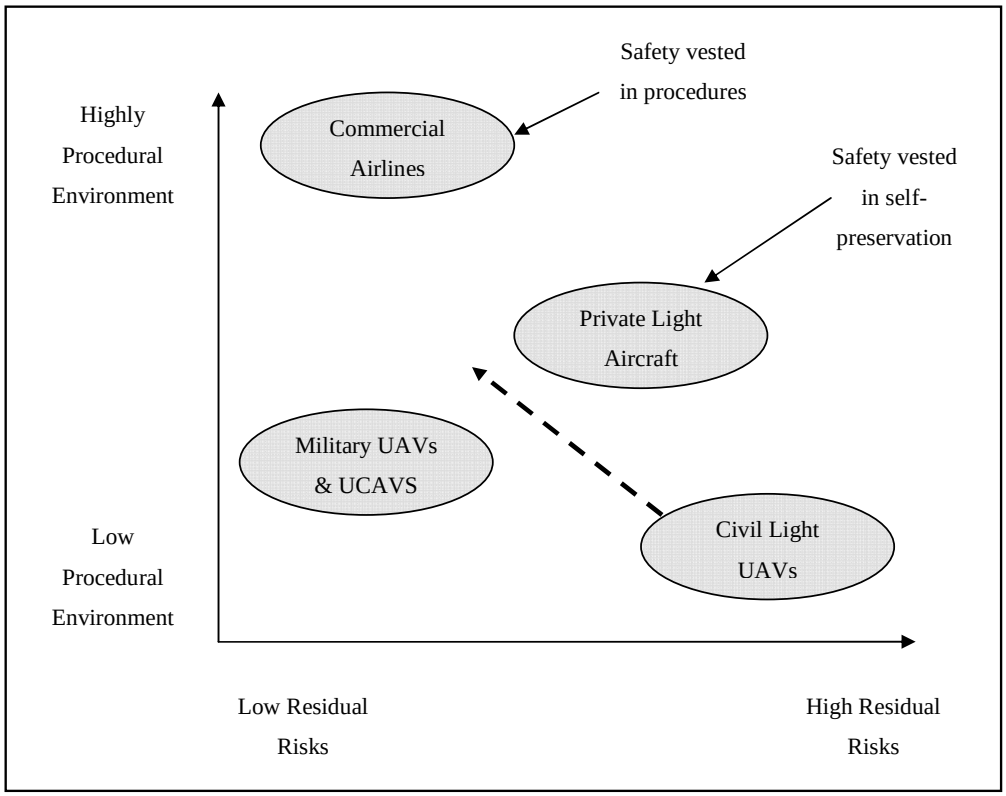


Fig 7.1 - Diagram illustrating the procedural and residual risks of various aircraft operations.

The need to include the human element, specifically the culture within an organisation has been shown as being very important in the overall scheme of safety within an operating system. By incorporating the human element with that of the technical aspects of the system the resulting output would appear to offer a much 'rounder' and complete argument of system safety. Whilst human factors engineering has been present within the manned flight environment for many decades, its use within the UAV environment is still relatively light; any human factors engineering present is predominantly focussed towards operator

training, competency and currency rather than systematically throughout the whole system. The author suggests that the system, within the context of Civil Light UAVs, should include not only the platform from a technical sense but the supporting business frame which facilitates the creation (or destruction) of a positive safety culture.

The following chapter introduces the reader to the concept of a 'Safety Case Elicitation Tool' (SCET) for Civil Light UAVs and the use of a more qualitative approach. The author proposes that some of the more expensive, time consuming and quantitative safety assessment methodologies which are prevalent within the safety 'world', may be reduced in usage for a more qualitative approach, especially when dealing with low cost, relatively low mass and low speed civilian UAVs.

CHAPTER 8

The Safety Case Elicitation Tool

8.1 Introduction.

The preceding chapters highlighted many of the deficiencies and limitations in the application and use of the typical industry model for safety cases. This chapter describes how a relatively simple guideline, for creating a safety argument, may be used for smaller and/or less complicated systems. Whilst the author believes that this approach may be developed and applied to almost any small modern system he has focussed on his experiences within the aerospace industry and that of UAVs.

The guideline itself, based upon experiences within the T&E environment, has been broken down into its component parts. Each component is listed and accompanied by both explanatory and descriptive texts to help maintain focus when being used as an elicitator for the creation of a simplified safety argument. The guideline is termed a Safety Case Elicitation Tool (SCET) and is designed to aid in the construction of a simplified safety case for light UAVs.

Much of the background leading up to the creation of the SCET is steeped in the methodology for creating safety submissions for the conduct of T&E trials on the UK's Ranges. Certainly well before the HSE suggested that major sites or hazardous activities should be underpinned by formal safety documentation (CIMAH 1984) the Air Ranges were demanding 'safety submissions' from potential users of Range facilities to demonstrate the robustness and effectiveness of any activity's control systems. The author is cognisant of the work conducted over the past decade by both himself and Rowley in attempting to document the requirements of a T&E Range specific 'safety submission'. The overarching problem in trying to create such a document was to avoid being too prescriptive whilst avoiding creating something which was so 'loose' as to provide little or no instruction.

In recent years the author has been involved with more UAV activities and has engaged with other technical experts across the company. The author is also duly cognisant of the work conducted by Ayliffe (2006) in the field of UAV flying and the checklists employed by him and his team in support of such activities at the WWUAVC. It is fair to say that the work conducted with Rowley was concerned predominantly with that of the technical abilities of the platform and the ability to terminate flight (missile and/or UAV) by using a predominantly probabilistic application. Ayliffe's checklist again focuses upon the technical and flying attributes of the UAV platform though there is some cognisance of the need to look at operator training and competences. Both of these approaches emphasise the trend which was highlighted by the author in preceding chapters where safety arguments are focussed upon the technical attributes of the system rather than including, systematically, the safety attitude and composition of the operating organisation.

As in many other industries, most practices are honed through evolution; new concepts are migrated into the standing practice as a result of new legislation or learning from an event whilst bad practices are removed, again through events such as accidents and/or significant near misses, through the application of new technology. Whilst the extant practices applied on the Ranges are relatively up to date and deemed to be more than adequate for current activities the author suggests that there is a degree of 'overkill' being applied to some activities which may be better managed by applying the SCET approach for smaller projects. To provide a degree of qualification for the SCET concept it was peer reviewed by the Air Ranges' Operations and Safety Trials Working Group (O&STWG) during July 2009. The results of this review are contained within chapter nine. The author is grateful to the working group for their time and their feedback on the tool.

8.2 The Author's Concerns and Observations.

Having been greatly involved in the development of the WWUAVC at *Parc Aberporth* the author has always had concerns over the safety assessment of those UAVs which would be operating from its airfield. Whilst many would operate with a mass greater than 150kg the potential was present for a number to be flown with masses within the Light UAV classification. Whilst the military registered platforms would be supported by safety cases driven by the relevant defence standards, the civilian platforms, especially those within the

Light UAV classification would lack a great deal of supporting evidence to argue their safety as discussed in chapter three.

Civil UAV activities have been predominantly based upon the recreational model aircraft environment; whilst the military UAV scene has developed greatly over the past decade the civil world has been quite static in terms of regulation and legislation hence the heavy reliance upon the LMA as discussed in chapter three. This observation explains the lack of specific regulatory requirements, including safety, demanded by the CAA for civil UAV operations under a mass of 150kg; such a minimal approach to safety can be explained by carefully analysing the operating environment in which such vehicles operate. Recreational model aircraft flying relies very much on 'green field' sites offered by friends, colleagues and 'friendly farmers' or, disused airfields, scattered across the countryside.

There may be occasions where model aircraft are flown alongside operational airfields but these occasions are relatively few and very highly controlled. The crucial and most important observation from such operations are the numbers of spectators present within the area at risk from the aircraft. In all of these flying scenarios the number of individuals who are within range of being struck by the aircraft, and being hurt, is quite minimal. During model aircraft demonstrations and 'air shows' there is a degree of crowd control and risk assessment but the overall number of observers (third parties) is very small compared to the number of individuals who may be at risk from a civil UAV operated over a populated area such as a town. The author suggests that the guiding mindset of an individual who has a recreational model aircraft background may not be completely aware of all of the potential hazards and risks that may be prevalent from operating a civil UAV outside the finite, and immediate, envelope of an airfield or 'green field'. The author would strongly suggest that the presiding mindset would not take cognisance of peripheral or indirect consequences; for example, an UAV crashing on a road verge and causing a car to veer into the path of another vehicle. Whilst the risk assessment may have reviewed the immediate risks to the platform and those parties within its near and intimate environment it may be limited, to some degree, by unconscious assumptions and ignorance of insight, implanted by many years of operating in a very benign, insulated and 'safe-by-default' environment. This mindset would be worsened, in the context of risk identification and

subsequent risk management, by the fact that the individual was participating in an activity which they considered to be fun and recreational; who in their right mind ever considers the full safety implication and documents the results of any assessment when actively pursuing their favourite pastime or hobby?

Civil UAVs, once established as a viable platform for various activities (e.g. data gathering, surveillance, etc.), will quickly need a more rigorous, yet easily populated, risk identification process which will require an assessment to be carried out of the whole system. The system, in its fullest sense, not only includes the hardware and software, but includes the human operator and the series of instructions and Human-Machine-Interface (HMI) procedures which are fundamental to safety. Civil UAVs may fly alongside, and even over, sites which could generate fatal events if the vehicle was to suffer a catastrophic failure. Sensitive locations such as petro-chemical plants, schools, hospitals, major roadways and even open gatherings of people (e.g. football stadiums, demonstrations) would suffer greatly if impacted upon by an UAV with a mass of up to 150kg.

Whilst neither of the first two mass categorised *Small Aircraft* classifications identified by the CAA (< 7kg & 7kg - 20kg) refer to any airworthiness certification, the third class begins to address airworthiness issues in design, manufacture and indeed flight testing. The overall presiding limitation for UAVs within this third category is that governed by their kinetic energy limits (Haddon & Whittaker, 2002) where both the speed and mass of the vehicles are limited in order to minimise damage and/or harm in the event of crash. The limitations imposed are such that the maximum combined operating mass and speed cannot permit the UAV's kinetic energy to exceed 95kJ given a free-fall condition from 400ft above the surface.

What is not addressed in any of these three categories is a formal requirement to clearly demonstrate engineering or flying competence in the planning, manufacture or operation of the air vehicle. Whilst researching the creation of a safety case for the initial T&E component the author self realised (akin to an epiphany!) that safety cases exclusively remain reliable only if the assumptions and/or conditions by which they were originally constructed are effectively implemented. One of the key determinants in maintaining a safe

operating environment, and complying with the requirements specified within the safety case, is that of the competence and underlying mindset of the personnel managing and operating the system in question.

The CAA's *Small Aircraft* policy, and its underpinning support by the LMA, is well suited for recreational activities such as model aircraft flying, but is now demonstrating its unsuitability and lack of rigour for a new era of commercial small aircraft flying in the guise of civil small and light UAVs. Recreational model aircraft flying is predominantly low volume and low technology and occurs within environments which are very low in terms of risk consequence and likelihood; the activity usually takes place away from large numbers of the general public and at a very low level of frequency compared to what commercial civil UAVs may be subjected to. It is now time to take the environment forward into a new era.

8.3 The Decision to Include Human Factors and Safety Attitude in the SCET.

In 1940 it was calculated that approximately 70% of all aircraft accidents were attributable to 'human error' or, more formally, human factors (CAA, 2002b). A further review by the International Air Transport Association (IATA) in the mid 1970's found that there had been no reduction in the human factor component in accident statistics (CAA, 2002b). Further studies in 1986 and 1996 again identified human factors as the major contributory factor to aircraft incidents (CAA, 2002b).

The topic of safety culture was discussed at length in chapter six; within the context of aviation it is widely accepted that the indigenous culture of an operation has a marked effect upon its safety statistics. Eiff (1998), within the context of aviation safety, corroborates what was highlighted in chapter 6, and suggests that "A safety culture exists only within an organisation where each individual employee, regardless of their position, assumes an active role in error prevention"; he also stresses that "Safety cultures do not spring to life simply at the declaration of corporate leaders".

The culture of an organisation is better judged by what is done rather than what is said; many organisations highlight very elaborate *mission statements* regarding safety, but this

may not reflect what is in place and is practised at the working levels. The CAA (CAA, 2002b) acknowledge the importance of a positive safety culture in CAP 715; they also acknowledge how difficult it is to measure the attitudes of an organisation's workforce. One of its recommended methods of measuring safety culture is to use a HSE developed questionnaire. This questionnaire has been used by the author, to some extent, to create the SCET; this allows the people component of the system under scrutiny to be analysed and reviewed to gain an additional insight into its safe operation.

Whilst UAV systems do not carry an onboard pilot, operational experience is already demonstrating that human error is presenting a hazard to their operation (McCarley & Wickens, 2005). Given the generally reported figures for pilot error in manned flight it is not surprising to see relatively high figures for pilot error in unmanned systems; with this in mind, it is foreseen that any ground based UAV pilot or controller will soon be replaced by a fully autonomous flight control and command system. Despite minimising human errors in the pilot function the degree of human intervention will remain relatively constant when it comes to maintaining and repairing such unmanned systems.

Tvaryanas *et al,* (2005) and the United States' Defense Science Board (2004), have reported that the accident rate for UAVs is higher than that of manned aircraft; the loss of operational unmanned military surveillance aircraft exceeds the loss of manned combat aircraft by a factor of 10 (Johnson, 2003). Johnson does acknowledge that some of these losses were directly attributable to the danger of the missions, but, human error was viewed as a contributing factor due to the lack of real-time situational information and fewer fault recovery options which were available to the pilot. Tvaryanas *et al,* (2005) and Williams (2004) found that a higher proportion of accidents in US Army UAVs suggested that system reliability may be emerging as a greater threat to UAVs than it currently is within the manned aircraft environment. This pattern may serve to increase the importance of maintenance, especially given the limited sub-system redundancies, within smaller UAV platforms.

8.4 Societal Concerns.

Formatted: Bullets and Numbering

No systems approach of safety, especially within the field of civil operated UAVs, would be complete without a brief discussion on the social aspects of the operation; these include 'soft' issues such as those of societal interactions and any concerns raised by the operation. Much of today's developments in technology happens in some isolation and results in developments which do not address our values structure or how it will fit within it. It may be argued that the interaction between technology and societal values can play an important role in the success or the failure of a new technology. The fact that the US supersonic transport programme was curtailed in 1971 as a direct result of environmental lobbying of Congress is a clear example of such an interaction. Whilst the interaction of technology within any values structure cannot always be predicted, any early due considerations, or even sampling of opinions, may help to support and/or direct its wider application and acceptance.

Risk is very much an emotive issue which is open to much debate and the many uncertainties of individual perceptions. UAVs in a similar manner to motor vehicles have the ability to change our lives considerably but many of the hurdles that lie ahead of the industry will be formed by public opinion and their reactions to any UAV incidents, whether fatal or not. When the motor vehicle commenced its life at the turn of the 20th century society demanded the use of a flag bearer to warn the general public that a vehicle was approaching; any incidents caused by the new 'contraption' were topical news at an international level. As society has grown to rely heavily on the motor vehicle's presence then so has society's perception and acceptance of risks caused by motor vehicles decreased and increased respectively. Hundreds of deaths per year on the roads of the UK alone are now accepted as part of the modern way of living; will this attitude to deaths caused by UAV incidents become the norm in a few decades? The author is not suggesting that there is an answer to the question but raises it as a topic for thought. Achieving timely and resilient social acceptance of UAV operations is paramount to the industry both in economic and cultural terms. If the industry fails to demonstrate cognisance of, or acts upon, society's concerns, misconceptions and power of influence then the road to an effective and resilient civilian UAV operation will be arduous, convoluted and painful.

Such an approach may only be delivered through the application of a methodical and iterative process of safety development utilising true systems engineering techniques.

8.5 Forming the Safety Case Elicitation Tool.

The SCET has been created by amalgamating the author's experiences of T&E related safety cases with that of his research into safety cases and safety culture; the latter bringing with it a revised approach of assessing an organisation's in-built safety regime. By applying a model based upon one of the HSE's core safety climate tools (HSE, 2001b) and amalgamating it with a bespoke engineering focussed safety assessment, the author has created a safety case elicitation tool which is largely qualitative in its approach. A degree of quantitative analysis is required to support the safety critical component of flight termination; this is driven very much by the requirement to correlate with operational safety targets mandated by both regulatory regimes and the H&SE.

The overall concept is very much based upon established and well honed practices within the commercial airline world. CAP 715 (CAA, 2002b) and CAP 718 (see bibliography) are clear examples of how seriously and important the commercial airline industry takes human factors within the maintenance and inspection of their platforms. Whilst an identical level of application could be ostensibly applied to the world of larger UAVs both civil and military, it would not be realistic in the case of small, light and relatively cheaper civil UAVs. The SCET is designed for the smaller, and budget limited organisations, which may decide to operate within the small and light civil UAV market. The argument which comes to the surface from the previous statement is one of trading safety against cost, the application of the ALARP concept again. Whilst the author is aware of the need to further qualify the statement he believes that to pursue the argument in detail would require another lengthy and in-depth thesis. The statement is made here to merely acknowledge the fact that further work may be required to qualify the 'cost versus effort' concept of the SCET.

8.6 The Safety Case Elicitation Tool.

By following the various descriptors against each of the following component headings a predominantly qualitative safety case may be constructed by a potential UAV operator. The author has included a brief explanation, in italics, with each question. The explanation, including references to the literature reviews, also includes exemplar answers and provides the reader with an insight into the reasoning and theory behind it.

The aim of this tool (in the form of a questionnaire) is to provide sufficient information to a regulator, or safety supervisor (such as a Range), that the system under scrutiny has been designed and manufactured with sufficient due diligence and has applied established safety and professional engineering practices. The tool also provides information relating to the safety and engineering management practices within the operating organisation, giving an insight into its underlying engineering and safety culture.

The questions provide the regulatory/supervisory body with a critical insight into the organisation's attitude and maturity towards safety in general. The questions are to be answered truthfully and in a descriptive 'free text' manner; the information gathered allows an appropriate and suitable degree of control and supervision to be applied to the activity. Whilst the questionnaire may be completed in isolation by the organisation under scrutiny the regulatory/supervisory body may decide to further investigate the organisation, through a further interview. The SCET questionnaire, and the answers put forward by the organisation, may be used as cues for such interviews.

The SCET attempts to include many of the people and organisational issues which are not covered in the 'traditional' quantitatively focussed safety case approach. The resulting model is acknowledged, within the aerospace T&E Air Ranges community, as the first ever 'systems' approach to a consolidated safety case for UAVs.

8.6.1 Introduction to the Organisation.

- Introduce and describe the organisation which has overall responsibility for the proposed UAV activities.

- Include the organisation's formal company trading name, address and business details.
- Provide the organisation's relevant contact details.
- Introduce and describe the organisation's history and background within the context of UAV construction and operating.

This first question offers both parties (the UAV operator and the regulatory/supervisory body) with an opportunity to identify with the foundational aspects of the proposed operation. Formal details of the company allow a degree of background checking to be carried out in relation to financial buoyancy, reputation within industry and even to understand if it is involved in any degree of incident or inquiry related to UAV operations. Contact details of relevant personnel allow the regulatory/supervisory party to gain an understanding and confidence in the technical and managerial staff of the company.

From a Safety Case perspective this first question begins to create a relationship between the two parties. It basically takes the first few steps in creating a Preliminary Safety Argument (4.11) and conveying the organisation's attitudes towards safety in general. This relationship, especially trust and honesty, will become very important if the regulatory/supervisory party is to gain a true insight into the proposed UAV operation.

8.6.2 Previous Experience.

- Describe the organisation's experience in the field of UAVs.
- Has this experience been as a prime contractor, sub-contractor or as a sole provider of an UAV system?
- Include details of previous projects including project names, dates and the role(s) that the organisation participated within.
- Have these experiences and skills been retained within the organisation?

Experience of previous UAV activities will have a major impact on the levels of scrutiny that the regulatory/supervisory body will need to apply. Learning from past experiences is cited by Lord Cullen as an important factor if an organisation is to improve its safety attitude (6.6, 6.7). A good safety culture (6.8) relies heavily upon commitment by senior

management, especially when they are involved in learning from past experiences. Senior management must be involved in the feedback, monitoring and analysis routes if 'learning from experience' is to be taken seriously.

It is extremely difficult to create an effective and robust safety case as a singular event within the lifecycle of any system; it is an iterative and very much an evolutionary process which relies very much on maturation through feeding back lessons learnt from preceding work. This form of learning from experience is referenced in chapter 4 (4.11).

One of the more important, yet intangible elements, that arises from working with individuals who have a degree of experience in the field is that of confidence. Confidence starts to grow, and any initial barriers are slowly dropped, as, through the use of bespoke languages, subconscious relationships begin.

Formatted: Bullets and Numbering

8.6.3 Introduction to the UAV System.

- Introduce and describe the UAV system from a high level perspective.
- Describe the system's purpose and mission intent; e.g. surveillance, target or detection platform.
- Describe the system's command and control concept; e.g. autonomous guidance or human operator/pilot control.
- Describe the system's history and concept of requirement if appropriate; include any evolutionary systems (prototypes) which may provide additional context and support to the overall safety argument.
- Has the system been certified to any standard? (E.g. Certificate of Airworthiness, Permit to Fly, UK CAA Type Certificate, Large Model Aircraft, etc.)
- To which countries standards has the certification been issued? Provide details of any form of registration.
- What regulatory guidance has been applied or has been referred to during the designing and manufacturing of the system?
- Has the system been flown elsewhere? Has flight been refused or been terminated by another organisation?

- Were the results of these flights satisfactory? Please provide information on such flights, including any safety issues within the system as a whole?

These questions simply build upon the preceding ones, delving deeper into not only the UAV system itself but the organisation behind it. By starting to tease out the UAV's mission criteria in conjunction with its command and control concept the regulatory/supervisory body will quickly form its own views on the risk strategy which has been used by the designers and constructors. The risk strategy used may have been completely obscured by the eagerness or enthusiasm of the technical team to attain a novel answer to a pressing requirement. The author has observed on numerous occasions how technical teams 'solution-ise' and get too involved with the hard engineering principles of an answer to the detriment of the holistic requirement, especially those fundamentals related to cost and safety.

Delving into the system's history, especially any evolutionary phases, enters directly into the requirement for an evolving lifecycle for safety argument development (4.10). Whilst the answers to these series of questions may be predominantly qualitative they will provide context to the overall presentation (4.8.3). A degree of quantitative evidence (4.8.1, 4.8.2) by deterministic and/or probabilistic means will help to convey the structure of the argument. The regulatory/supervisory body, from such information, will begin to build a model in their minds of the competency (6.10.5) within the organisation and the degree of risk acceptance that the business is operating at. Risk averse organisations will behave in a much more reserved manner when dealing with most forms of risk; alternatively, 'risk keen' or 'risk ignorant' organisations will demonstrate a cavalier type attitude to risk.

Designing, constructing and operating an UAV to any standard will be considered by the regulatory/supervisory body as demonstrating a certain degree of organisational maturity and the application of due diligence from a management perspective (6.10.1). With a positive response to this question the UAV company would provide a clear indication that its management is aware of it's legal requirements; this ties in to the attributes of a good safety culture (6.8), competence (6.10.5) and effective communications (6.12).

When combined these answers will demonstrate the UAV company's holistic view towards safety as a system. The company will ultimately demonstrate its maturity if it allows observations and/or learning from other UAV related activities to be openly discussed. A typical example response may look like the following;

> *The Archimedes II UAV flew its maiden flight at Tonopah Test Range in the Nevada Desert during May 2007. After completing two half-hour flights it was sent out on a three hour mission. On this third flight it suffered a catastrophic failure and crashed after one and a half hours. The cause of the failure was deduced by the chief engineer to have been caused by overheating of the fuel cells within the wings which led to failure of the epoxy glued main bearers. The overheating was caused by the excessive climatic temperature of the desert and the excessive current drain demanded by the payload.*
>
> *The Archimedes III, which is planned to be operated at Lochinver airfield will not be operated for any periods longer than one hour and will not be subjected to any climatic temperatures akin to those experienced in Nevada; this statement is supported by a formal Meteorological Office report. Additionally, the UAV will not operate any payloads during these flights.*

Formatted: Bullets and Numbering

8.6.4 System Technical Overview.

- Describe the system's overarching functionality.
- What are the physical dimensions of the system?
- Describe the method by which the system is launched. (E.g. spring assisted launcher, 'Bungee' launcher, Jet Assisted Take-Off (JATO), runway, etc.)
- Describe the method by which the system is recovered. (E.g. parachute recovery to land or sea, runway, sacrificial target (no recovery), etc.)
- What are the flight performance parameters of the system? This information must include data on all phases of flight including the recovery and/or flight termination phase. (E.g. for parachute based recovery systems the rate of descent must be stated.) Typical parameters included within this category include, for example,

maximum altitude, climb speeds, susceptibility to adverse weather such as static and/or icing conditions, etc.

- What are the flight characteristics of the system? This information must include data upon all phases of flight including the recovery and/or flight termination phase. (E.g. stalling speeds, general stability, roll rate, pitch rate, typical turning radius, etc.)

These questions relate entirely to the technical capabilities of the UAV system. The information will predominantly be communicated through free text (4.9.1) and will be almost entirely of a qualitative nature augmented by some quantitative analysis from a recognised authority. The quantitative aspects will offer evidence to support statements on fundamentals such as risks to third parties from inadvertent or flawed launches. A typical example may include a probabilistic (4.8.2) assessment of the likelihood of a JATO exploding on the launch area rather than burning in a controlled manner or, for one JATO in a two JATO launch system, to initiate whilst the other does not. The probabilistic risk assessment for this latter scenario would focus upon the probability of an asymmetric launch and the hazards, including lateral throw of debris, from such an event. A typical example response may look like the following;

> *The Archimedes III will be launched from a Stealth IV spring assisted launcher into a head wind of no more than 40 knots. A full failure effects analysis by the launcher Design Authority, certified by our Chief Engineer, states that in the event of a catastrophic failure, all components and associated debris will be contained within a circular hazard area, of radius 65m, centred on the launcher's single steer-able jockey wheel.*

Such a response would convey to the regulatory/supervisory body that an appropriate level of management engagement (Chief Engineer) had occurred in the safety assessment process (6.10.1). The fact that previous work had been demanded by the UAV operator upon the supplier of the launcher also suggests that a Safety Management Plan (4.11) with associated levels of hazard analysis and risk management (4.12.2) had been initiated. A

similar type of response for the recovery activity would also convey a similar type of message to the regulatory/supervisory team.

The author would consider that the information on flight performance and any operational limitations could be conveyed using a simple table. In order to communicate the various types of mitigation used to minimise any transgressions of design limitations the company may consider simply adding another column into the table. The following example illustrates;

Flight Performance Parameters	*Maximum*	*Minimum*	*Mitigation / Control Measures*
Operating Temperature	*+ 35º*	*- 15º*	*Met forecast prior to flight. Flight profile pre-planned by pilot and peer reviewed by Chief Engineer.*
Recovery Parachute Rate of Descent	*800ft/min*	*1,000ft/min*	*Met forecast prior to flight. Flight profile pre-planned by pilot and reviewed by Chief Engineer.*
Stall speeds	*160knots @ 5,000ft*	*120knots @ 1,000ft*	*Flight profile pre-planned by pilot and reviewed by Chief Engineer. Use of current and competent pilot.*

The use of terms such as competency and currency by the UAV company displays cognisance of established requirements for airmanship. The use of a company senior engineer who holds a trusted position in management also demonstrates company ownership at senior level (6.8, 6.10 and 6.10.2).

Formatted: Bullets and Numbering

8.6.5 Operational Environment.

- What is the maximum wind speed, including any cross-wind component, or sea state, for the system during launching and recovery?
- Are there any limitations imposed upon the system from an environmental perspective? (E.g. static, precipitation, lightning, visibility, saline environments, etc.)
- How have these environmental limitations been ascertained? Please provide evidence to support this response.

Continuing from the preceding answers these questions expose how the company have reviewed their operation in a wider sense, i.e. with a systems strategy (7.8, 7.10). Not only does the SCET focus upon the technical task of preparation, operation and recovery from an engineering perspective, it is concerned with understanding any environmental limitations that may be imposed.

Static or thunder risks are well known to be a threat if explosives or pyrotechnics are to be handled or operated by personnel. High cross-winds or tailwinds may make take-off and/or landing dangerous or virtually impossible to control; excessive winds may invalidate any pre-planned debris hazard area or operational safety trace. A typical example response may look like the following;

> *The Archimedes III will be launched from a Stealth IV spring assisted launcher into a head wind of no more than 40 knots; the maximum deviation in heading from the wind component will be ± 15º. Recovery to the sea surface, using the onboard recovery parachute system, will be conducted in tailwinds of no more than 30 knots (max gust).*
>
> *For flights where recovery to sea is anticipated a saline sacrificial plug is to be fitted to the main fuselage section. When immersed in sea water this plug will deteriorate over a period of two to three hours (depending upon sea state) and will eventually allow water to fill the fuselage. This functionality is designed to sink the UAV and therefore minimise risk to marine surface traffic; without such a device the UAV would float with a relatively neutral degree of buoyancy, just below the surface of the water.*
>
> *If the UAV is to be flown in airspace which is likely to contain manned aircraft the vehicle is to be configured in its 'conspicuous dress'. The UAV's fuselage is to be painted in Day-Glo orange and will have an approved organic dye added to the fuel to increase conspicuity whilst under powered flight. A full environmental assessment and hazardous material handling procedure is supplied for the dye.*

The aforementioned paragraphs suggest that the company is aligned with the need to be cognisant of other parties who may be under a degree of risk from the UAV operation. The UAV company would be seen by the regulatory/supervisory body as having a good understanding of the principles of risk management (4.12) and in the application of risk reduction in accordance with the HSE's ALARP argument (4.12.2.5).

Formatted: Bullets and Numbering

8.6.6 Concept of Design.

- What approach or design strategy has been taken by the organisation?
- Have any formal 'Systems Engineering' concepts been used in the construction of the system? If so then please provide a degree of evidence to support this response.
- What form of professional competence in engineering has been used in the design of the system? Please provide evidence to support this response. (E.g. Chartered or Incorporated Engineers; formal qualifications in aeronautics, engineering, structures, etc.)
- What quality assurance status does the organisation hold? (E.g. ISO 9001, etc.) Please provide evidence to support this response.
- Does the organisation hold any formal approvals as a 'Design Organisation'? Please provide evidence to support this response.
- Does the organisation hold any formal approvals as a 'Production Organisation' or a 'Maintenance Organisation'? Please provide evidence to support this response.
- What standards and/or principles have been applied to the system (including hardware, firmware and software) during design, build and test? This information must include data upon all aspects of the system including design drawings, prototyping, assembly and testing.
- What process is used by the organisation to ensure that design requirements, including health and safety related requirements, are effectively communicated to any third party supplier?

The use of a well structured design strategy communicates that the UAV has been evolved from first principles in an evolutionary manner and with a staged approach (4.11). In parallel with the design lifecycle the safety case should have been evolved in a similar

manner (4.11, Fig. 4.4). A typical example of a staged approach to creating an evolutionary safety case is used by the MoD (4.10, 4.11).

The application of a 'Systems Engineering' approach demands that the problem, and its complexities, are fully understood (1.6); having decomposed the problem the engineer may adopt a suitable 'systems' approach to generate an optimal solution. Such an approach would include the generation of a Systems Engineering Management Plan and an holistic approach throughout. Systems Engineering is about being cognisant of the whole entity, both from within the system under scrutiny and also how it will interact with the external environment. By delivering a diligent 'systems' focussed report on the UAV the regulatory/supervisory body gain more confidence that the company is professional in it's engineering and safety related thoughts processes and actions.

A 'Systems' approach would be reflected in the competence and skills of the assembled team supporting the UAV. For example the Chief Engineer may be formally qualified in Aeronautical Engineering or Electronic Engineering and would possibly have had subsequent training and experience in various other fields to create a very rounded and professional individual who is cognisant of the wider issues that may affect the UAV. He/She would most certainly be a member of a number of professional bodies and hold Chartered Engineer status or be working towards it. The absence of such an individual from the project would not preclude the operation but would simply allow the regulatory/supervisory party to pay more diligence to some of the engineering management aspects of the aircraft.

The Chief Engineer may be supported by specialist engineers and scientists who may be members of other professional bodies and hold experience demanded by the sub-systems employed. Typical examples may include explosive experience for work upon pyrotechnics within the aircraft systems (e.g. JATO motors, parachute reef line cutters, etc.).

Periodic design reviews, chaired by the Chief Engineer, allows a clearly auditable trail to be displayed to any auditor. Such an approach not only allows hazards and issues to be tracked but also documents how they have been resolved. Third parties, such as sub-

contractors, may be requested to attend and deliver formal responses; such attendance helps with communication and risk acceptance (6.11, 6.12).

Formatted: Bullets and Numbering

8.6.7 Organisational Safety Management.

- Describe the organisation's safety management system. Include a reporting structure which clearly identifies responsibilities for health, safety & environmental issues.
- How does the organisation manage health, safety and environmental management across its whole structure? (E.g. monthly/weekly briefings, newsletters, etc.) Please provide evidence to support this response.
- How do staff within the UAV system's supporting team have any health, safety and environmental related information communicated to them, especially if they are away from their home site? Please provide evidence to support this response.
- Has the organisation ever been subjected to an internal or external health, safety and environmental review? Please provide details of any findings or observations.
- Has the organisation ever been requested to cease operations, by the Health & Safety Executive, on grounds of health, safety or environmental reasons? If so, then please provide details of the event(s).

This question focuses upon the Safety Management Plan (4.11), which in itself should sit under the Systems Engineering Management Plan. Whilst the author uses these quite specific terms for these management plans, they be termed differently in these rather smaller UAV companies. What is more important than the terminology is the information contained within the submission. For very small companies such management plans may be in the form of a few sides of paper but the company must convey the engineering and safety approach taken for the UAV in a manner which satisfies the regulatory/supervisory body.

Communication is probably the key to maintaining a safe system of work. In the author's experience many health, safety and environmental issues are forgotten or are simply not communicated due to a lack of established process. Most projects, facilities and activities start with good intentions and issue copious amounts of safety related information such as newsletters and 'kick-off briefs'. Very quickly, possibly due to other commitments,

forgetfulness, etc. the initial surge of safety information becomes stale and outdated. For effective safety management there is a need for team leaders and senior managers to maintain a weekly or monthly briefing on safety related matters (6.8, 6.10.1). Of benefit, is the intertwining of safety related briefings with more business or technically orientated meetings or briefings; safety should not be briefed in isolation but should be seen as an important element seeping through all of the company's activities. Teams when working at remote sites may not have access to e-mails or newsletters but the team leader should demonstrate a degree of initiative to maintain the team's indigenous safety culture. This is very important when third parties are involved in the operation. A typical response to this question may look like the following;

> *The Archimedes III UAV team, deployed to Lochinver for January's series of test flights, will consist of five individuals, including a Chief Engineer, from the company. They will be supported on an ad-hoc basis by two contract staff from the Meteorological Office. All Health, Safety & Environmental matters during the deployment shall be channelled through the Chief Engineer. Daily operational briefings, including safety briefs, will be conducted each morning at 08:30hrs in the hotel's conference room; an end of week 'wash-up' will commence at lunchtime (13:00hrs) each Friday. All staff are to be present for all briefings.*

For activities which rely heavily upon a third party, such as a boat which is recovering an UAV from the sea, there is a need for the UAV company to be explicit in its explanation of how the risks are being managed and by whom. The following example helps to illustrate this;

> *It is intended to recover the Archimedes III into the sea on Thursday's sortie. A final call on the ability to fly and recover will be made during Thursday's morning brief. The Chief Engineer's call to allow the sortie to be flown will be based upon the serviceable state of the aircraft, a formal meteorological brief and a discussion with the skipper of 'Blue Oyster II'. The final decision on suitability of sea state for recovery of the UAV lies unequivocally with the skipper. The skipper and his crew are to be briefed on the potential hazards of the UAV and its payloads on*

Wednesday afternoon; during this briefing the crew will sign all necessary risk assessment paperwork.

8.6.8 Configuration and Engineering Control.

- How are any modifications to the state of the system recorded? Is a database or index used to control build standards? (E.g. Master Records Index, Configuration Control Processes, etc.)
- What competencies does the organisation have in developing and implementing engineering changes include hardware and software?
- What engineering management systems are in place to ensure that all engineering change requests are appropriately and effectively managed?
- How do technicians and engineers raise observations and concerns into the engineering management system? Please provide evidence.

These questions are relatively self evident and relate to good engineering practices for configuration control. Configuration control is paramount if the UAV company is to demonstrate tangible safety management processes. In the case of an incident there must be a clearly auditable trail back to the configuration which was flown.

The author would not expect to see an overbearing and complicated configuration control process for a relatively small aircraft; a logbook for the aircraft which contained entries for any engineering activities carried out upon it would be sufficient. All entries would be signed by the engineer responsible whilst a periodic check and countersignature pre-flight and/or weekly by the Chief Engineer would add credibility to the procedure. Such an approach would convey an appropriate degree of risk management (4.12.2) and the presence of both good engineering standards and safety culture (6.8).

8.6.9 Materials and Construction.

Formatted: Bullets and Numbering

- What materials have been used in the construction of the aircraft?
- Why and how have these materials been used for their specific roles?

- What methods and standards have been used in the design verification and construct assurance of the aircraft? (E.g. Critical Design Review, etc.) Please provide evidence.
- What is the structural safety factor for the aircraft? Have any analysis been conducted on the stresses imposed during all stages of flight? Please provide evidence.
- How have any identified limitations, in design or test, been recorded and communicated within the design, maintenance and operational teams? (E.g. maximum flight hours of the aircraft, material fatigue issues, non-destructive testing application, etc.) Please provide evidence.
- What controls are present to ensure that correct procedures, parts and tools are used in the construct and maintenance of the system?
- What measures have been taken to ensure that all personnel are appropriately trained and have been deemed suitably competent to work on the system?
- What measures have been taken to ensure that all personnel behaviours and attitudes are safe and appropriate for working on the system?

Again these questions explore the fundamental engineering principles being applied to the aircraft. A simple and cheap UAV may rely upon a pre-manufactured (COTS) recreational airframe. Reference to manufacturer's data sheets and specifications may give a degree of supporting information whilst additional data may be gathered from evolutionary tests in relatively benign conditions (e.g. climatic chambers, wind tunnels, etc.). This type of foundational work carried out would align with established engineering and safety management best practices (4.11, 4.12.22)

The latter series of questions starts to delve into some of the more systemic behaviours and attitudes within the team. The last question is open ended with the intent that it offers the UAV company an opportunity to create a foundation to work from. For a relatively large company there may be an opportunity to include results of psychometric analysis or behaviour mapping which may have been used as part of a recruitment technique or in-company process safety mapping. For relatively small companies the response may be quite a personal piece of text explaining the backgrounds of the individuals involved with

the project and how they behave in general terms. A typical example response from a small company may look like this;

> *UAVs 'R' Us is a small company which consists of me, the Chief Engineer, Ron Baxter; a Mechanical Engineer, Dave Watkins and a Pilot, Mike Rogers. I have known both Dave and Mike for over ten years as we all worked at Sony Aerospace on the Moon-shot V project.*
>
> *Neither Ron nor I have ever been in trouble with the police though Dave has been caught speeding twice in the last four years. We regularly meet up socially for a drink and to discuss the UAV project. We do not drink whilst we are working on, or flying, the aircraft.*
>
> *As the project's Chief Engineer, and a long standing Chartered Engineer, I am fully aware of the requirements to behave professionally, diligently and with cognisance to others who may be affected by my actions. Our experience and training in the aerospace industry has a great effect upon our attitudes and behaviours towards safety, especially when dealing with an aircraft. We ensure that we are all fine for work by having a cup of tea together as a team every afternoon; by doing this we learn about each others problems both with the aircraft and at home. All of the designing, building and flying of the aircraft has been done as a team effort; any issues which have arisen have also been dealt with as a team. This way we can discuss all of the options available to us and review each others work.*

8.6.10 Hazardous Materials.

- Please provide a list of all potentially hazardous materials that are contained within the system. (E.g. Man Made Fibres (e.g. Kevlar, fibreglass, carbon fibre, etc.), Batteries (e.g. Lithium, Cadmium, etc.), pyrotechnics (e.g. parachute reef line cutters, flight termination cutting charges, etc.)).
- Have these hazardous materials been risk assessed? Please provide evidence.
- Have these hazardous materials been assessed for their environmental impact? Please provide evidence.

Identifying hazardous materials forms the first few steps in managing and estimating any risks within the system (4.12.2, 4.12.2.1). A basic brainstorming exercise will allow a list of hazardous materials to be generated. The following example is typically what the author would envisage;

Hazard Location	*Hazard Source*	*Specific Hazard*	*Mitigation / Control Measures*
UAV fuel tanks	*Fuel*	*Fire, Explosive Atmosphere, Skin Irritant*	*No naked lights, Fuel at launch site only, Use of competent persons, Ensure adequate ventilation,*
UAV Pyrotechnics	*Minor Pyros*	*Fire, explosive dust, detonation.*	*Ensure appropriate training, Use self contained items,*
UAV fuselage & wings	*Man Made Fibres (MMF)*	*Inhalation of MMF dust*	*Appropriate Personal Protective Equipment (PPE), Training*

Having identified the source of the hazard a method of mitigating and/or controlling it may also be identified; any hazards which require further attention before sentencing may be set aside as appropriate. This list of hazardous materials may also be used to base the environmental hazard assessment upon.

Formatted: Bullets and Numbering

8.6.11 Command & Control System.

- What type of Command & Control link is used by the system? (E.g. Radio Frequency, Laser, etc.) Please provide details.
- What frequency and data encoding does the system operate on? Are the frequencies registered with the national authority for spectrum management? Please provide details. (E.g. Bandwidth, Emission/Modulation type (e.g. AM/FM/FSK/TDM, etc.)
- Is there technical redundancy built into the command and control system? (e.g. 'Hot' standby transceivers, etc.)
- What antennas are used within the system? (E.g. directional, omni-directional, etc.)
- Is the performance of the command and control link aligned with the expectations of the flight/mission requirements? Will the link be operating at the limits of its operational budget? Please provide details.

- Is the system reliant on an on-board autopilot? Please provide details and an overview of its operation.
- Does the system respond to de-faulted and pre-set commands at the loss of command link? (E.g. enters a loiter phase, climbs and holds, deploys a parachute, etc.) Please provide details.
- What form of resilience and interference testing has been conducted on the system? (E.g. Electro-Magnetic Interference, Mutual Compatibility with other sub-systems, etc.) Please provide details.

These series of questions relate to the ability of the UAV pilot to effectively and safely control the aircraft during flight. The regulatory/supervisory body will be interested in the theoretical calculations and/or empirical testing that may have been carried out to ensure that control of the aircraft is guaranteed for the duration of the flight. For smaller UAV systems which have been based upon a recreational model aircraft there may be a requirement to demonstrate the effective coverage of the command link at the boundaries of the proposed flight plan.

Cognisance should also be shown to other users of the frequency in use and the ability of one system to interfere with another. In the case of a command link failure does the UAV default to a state of level flight until command is recovered or it runs out of fuel? Simple compatibility checks and/or the use of a frequency band which is protected may be considered by the regulatory/supervisory body as an example of due diligence and acceptable risk management.

Formatted: Bullets and Numbering

8.6.12 Propulsion System.

- What form of power-plant does the aircraft rely upon? (E.g. electric motor, turbo-jet, turbo-fan, normally aspirated piston engine, etc.) Give details of performance characteristics.
- Provide details of how the power-plant is tested before initial installation and before flight.
- Provide details of how maintenance is carried out on the propulsion system.

- What form of fuel/energy supply does the aircraft require? (E.g. battery, hydrogen fuel-cells, etc.)
- Is the power-plant designed and built as a bespoke item for the aircraft? Give details of the power-plant's capability and limitations.
- Provide details of how the power-plant and fuel/energy supply has been designed and proven to minimise/avoid fuel starvation and/or interruptions? (E.g. Anti-Vibration Fuel and Power Connectors, Carburettor Icing, Fuel Line Cavitations, etc.)
- How is the power-plant connected to the rotor or propeller? For rotor driven aircraft please describe the complete drive system including any clutch and/or disengagement mechanisms.
- Can the power-plant be re-started during flight? Please provide details.
- What mechanism is used to communicate to the operator how much flight endurance is remaining? What and how is endurance data gathered on-board and displayed to the operator?

These questions continue to explore the fundamental engineering principles and level of good engineering practice being applied to the aircraft. The initial questions will allow the regulatory/supervisory body to make judgements on the type of competency and experience required to support and effectively manage the platform described. For example, jet powered UAVs are relatively specialised and require regular inspection of the turbine blades whilst normally aspirated power plants may suffer from increased wear and/or vibration. Subsequently, maintenance regimes will differ as will the level of competency required.

The fuel/energy supply feeds heavily into the degree of hazards present and subsequent risk assessment and management techniques used. Energy cells such as batteries may require venting of toxic gases and may quickly cause a fire if inappropriately handled. The questions relating to fuel starvations or energy supply interruptions will indicate if the system has been designed and engineered as a holistic entity; the preliminary design for the aircraft should identify how the specification meets the requirements of the customer. Reverse engineering some overlooked requirements may be costly or simply unworkable.

The question relating to any clutch or disengagement system for rotary wing powered UAVs relates to the ability of the aircraft to attain auto-rotation, thereby minimising the energy at ground impact, despite suffering a catastrophic power plant failure. Understanding how much endurance remains within the aircraft is paramount when embarking on relatively lengthy flights; flying into head winds and at lower altitudes, especially when carrying payloads, may completely ruin any theoretical calculations.

Formatted: Bullets and Numbering

8.6.13 Performance Limitations.

- What is the Maximum All-Up-Mass of the aircraft for flight? Please provide details of these calculations.
- What is the maximum speed attainable for the aircraft within the environmental limitations specified? This figure should take into account the maximum permissible tailwind for energy calculations in accordance with the UK Civil Aviation Authority's policy on Civil Light UAVs (Maximum energy of 95kJ).
- Are there any regulatory or supervisory limitations imposed on the aircraft? Please provide details if applicable.
- How has any flight or operational limitations been communicated to the operator? Please provide details if applicable.

Mass and velocity information will allow the regulatory/supervisory body to calculate the potential kinetic energy exhibited at impact with the ground (3.12.1). This calculation allows the regulatory/supervisory body to fully align itself with extant CAA Light UAV policies for civil operated UAVs.

Additional information on the physical layout and shape of the aircraft may allow the regulatory/supervisory body to veer and haul CAA guidance on a subjective basis based upon aerodynamic drag (bluff body characteristics, table 3.3) and/or any built-in arrestor systems (e.g. parachute deployment).

8.6.14 Safety Overview.

- How has safety been designed and engineered into the system? Please provide a predominantly textual narrative of how safety has been approached for the whole system.
- Explain how any major sub-system, both Commercial-Off-The-Shelf and bespoke, have been integrated into the overall system. Please provide details of any 'bench-testing' and/or 'de-risking' which have been carried out.
- The use of simple diagrams may be useful to support the aforementioned points.

The answers to these questions should reflect good safety management and safety engineering practice as stated in 4.10 and 4.11. Some responses will automatically jump into a 'hard engineering' analysis; such a response should encourage the regulatory/supervisory body to engage further and ask for additional information on how the 'softer' and people aspects (5.9) of safety management was implemented. Training, experience and competency should play an important part here (5.9).

Typical responses should include reference to safety arrangements (6.10.3) such as the use of safety committees, safety management plans and systems as well as identifying any industry safety models which may have been used. A degree of independence within design reviews or safety reviews would add further credence to the answer. Smaller companies may decide to ask the regulatory/supervisory body to allocate an independent reviewer to validate any observations.

As stated in previous questions, there is a clear need for the safety aspects to have been treated holistically and to have been 'grown' from inception to delivery.

8.6.15 Safety Assumptions and/or Boundary Conditions.

- Please provide details of any assumptions and/or boundary conditions used in the design, manufacture or operation of the system? (E.g. Maximum altitude, Maximum rate of turn, Minimum temperature, etc.)

- How have these assumptions and/or boundary conditions been carried through the life of the system? (E.g. Design Reviews, Documented within operating manuals, etc.)
- Who has agreed and authorised the design and technical reviews? Please provide details. (E.g. Chief Engineer, Chartered Engineer, Engineering Consultant, etc.)

Systems Engineering demands that boundaries are consciously understood at the initial stages of providing a solution to a problem (1.6). Very often the problem area, and therefore the boundaries of the solution, are incorrectly defined and quickly lead to problems such as 'requirement creep', extended costs, a solution which is a 'jack-of-all-trades and master of none' and of course, suffering from an inappropriate safety case. By ensuring that the boundaries and assumptions are well defined at the initial stage the project may be designed and evolved in its engineering and safety related aspects concurrently and in a co-ordinated manner (4.10, 4.11).

The use of a Chief Engineer and/or individuals with professional standing convey the fact that the UAV is being managed and owned by senior managers within the company (6.8, 6.10). Recognised and accredited professional bodies, through interview and revision of formal qualifications and experience, provide much needed assurances of the type of individual and behaviours required at certain levels. For example, prospective Chartered Engineers are required to hold first degrees, hold a position of responsibility and to have gained some form of experience in an engineering management position, prior to being accepted by the Engineering Council as a Chartered Engineer. Whilst such accreditation may not guarantee that the individual will always act with professional integrity, the fact remains that professional status requires a considerable amount of time and effort to achieve and subsequently sets a default mindset which is honourable. It should also be noted that professional status, in some trades, brings with it accountability for personal actions by law.

8.6.16 Safety Traces / Safety Boundaries.

- Please provide details of any surface area and/or any volume of airspace which requires delineation and segregation in order to manage risk exposure. This will

take the form of a scale drawing and will be formally authorised by the appropriate system design authority. (E.g. Launch Safety Trace for energetic launchers (e.g. Jet-Assisted-Take-Off, 'Bungee Launchers', Compressed Gas Launchers, etc.), Recovery Areas (E.g. Parachute Recovery to Land, Snag Wire Recovery, etc.)).

- All Safety Traces / Safety Boundaries must include information on all flight parameters. (E.g. Operating Height, Speed, Track, Attitude, etc.)
- All Safety Traces / Safety Boundaries must include a full description of the methodology used to identify the area, or volume of airspace, at risk.
- All Safety Traces / Safety Boundaries which incorporate wind allowances must include simple calculations to enable computation of mean wind to the maximum applicable height of the safety trace.

Safety information such as scale drawings must be authenticated by the design authority of the subject system. The regulatory/supervisory body may require sight of the base assumptions (boundary conditions) as well as the mathematical calculations which support the safety trace information. The assumptions will list typical variables which have been included within the safety calculations; for example an UAV launch launched by a JATO system will need to take into account the possibility of the JATO detonating rather than operating in the correct manner. For such an event the safety trace may need to preclude all personnel within a radius of many hundreds of metres from the launch site. For platforms which are launched by less energetic methods such as hand launching there may be a safety trace of a few metres and the use of an exclusion zone for other personnel within a few tens of metres to minimise slips, trips and falls.

Parachute recovery may at first seem like a an easy method of recovering a target and minimising any damage from impact; additionally it may help to satisfy the requirement to limit the kinetic energy at impact to within the CAA's limit (3.12.1). Key to such a safety argument is the probability calculated for the parachute not opening meaning that impact with the ground would be at a much greater energy level; could this prove fatal? When the parachute opens correctly the direction and strength of the wind may take the UAV out of the prescribed operating area and create a hazard greater than were it to have failed and

plummeted to the ground within it. Such occurrences could include an UAV drifting on a parachute onto a major road, into a busy shopping centre or even a school playground.

The safety trace information will be quantitative as far as diagrams and scale drawings are concerned but will rely heavily on a qualitative narrative to explain and support the methodology and assumptions included within it.

Formatted: Bullets and Numbering

8.6.17 Flight Termination System.

- Is the UAV system fitted with a Flight Termination System? If so, please provide details of its operation. Please ensure that the details supplied identify the method by which flight is terminated. (E.g. is flight terminated by driving control surfaces or by initiating an explosive device?
- Does the Flight Termination System rely upon the prime operational 'Command & Control' link or is it a completely independent system? Please provide details.
- Does the Flight Termination System default to a 'safe' or 'flight terminated' state if the Command & Control link is lost? Please provide details.
- Please provide a simple safety analysis of the Flight Termination System, including a quantitative (probabilistic) approach, to system integrity. This analysis must demonstrate any critical causal paths and methods employed for mitigation and reliability assurance.
- How has the Flight Termination System been tested for reliability? Have any engineering or safety standards been used in the system's design and/or manufacture? Please provide evidence.
- Please provide details of any reliability testing and/or instances where the system has failed to operate. These details should include results of any design reviews, reliability/suitability testing such as electromagnetic interference, environmental testing and system testing following integration into the aircraft.

The author believes that any UAV which uses a Flight Termination System (FTS) must communicate the effectiveness and robustness of the termination process to the regulatory/supervisory body in a predominantly quantitative manner. Whilst a qualitative narrative will be required to explain the assumptions and conditions behind the safety

argument the regulatory/supervisory body may require an ultimate quantitative figure to ensure alignment with the HSE's tolerability framework. The author, from experience, suggests that FTS systems are predominantly used, in the true sense of flight termination, on platforms which operate at relatively medium to high altitudes and with relatively high speeds. The potential energy available from such an UAV impacting with the ground is relatively large and is probably orders of magnitude greater than those levels specified by the CAA.

The regulatory/supervisory body may require the quantitative analysis to take the form of an FTA which may decompose the final event of a terminate action (e.g. explosive charge initiation, servo actuation of control services, etc.) down through the various components, including the command link.

The qualitative component of the safety argument would communicate the various logic states of the FTA and relate them to the various individual components which were operational within the UAV at that point in time.

Formatted: Bullets and Numbering

8.6.18 Hazard Register and Failure Modes.

- Please provide a list, or log, of all hazards and failure modes within the whole system and describe how they have been mitigated, or controlled, to an appropriate state.
- This list/log will include not only items which are based on the pre-dominant, 'hard engineering' sub-systems (e.g. aircraft, command console, etc.) but the whole operation as a system (e.g. impact of weather change whilst aircraft is airborne, recovery of aircraft components following a crash, etc.)
- Please identify within the list/log any hazards which are mitigated, or controlled, by procedure.
- This list/log will clearly identify first, second and even third order hazards so that all parties are aware of roles and responsibilities; such a list/log will clearly identify who owns any particular hazard or risk.
- Please describe the process on how the list/log was assembled. Who participated in the exercise?

- Has the list/log been independently verified? Please provide details.
- Has the list/log been revisited as the project has matured? Have 'lessons learnt' from incidents and/or trials been fed into the list/log? Please provide evidence.

A simple hazard register may be created in a similar manner to the hazardous materials log described within 8.6.10. The hazard register augments the hazardous materials log and communicates to the regulatory/supervisory body that an effective degree of hazard identification for the whole operation has occurred within the project (4.11). A typical response from a small UAV company may look like the following;

Hazard Location	*Hazard Source*	*Specific Hazard*	*Mitigation / Control Measures*
UAV aircraft.	*Fuel.*	*Fire and Explosion from lightning or high static.*	*Preclude operations on fully assembled aircraft during thunderstorms. Earthing systems.*
UAV aircraft.	*Impact with public property.*	*Destruction of property, bodily harm or death.*	*All flights conducted by competent and current UAV pilot.*
UAV Launcher Unit.	*Stored energy in launch springs.*	*Strike by inadvertent release of bogie causing bodily harm or death.*	*Use cordoned area & safety key. Do not leave charged system unsupervised.*
UAV aircraft.	*Parachute ejection system.*	*Facial or limb strike by parachute ejector cover when working on live system pre-launch.*	*Safety pins to be removed during pre-launch checks. Use of trained and competent launch crew. Warning signs on fuselage.*

Smaller and simpler UAV project teams may not have conducted a formal HAZOP exercise (4.12.2.1) but will have considered listing the predominant risks in a table following a 'brainstorming' exercise. The hazards identified should encompass all potential hazards that may risk the safety of the operation; these will include hard engineering issues, people issues as well the environment of operation.

Formatted: Bullets and Numbering

8.6.19 Residual risks.

- Please list all residual hazards and failure modes inherent within the complete system.

- It is essential that any outstanding and/or residual risks are given the required level of focus to ensure that they remain within the identified boundaries. This approach also minimises any opportunity for an independent safety assessor to erroneously believe that all identified system hazards have been effectively neutralised through the control and mitigation process.

The ability of an UAV project team to highlight and disclose the residual hazards within their system shows both maturity and cognisance to other parties that may be affected. Many of the residual items may be discussed with the regulatory/supervisory body who may offer guidance and support on various methods that may be used to mitigate and/or limit the consequences and likelihood of an event occurring. In the author's experience it may be requested by the regulatory/supervisory for the UAV to be operated in a relatively benign environment prior to being allowed to operate in a 'riskier' environment.

Formatted: Bullets and Numbering

8.6.20 Environmental Information.

- What environmental assessment has been conducted on the complete system?
- What impact will the system have upon its operating environment? Sufficient information must be included to demonstrate that an effective and consolidated environmental impact assessment has been conducted.
- What environmental research and/or risk assessments have been conducted to identify any environmental issues? (E.g. fuel spillages, fire risks, noise contamination, man-made fibre contamination, etc.)
- What instructions and (emergency) procedures are in place to manage, control and mitigate any environmental occurrences?
- How has the support/operational team been briefed on instigating those procedures? Please provide evidence.
- Do the environmental risk assessments deal with any social impact of operating the system in the vicinity of the general public? (E.g. how noisy is the system? Could it become a nuisance to third parties? etc). Such information must demonstrate the application of due diligence, and cognisance, to third parties who may be within the periphery of the operation. (E.g. Noise during launch, Exhaust fumes, etc.)

It should be noted that for any flights scheduled to be flown over the sea, or within littoral environments, specific requirements are placed upon the operator of the UAV and the owner/operator (if applicable) of the sea area (e.g. T&E Ranges). Any article(s) which may be deposited into the sea, regardless of any intent to recover to land, requires a full materials list of the system to be provided to the Environmental Agency, or licensed authority acting on its behalf, (e.g. Range Operator). The materials list allows the authority to ensure compliance with the requirements of the Scottish Environmental Protection Agency (SEPA) and/or the Food & Environmental Protection Act (FEPA), as appropriate.

These series of questions focus specifically upon the environmental impact of the UAV operation on the flora, fauna and human components which may be affected by the activity. A typical response may identify that the noise from the power plant is irritating rather than too loud; control measures to help minimise complaints from the public may suggest that no engine runs are to be conducted before 09:00hrs and after 17:00hrs.

If the UAV activity demands that hydrocarbon based fuels are to be used for the power plant then fuel stores may require the appropriate degree of bunding to ensure that storage leaks are minimised and that a designated area is used for aircraft fuelling. The latter may demand the use of drip trays and for emergency spill kits to be made available.

Whilst the whole operation must be supported by the appropriate risk and hazardous substance assessments, there is an overriding requirement for emergency procedures to be at hand to ensure that any occurrences, which have the potential to impact upon the environment, are effectively dealt with.

8.6.21 Training, Competence and Responsibilities for Health and Safety.

- How are the managers and workforce within your organisation made aware of their responsibilities for health and safety? How does your organisation ensure that those individuals fully understand the health and safety risks associated with their roles and tasks?
- How does the organisation ensure that the health and safety related instructions and procedures used are appropriate for the level of understanding that the staff may

have in that area? How are the principles of the risks and control measures effectively communicated to those staff?

- How does the organisation allow any individuals to feed back any issues or uncertainties regarding health and/or safety to the organisation's controlling mind?
- How does the organisation demonstrate a clear understanding of those aspects of the tasks which are critical to safety?
- How are individuals within your organisation consulted to establish their foundational and developmental training needs? These training needs relate to any health, safety and/or technical requirements of the organisation.
- Please identify any competence gaps within your organisation, e.g. technical, safety, managerial, flying, etc. By identifying any competence requirements the supervising authority may work with your organisation to overcome them and to assign the appropriate degree of support and supervision.

These series of questions relate the understanding of safety from within the UAV project to the regulatory/supervisory body. This is a qualitative assessment and relies heavily upon the competency, training and experience of the regulatory/supervisory body to tease-out and understand the depth of skills embedded within the UAV organisation (6.13.1).

Manager and workforce awareness and attitude towards a positive safety culture are affected greatly by the level of communication within the organisation (6.12). For larger companies, the regulatory/supervisory body may explicitly require related information on both the company as a whole and from the UAV project team due to the prevalence of sub-cultures within larger organisations (6.11). Effective communications allow positive safety arrangements (6.10.3) to be created across the whole organisation including management safety meetings and safety management plans.

The competency and experience profiles of key individuals such as Designers, Chief Engineers, Lead Engineers, Supervisors and Pilots, when supplied to the regulatory/supervisory body, will convey the UAV organisation's abilities in a qualitative way. Note that formal training in general health and safety may be weak in some

organisations (6.10.5) and therefore there is a clear need to understand what the standards are within the UAV company.

8.6.22 Employment Security and Satisfaction.

- How secure do you consider your organisation's future? (There is no requirement to state any financial or confidential business information here.)
- How important to your organisation's future is this activity? What are the implications (if any) of slippages to your planned timeline?
- What is the typical staff turn-over rate in your part of the organisation? Have any of your team members recently left or joined your team; if so, why?
- What impact do you consider that job security has on safety within your organisation?
- Does this UAV activity involve any repetitive or boring tasks to be conducted by any members of your team?
- What mitigations are in place to minimise, or highlight, any departure from procedure? Please provide details.
- How does your organisation challenge and motivate its staff?
- How does the organisation measure job satisfaction within its staff? What does it do with the results?

Adverse reactions from work related pressure may affect a manager's ability to operate efficiently and safely (6.10.4). The whole UAV team may be under some form of pressure to deliver a successful series of flights; these pressures will be somewhat different for a senior manager that it would be for a team member like a technician. The pressures will also vary considerably if the team is a small and rather personal unit rather than a part of a major company. Small companies may have personal contributions of money at stake; houses may have been mortgaged or money may have been borrowed to enable the activity to take place. Such personal risks may bring with them a degree of risk taking in order to reduce costly timelines or to fulfil promises made to others. Larger companies may use peer pressure to greatly influence the decision making process that a senior manager may take in tackling a problem. The regulatory/supervisory body would seek to understand how

important the UAV project is to the team and to understand how the activities fit into a larger activity or business opportunity.

Regulators and supervisors, from experience, understand that it is very difficult to try to identify and formally record every activity that may be carried out on an UAV system to allow it to be constructed, operated and maintained in a formal manner. There are always opportunities for issues or faults to be raised which have not had an instruction written for them; it is on these occasions that the indigenous and positive safety culture of the team will be relied upon. Any variations from, or vagueness within, the written procedures should be instantly raised with the Chief Engineer and dealt with appropriately. Upon the reporting of such instances the team may be offered a team reward to both support the safe and professional attitude and to motivate.

8.6.23 Work Related Pressure.

- How often within your organisation is safety relegated due to financial and/or operational pressures?
- Does your organisation consider that processes may need to be accelerated or changed, on occasions, in order to deliver an important operational requirement? If so, then how is this done?
- Is there sufficient staff available to enable tasks to be completed without undue pressure or excessive overtime? As a percentage, or effective man-hours, what is the typical overtime level for the team involved with this planned activity?
- Do the supervisors and staff within the team feel comfortable that flying operations could be halted on safety grounds despite high operational and delivery pressures? Provide a degree of evidence to support this response; e.g. company policy, operational briefings, personal e-mail exchanges, etc.

These questions explore in more depth many of the issues raised in the preceding questions. However these questions are less subtle and demand some quite candid answers on the UAV company's behaviours. A degree of cross-checking with previous questions may be used by the regulatory/supervisory body to help unveil the organisation's true attitude towards, and understanding of, safety. Fatigue, through excessive hours of work, has been

shown to be a major contributor to air accidents, especially within the military; sight of any policies or work rosters may provide sufficient information on manning in support of any operations.

8.6.24 Safety Related Organisational Communication.

- How do individuals, including supervisors and managers, communicate any concerns and issues upwards through the management chain to the controlling mind of the organisation? Please provide evidence.
- How are contractors and support staff communicated with? Are there any 'full loop' checks in place to ensure that information is communicated appropriately? Please provide evidence.
- What mechanisms are in place to ensure that appropriate information is exchanged at shift handover; e.g. in support of day and night operations, or in support of long endurance operations, etc.
- Do the current staffing levels within the organisation contribute to effective health and safety management?
- How does your organisation ensure that health and safety is taken seriously by all members of staff and that it is not merely an 'overhead' to protect the management?
- How does your organisation ensure that information relating to accidents, incidents or any unplanned event is communicated to the relevant and appropriate staff? Please provide evidence.

Periodic briefings (e.g. daily, weekly, etc.) by the management and supervisors help communicate business and operational agendas; safety should be entwined within such briefings and not 'bolted on' as a 'must have' or 'need to do'. Such briefings should be conducted in an informal, or at worse, a semi-formal manner, so that the environment is less intimidating for the feedback from the team.

In the interests of a holistic attitude towards safety, any third parties such as support contractors should be included in the periodic briefs. If there are commercial issues to be discussed then these may be taken outside the briefings if they constitute no threat of safety to others.

The issue of handover instructions from one operational crew to another has been cited many times in recent years as a major contribution to incidents which have resulted in personal injury and death; recent related examples that the author has cited in this thesis is the BP Texas City incident of 2005 (1.2) and the Piper Alpha oil platform incident of 1988 (4.4). Long endurance flights of UAVs may require handovers of both pilots and engineers, including ground crew; the regulatory/supervisory body may require sight of pre-planned briefings to accommodate such handovers.

8.6.25 Accident, Incident and Near-Miss Management.

- What training and competences are in place within your organisation to allow accidents, incidents and/or near-misses to be effectively analysed?
- How does your organisation identify true root causation; are some investigations classified as 'human error'? Please provide evidence.
- Does your organisation consider management and policy influences as important as engineering and human factors in investigations? Provide a degree of evidence to support this response.
- How are accidents, incidents and near-misses reported within your organisation? Please provide evidence.
- How does your organisation hold individuals accountable for their actions and/or inactions? Please provide evidence.
- How is the information on any accident, incident or near-miss communicated within the organisation? Please provide evidence.
- Is any feedback, in the guise of reports or briefings, given to the staff who were involved in the accident, incident or near-miss? Provide a degree of evidence to support this response.

Fault and/or accident investigation is well structured within the manned aircraft environment; it is imperative that the same issues are dealt with in a similar manner within the unmanned environment, especially if the root causes are to be determined and fed back into the operation to minimise recurrences. As the civil light UAV market is still within its infancy the industry must take relatively cautious and professional steps forward as it gains public interest. To be shown as an uncaring, unconscious and amateur company will not

bode well for public or even industry acceptance. Specialist courses are available to support companies with a need to understand accident causation; the regulatory/supervisory body may draw conclusions based upon the absence or presence of suitable experience and/or training.

It was highlighted in the research on safety culture how commitment to safety by senior management and feedback on issues (6.8) were seen as positive attributes of a good safety culture. An open and honest attitude to incident reporting within the team, combined with appropriate root cause analysis training, will deliver good opportunities to understand true root causation. For smaller UAV companies the ability to sit down as a team and discuss all of the components involved with an occurrence may be shown as an example of good practice, especially if notes are made and lessons learnt. From the author's experiences one of the greatest hurdles to overcome in any analysis of an occurrence is the actual realisation that a degree of investigation is required; so often an incident or occurrence is sentenced as a 'mishap' or 'human error' and is quickly ignored and/or forgotten.

8.6.26 Adherence to Instructions and Procedures.

- Does your organisation consider that some procedures and/or instructions can be changed to allow a task to be completed more efficiently? If so, then give some examples on how and why this was done.
- How often do staff, or teams, breach an instruction and/or procedures to deliver an operational requirement or complete a task? If so, then please give some examples and provide information on how such occurrences are minimised.
- How are extant instructions and/or procedures by-passed or re-engineered? Do some managers and/or supervisors have the authority to implement such deviations? Is so, then how and why?
- What procedures and/or mechanisms are in place to allow staff to communicate to managers that health and safety instructions and/or procedures have been breached?
- How does the organisation ensure that a positive safety attitude is promoted? Provide a degree of evidence to support this response.

These last series of questions allow the regulatory/supervisory body to further explore, in a qualitative manner, the UAV company's maturity towards real-time operational and safety related issues. If the instructions and/or risk assessments have been written in isolation, without a degree of realism or experience, then the information contained within may not be appropriate or efficient for managing the task. It is upon such occasions that engineers and technicians deviate to overcome a real-world problem without due consideration for any formal assessment of risk; the 'coal face' operator gets too involved in completing the immediate task. These questions not only challenge how the organisation minimises such occurrences but asks them, implicitly, if they are cognisant that such issues may occur within the UAV's project team. A relatively candid reply of "we have no incidents where our team don't stick to procedures" would probably start to make the regulatory/supervisory body suspect that the dynamics of the team were not optimal for a positive safety culture. Honest answers, including examples of failures and/or breaches, combined with lessons learnt exercises, would certainly indicate that a good safety culture and honest relationship was present.

Whilst blatant breaches of safety and gross incompetence may have to be dealt with in a very stringent manner, less serious events may be dealt with as a learning exercise which may foster and encourage open incident reporting. Information collected from such events may be used constructively as leading indicators and hopefully give sufficient warning before a major mishap occurs.

CHAPTER 9

Guidance, Validation & Discussion

9.1 Guidance on Completing the SCET.

The author has erred on the side of caution in constructing guidance for completing the SCET. The fundamental principle of creating a safety argument for a system under scrutiny is that of allowing as much pertinent information as possible to be presented by the system's owner, designer and/or operator.

One of the dangers which may have resulted if a robust and lengthy guideline was created for SCET users could have been a relatively rigid model; such a model may have limited the amount and type of information which should have been presented and may also have introduced a fundamental bias or change in mindset. Such a mindset could effectively undermine the objectivity of the exercise and even affect the independency of the supervisory/regulatory body. If this approach had been adopted then the guideline would have become far too restrictive, onerous and prescriptive.

Another more simplistic form of guideline could have been written in a form akin to a 'tick-box' though the constructiveness and objectivity of completing such an exercise would have been extremely dubious. The author believes that the use of the SCET by any UAV organisation should not be in complete isolation and that the supervisory/regulatory body should remain open to communication and offer direction as necessary. For example such direction may include, as a function of platform complexity, a limit on word count, references to extant organisational or regulatory documentation, etc. It is reiterated that a safety case is designed to communicate a safety argument to another party and that for effective communication to take place all interactions should be two-way.

Whilst the SCET within this paper includes example responses, they are included for contextual and academic purposes; these examples are not to be included if the SCET is issued for a real and genuine purpose of elicitating a safety argument.

9.2 First Level Review of the SCET by the O&STWG.

The Operations and Safety Trials Working Group (O&STWG) is a body of SMEs, from within QinetiQ's Air Centre, which meets quarterly to discuss safety and operational matters. It consists of senior safety, operational and technical managers from across the four Air Ranges and the UK's Combined Aerial Target Systems (CATS). In order to provide the reader with an insight into the body's qualifications, experience and professional status details of its competence is included in Appendix S. The author also believes that such a rich pedigree provides much needed credibility to this thesis, especially as it is based upon operations predominantly conducted within a very specialised field and by a very few specialised individuals.

The working group was presented with the background for the thesis and given an overview of the three prime areas which have been investigated; the concept of developing a safety case structure for the civil light UAV environment, the use of a more qualitative approach to safety and the focus upon the human (people) element of organisations. Whilst comments were raised during the presentation, the majority of discussion took place at the end.

The largest observation which struck the author was how those present were predominantly split into two general groups; the first being quite vocal and voicing concerns and comments which were wholly driven by their engineering (and quantitative) backgrounds. The second group were more pensive and thoughtful; probably reflecting deeper on what was being offered as a change in procedure and protocol; change being the key descriptor! The author believes that the first group were acting virtually on a reflex action; many of the questions which were voiced were very specific and very much driven by the extant methodologies applied to extant safety cases within the Ranges environment. What was interesting was how the first (vocal) group quickly became subdued as the second group started to explore the concepts through question, debate and open reflection.

Three of those individuals present fell outside the two generalised groups; they had been heavily involved in the *Synergy* project and were aware of the wider influences of people within the engineering safety and operational safety environment. Two of the three have

just completed Masters level education in Safety Engineering and Health, Safety & Environmental Management; the third is approaching his final year in Defence Systems Engineering; the author believes that they are very much aware, and cognisant, of the concepts which were presented to them in the workshop.

Once the initial flurry of questions and discussions had subsided, the author begun questioning their thoughts and comments on the concepts presented. Quite clearly, having taken time to carefully highlight some of the key conditions (minimal regulatory advice for civil light UAVs, importance of qualitative data and the high degree of human error within accidents and incidents) which underpinned the investigations, the whole group started engaging and discussing the concepts. A number of observations and issues were identified in the ensuing engagement; they are listed, in no particular order, below.

- The SCET concept could work but only if the regulatory body (CAA) was content with its use. This thought is driven by the fact that the safety community is reliant upon a regulatory, and or legal framework, to work within. Despite the fact that the extant controls and compliance framework is minimal for civil light UAVs, the idea of adopting a revised (and even safer and tighter) regime, was seen by the working group as something that the regulator must agree to.
- The idea that the SCET concept could be used by the T&E Ranges to create more rounded and 'wholesome' safety arguments for any small UAVs (either military or civilian) was agreed as acceptable. Notwithstanding the aforementioned view on regulatory adoption, the body believed that the final safety case would offer much more of an insight into the operating company's state of health. It would be more difficult for them to hide behind numbers and lie.
- The idea of reviewing qualitative data, as well as focussing on the culture related information, raised concerns regarding the competencies of the safety managers. Whilst some of the working group had received an introductory overview in human factors, this was believed to be merely a 'taste' of what the topic involved. The idea of using people related information to gather a greater insight into an organisation's ability to plan, build and operate a safer product was received positively, but this was tempered by the fact that the challenging or regulating authority would require

a better understanding of what could be unveiled by adopting such an approach. This observation relating to the competency of the regulatory/supervisory body is fundamental to the effective use of the SCET.

- Related to the preceding observation was the concept that whilst the current method of reviewing a safety case for an activity, or a system, was carried out by a single 'Trials Safety Manager', the SCET may require a body of individuals to review the safety argument. Such a body need not be overly large, but could vary between two and maybe five individuals with specialist knowledge covering safety, systems and human factors engineering. The body could be increased and decreased in size as a direct function of the complexity, and/or the number of specialisms, covered by the system under scrutiny.

9.3 Validation of the SCET.

The author tested the SCET on three extant and fully operational UAV systems which had been operated on the UK's T&E Ranges within the previous 12 months. These systems included;

- A military UAV built and operated by a well established international defence company on behalf of the UK MoD.
- A civil UAV which was built by a well established defence company, operated and maintained as an aerial target by QinetiQ.
- An UAV designed and operated by Cranfield University as part of a joint project between a major international defence company and a number of academic partner institutions.

Collectively the systems covered an extensive variety of technical disciplines, regulatory demands and organisational structures; such a variety provided a high degree of confidence that the SCET was indeed veritable across a wide application. Due to the sensitive commercial and security natures of the systems reviewed, the author cannot discuss specific elements of his findings; however, some brief and subjective observations are included in the following text. A qualitative validation of the SCET driven safety cases revealed a high degree of confidence that all pertinent safety and operational related information had been included.

The following table identifies the author's observations and findings when comparisons were drawn between the SCET approach to constructing a safety argument and the more traditional, goal-based and quantitative approach.

Matters covered within both approaches	Matters covered within the traditional safety case	Matters covered within the SCET
Quantitative safety figures.	Overall quantitative figure highlighting gross risk to public from complete system.	Quantitative figure of safety system or command control sub-system failure.
Overall system technical description.	Some degree of dilution within the technical description.	Greater granularity of system technical description.
Operational description	Some degree of dilution within the operational description.	Greater granularity of system operational description.
	Cursory information on design and manufacture; heavy reliance on quoting standards.	Focus on engineering design & manufacture competence; including standards and people.
Maintenance & Repair regime.	No depth of how maintenance and repair is managed and/or delivered.	Greater amount of information supplied regarding maintenance and repair.
Competence of engineering staff.	Dilution of competence requirements.	Greater focus on competence of engineering staff.
Competence of pilot/operator.	Dilution of competence requirements.	Greater focus on competence of pilot/operator.
		Focus on organisational safety, culture & drivers.
	Reliance on hierarchical command of responsibility.	Focus on individual & team responsibilities.
	No focus on operating environment. Work related pressure categorised and managed under European working-time directive.	Focus upon operating environment including employment security and work related pressure.

Table 9.1 – Comparison between SCET and goal-based safety cases.

The left hand column of the table identifies those elements of the UAV systems which were covered by both the traditional and SCET approaches to safety case development. The

middle column lists those elements which were covered by the traditional safety case approach, but were not included in the SCET approach. The right hand column identifies those elements which were covered by the SCET approach but were not seen to be addressed within the traditional approach.

The overarching conclusion from the analysis is that the SCET, through being more prescriptive and direct, demands much more detail of the sub-systems. This may merely be a function of the three reviewed safety cases but may also be an emergent property that the SCET has; the SCET is purposefully designed for the UAV industry and this brief qualitative analysis certainly provides evidence that it is targeting the correct sub-system areas. It should be reiterated that the detail is largely qualitative in nature and does not contain numerous amounts of numerical data to 'back-up' or justify relatively weak statements of activity. The only intensively numerical data is focussed upon the platform's flight termination and control systems; this is predominantly to allow comparisons to be made with published regulatory risk criteria.

The author was already aware that any questions related to the softer and wider issues of an organisation such as work pressure, working environment, competency of support staff and organisational culture would not be readily observed within the traditional goal-based safety case approach. Whilst this observation may hold true for the direct and explicit questioning related to the softer issues, it was alarming to see that competence and 'professional trust' was a strong influence in an informal and implicit manner, especially in the context of safety. Of particular note was the specific example where an UAV system, which had been designed by an University, had been subjected to far less scrutiny by the Range safety organisations than systems that had been designed by other authorities. Follow-up discussions with members of the Range safety team, corroborated by the O&STWG, revealed a mindset which believed that the University, as a learned organisation, had a high degree of competency in system design through default; this was further driven by the fact that the individuals concerned believed that such an organisation would not have been so onerously driven by financial pressures. Such observations may, or may not, be accurate but they do provide an insight into some of the human related,

intangible and subjective thoughts that the supervisory/regulatory body may exhibit when trying to conclude if an UAV system is safe to fly, or not.

The SCET itself may be utilised in two distinct ways; the first as a tool to aid an UAV organisation to comprehensively and diligently design, build and operate a system, and secondly as a skeleton by which supervisory and/or regulatory bodies may comprehensively review the complete system for a safe operation. If applied in its first guise the SCET may offer good opportunities for an UAV organisation to minimise costly re-design and re-engineering activities which may have only been uncovered at the final 'approval to fly' phase.

When applied in its second and predominant state the SCET acts as a screening function to eliminate some organisations which may be lacking in competency, and to clearly establish where more focus may be required before a robust safety case may be accomplished. The commercial opportunities offered by the expanding UAV market was highlighted and discussed in chapter three. Such opportunities will, without question, attract organisations (e.g. utility companies, media companies, private security companies, etc.) from outside the aerospace industry who may wish to build and operate bespoke UAV systems. The SCET would provide an excellent foundation by which a degree of technical assurance and compliance may be applied to any proposed UAV platform. Any organisations who are eliminated, or fail to provide the required level of assurance, may continue in dialogue with the supervisory/regulatory body and gain an understanding of what additional information and mitigations are required to advance towards an approval to operate. The SCET questions, and any subsequent responses, discriminate any potentially high-risk issues to the planned operation; further questions may then be asked by the supervisor or regulator to augment what has already been supplied. In a similar manner further questions may be added to the SCET as and when the 'sense and avoid' issue is effectively dealt with by the aerospace industry.

9.4 Discussion.

The intent of this thesis was to develop a revised approach for managing the safety aspects of operating civil Light UAVs within the UK; the need was identified by the extant

minimal level of regulatory requirements demanded by the CAA. Analysis of the civil UAV environment suggests that this minimal level of requirement is not driven by a specific and easily identifiable reason; it is suggested by the author that it is due, predominantly, to the fact that the regulatory bodies have not kept abreast with the changes within the business and technological arenas of the civil UAV market. The extant regulations are virtually wholly focussed upon the very sparse number of recreational designers and operators within the model aircraft world. The extant regulations have served these recreational users very well for many years but now, predominantly due to 'loose' categorisations and definitions, the potential is present for such minimal regulations to cause harm to the commercial civil UAV market unless tighter restrictions are imposed on any commercial venture.

Whilst the SCET allows most, if not all, of the interested parties concerned with the development and operation of an UAV platform to gain an understanding of the type of engineering methodology which should be applied to achieve a safe and homogenous system it has a number of drawbacks. One of the fundamental tenets of any form of safety case is that of the provision of true, honest and system representative data. The traditional quantitative safety case demands many numerical elements to be provided which cannot be easily disguised; for example, the failure rate of a mechanical component may be constant under quoted stress and environmental criteria; the numerical answer is clearly defined. Within the SCET approach increased reliance is made of the qualitative and often subjective views of, at times, a team of individuals. Given the diversity of language and the way that different words can be arranged in different sequences, the message conveyed, both explicitly and implicitly, can change dramatically. The SCET demands quantitative data, predominantly in relation to the control & command and safety related flight termination system; this approach not only ensures compliance with published regulatory risk criteria but to limit the degree of 'qualitative freedom' which may be applied by any potentially unscrupulous UAV organisations.

Another drawback that the SCET exhibits is the fact that due to its reliance upon a more qualitative approach it relies upon words, lots of them. Conscientious organisations will endeavour to provide as much detail as possible, quite possibly to a level of detail which

would make the task of scrutiny very laborious and even ineffective. Extant traditional safety cases can be very large and may exhibit a high word count; the SCET, by demanding information on human factors and other soft issues within the UAV organisations, will predominantly increase the level of supplied text. With this in mind the author suggests that word limits are applied to the information supplied and that, if appropriate, existing organisational and regulatory documentation should be merely referenced. Such an approach already exists in many professions which demand and rely upon fundamental source information in order to make important and long-standing decisions; examples include applications for Chartered Engineer status (CEng, 2010) and applications to become a medical doctor (UCAS, 2010).

In instances where the supplied data is minimal in detail, relatively weak and/or deemed inappropriate by the regulatory/supervisory body then, as part of an interactive and iterative process, more information may be supplied on demand. Whilst unscrupulous organisations may decide to offer minimal information at first, and then to simply supply more on demand, the experience, expertise and professional judgement of the regulatory/supervisory body will no doubt sense the presence of iniquitousness.

Having been immersed in the UAV environment for an extended period of time, the author believes that one of the key issues which is seriously affecting the whole civil UAV environment, certainly within the UK, is the 'sense and avoid' issue. Until a way forward is identified to deal with this impasse the potential for market and investment growth will continue to suffer from acute strangulation. This is true for most countries which have a relatively well established and structured airspace management policy for manned aircraft and struggle with the idea of allowing unmanned platforms to co-exist within the same piece of airspace. This thesis has not attempted to deal with the 'sense and avoid' issue though the SCET could be amended to incorporate any key elements which would underpin safe flying within shared airspace.

Though the SCET does not tackle the 'sense and avoid' issues it does provide a framework by which a more vigorous and in-depth analysis may be made of the UAV system. The SCET attempts to provide the regulating or inspecting authority with a body of evidence

which is more ‘rounded’ in its approach; providing a better insight into many of the traditionally ignored aspects of engineering, safety and operations. By delving into the safety industry and those important components which it relies upon the author has uncovered an array of issues, predominantly concerned with the ‘softer’ parts of the system, - the human.

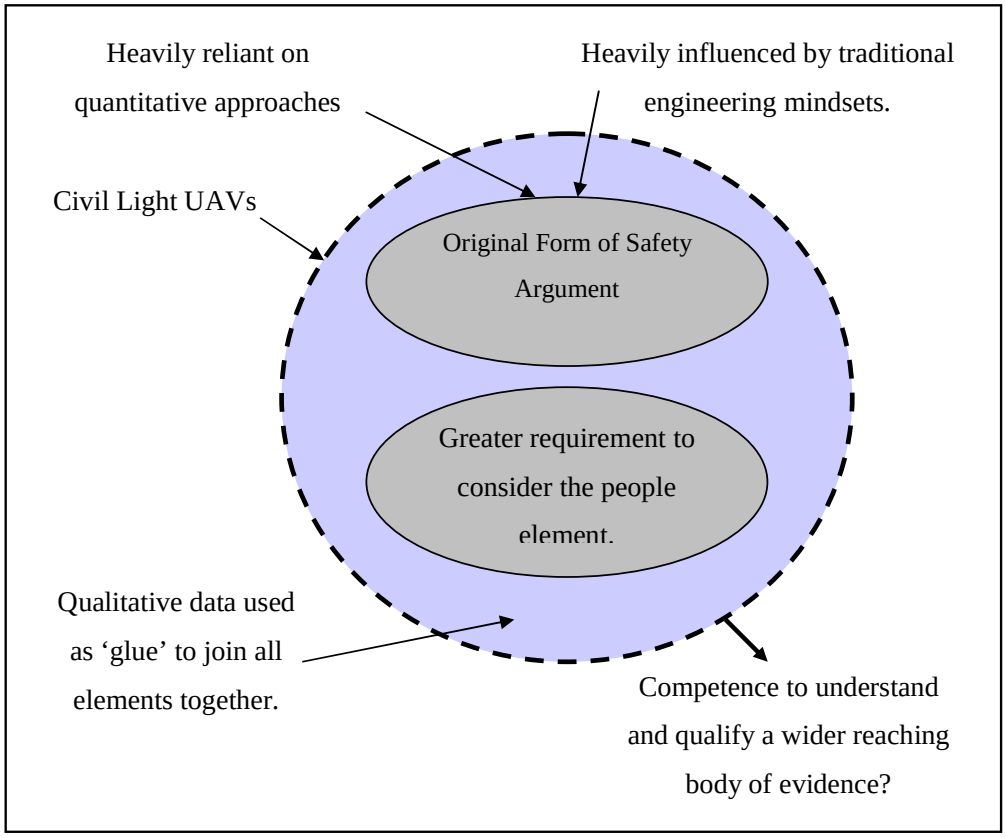


Fig 9.1 - Diagram illustrating how qualitative data strengthens traditional safety cases and combines the people element of systems.

Whilst the more traditional (certainly for the last thirty years) and established method of establishing that a system was safe is focussed upon numbers and probabilities, there is much to gain from the qualitative side of the equation. By adopting a more qualitative approach the tool for assessing and/or arguing safety can better accommodate the people aspects of the system under scrutiny; surely this is a step in the right direction when the

majority of failures and accidents within the industry are linked to human error. Figure 9.1 illustrates the author's thoughts on the revised safety approach. The qualitative component is seen as the mortar which is holding the key components (akin to building blocks) together to create a more detailed and valuable argument for the system as a whole. Upon reflection the concept of using a more qualitative approach seems relatively acceptable and would seem to align with some of the principles of good common sense such as practicality, discernment and sensibility.

The author believes that whilst the qualitative component offers another way of assessing and processing information, in a way which is parallel to the quantitative way that we use, he strongly believes it has much more to offer. Qualitative data provides so much richness and context to the whole aspect of a system. Whilst he acknowledges the difficulty that can arise in trying to create a safety argument based wholly upon qualitative data, the author envisages an approach which combines the qualities of both approaches. In plain terms it could be said that the 'safety pendulum' has swung too far into the quantitative direction over the past few years; it may be time to start bringing it back in the other direction for a more balanced view to be made available. Such an approach aligns very strongly with the work of Hollnagel (2004) and his suggestion that trends in attributed accident causation has changed over time. Figure 6.1 illustrates how accident investigation and the sentencing of causation is now focussing more upon organisational failures such as inappropriate cultures, behaviours and attitudes.

It has already been highlighted in Chapter 7 how UAVs, in general terms, are challenging many of the established and more traditional concepts of safety management. Figure 7.1 illustrated how the light civil UAV regulatory environment compares with other flying activities within the procedural and residual risk categories. Given that there is no human aboard, the mindset of life preservation from both the pilot's perspective and that of the support organisation (e.g. design, maintenance, repair, etc.) are possibly not vested as strongly or as emphatically as within a manned aircraft. Quite clearly from this lucid comparison there is a clear and immediate need to include a wider reaching and greater variety of non-quantitative and 'softer' engineering elements in any safety argument to support UAV flying operations. The need to include the human element, specifically the

culture within an organisation has been shown as being important in the overall scheme of safety within an operating system. By incorporating the human element with that of the technical aspects of the system the resulting output appears to offer a much ‘rounder’ and wholesome argument of system safety and integrity. Whilst human factors engineering has been present within the manned flight environment for many decades, its use within the UAV environment is still relatively light; any human factors engineering which is present is predominantly focussed towards operator (pilot) training, competency and currency rather than systematically being applied throughout the wider system.

CHAPTER 10

Conclusions & Recommendations

Formatted: Bullets and Numbering

10.1 Conclusions.

The author believes that there is a need for a relatively large change in mindset if a more qualitative and 'people' orientated safety case is to be adopted within the general engineering environment. Within, and peripheral, to the industry of T&E, the author is cognisant of the fact that the current safety mindset is heavily biased by the probabilistic and goal driven regulations which utilise quantitative safety analysis. Whilst quantitative approaches appear to be objective, in reality they may be judgmental. Such judgements may be quite explicit where data is not available but can be quite implicit where both numerical and qualitative data is present; for the latter these judgements may be unrecognised and lead to serious unconscious assumptions. Overlooking, or disregarding the significance of such judgements may lead to false predictions in the quantitative figures which are revered so much in today's engineering environments. Decision making relating to hazard and risk management is a complex activity which must rely upon many other key contributors such as social, political and economical factors, and not merely the quantitative aspects of risk prediction.

Whilst this thesis has focussed upon the civil light UAV arena, there are large parallels and similar opportunities available for such an approach in other environments. Within the field of civil light UAVs the author strongly believes that the problem surrounding the 'sense and avoid' issue is taking much energy and focus away from the need to evolve and grow the industry as a whole. The 'sense and avoid' issue seems to be stifling much needed advancement in other areas of civil UAV use such as engineering safety and human factors. Quite possibly, by creating a more welcoming, better regulated and well governed civil UAV environment, the problem of 'sense and avoid' could be better solved from within the environment. By creating a realistically operational and relatively well structured civil UAV environment, the regulatory authorities could allow a degree of evolution to take place through the adoption of good practice, learning from incidents and accidents (from within a relatively sterile operating environment) and technology advancement. The

opportunity beckons to allow controlled evolution rather than the creation of a revolution in the field of civil unmanned aviation.

Clearly from the research into safety culture and safety climate (chapter six), there is a great deal of qualitative information available to underpin the predominantly quantitative approaches within the modern business. Informal discussions with Independent Safety Assessors (ISAs), reviewing some of QinetiQ's major projects, suggests that the current bias towards a quantitative approach needs to be rebalanced.

The author is conscious that the interpretations and thought processes within this thesis are based upon his own self beliefs and perceptions based upon research and experience; the latter based upon over twenty years within the T&E environment. Risks and hazards are very subjective and the boundaries by which they are sentenced and managed varies greatly on the immediate environment and experiences of the reviewer. The author would have liked to have had the opportunity to discuss the SCET with other cultures in different countries in order to better understand the variation in subjectivity and to better understand the weaknesses, and strengths, within the SCET.

Safety, like many other professional disciplines (such as medicine) will evolve with time, and quite possibly will come 'full circle'. Virtually all of the research and background to this thesis, including the author's experiences, relate to the western world and its doctrine for analysing and managing safety. If safety evolves again into a more qualitative era then we may have much to learn from less restrictive cultures where the focus is not on numbers, compensation and materialistic trophies but on communication, 'common sense' approaches and enjoying life. Whilst based upon sound and moralistic foundations to minimise damage to our loved ones and our employees, has safety evolved to be solely a tool to minimise management litigation; or has it created an industry of self perpetuating professionals which justifies its presence by hiding behind legislation and the ignorance of the uneducated? The author offers no answers but raises the questions to stir the mind.

10.2 Original Contribution to Knowledge.

Formatted: Bullets and Numbering

The following points describe how this thesis offers an original contribution to knowledge;

- From investigation of past and current literature, a distinct and extant gap in the safety management and regulation of civil light UAVs (< 150kg) has been identified. This thesis analyses this gap and offers a tool to allow organisations, and individuals, operating within the environment, to create and review the safety of their system with a degree of robustness.
- Having reviewed past and present literature on the creation and management of safety cases, the author has identified that whilst there are general definitions for what a safety case is, the level of granularity for what should be included is minimal. This thesis, and the SCET contained within it, attempts to provide another level of granularity, specifically within the field of civil light UAVs.
- By adopting a *Systems Engineering* approach, and by investigating the areas which cause the most accidents and incidents within the general UAV environment, the author has identified the need to take more cognisance of the human element within any safety argument. Whilst 'human factors' is used to sentence some incident causations, the degree of investigation to find the absolute root cause is minimal. Review of past and current literature suggests that whilst the industry is aware of these issues, rarely are they combined at a single point such as a safety case.
- Having established the need to use more data from the human element the author has identified the need for a more qualitative approach to safety cases. Safety cases are predominantly assembled by engineers, or individuals with a quantitative background. Employing such individuals automatically creates a mindset within the safety community which is almost wholly focussed upon a quantitative approach. In-depth discussions within the thesis identifies how qualitative data contains important information relating to safety and that quantitative data in isolation may be subject to errors in interpretation. This thesis attempts to highlight this observation and to readdress the balance between a quantitative and qualitative approach.
- The civil light UAV market is in its infancy within the UK. The SCET's qualitative approach allows smaller businesses and organisations to create a safety argument

without the need to employ relatively complicated, expensive and specialised quantitative analysis tools. The use of such tools can be restrictive due to the training required to ensure that the tool is not only used correctly but is applied with the appropriate degree of context for the argument. The SCET allows for lighter and smaller UAVs to be safety assessed in a less expensive and onerous manner whilst maintaining an acceptable, yet alternatively derived, body of safety information.

This revised approach to assembling a safety case for Civil Light UAVs does not tackle the most demanding of current UAV challenges which is that of 'sense and avoid'. The aim of this new type of safety case approach is to facilitate a more complete body of evidence so that safety engineers, safety managers or regulators may make a more accurate, relevant, and consolidated judgement of the system under scrutiny. The decision upon how to manage the 'sense and avoid' issue may be incorporated into the safety case, at a later stage, once an agreed policy and procedure has been identified by the relevant regulatory authorities.

Formatted: Bullets and Numbering

10.3 Recommendations.

The following recommendations are made by the author;

- The SCET be used by the civil UAV community to allow a more detailed and holistic body of information to be assembled in support of light UAV (< 150kg) operations.
- The SCET be adopted by the T&E safety management environment (primarily through the O&STWG) as the basis for safety management of UAVs and weapon systems. Whilst the extant regulatory and operational framework suggests a quantitative approach, additional data in qualitative terms may be gathered, especially in relation to organisational culture and the people element of the business.
- Further work is carried out to gain progressive assurance of the SCET's validity through continued applications. This may be achieved by obtaining feedback from both military and civil users of the tool in a wider application.

- This thesis is used as a catalyst for more research in the creation of safety cases which take serious cognisance of the human element within systems; such an approach should see humans as an integrated component and not a somewhat isolated ‘soft system’ to be bolted onto the ‘hard engineering’.

This page left intentionally blank.

REFERENCES

Aberdeen (1995) *An Interim Evaluation of the Offshore Installations (Safety Case) Regulations 1992*. Aberdeen University, Scotland, UK.

Atkinson, W. (2000) Behaviour-based safety. *Management Review.* February. pp41-46.

Ayliffe, A. (2006) *West Wales UAV Centre ParcAberporth Safety and Qualification Questionnaire*. QinetQ/D&TS/SES/SA0605843/0.1. QinetiQ Proprietary, 28th April, 2006.

Balchin, N. (1947) Satisfactions in Work, *Occupational Psychology.* July, 1947.

Barraclough, I. & Carnino, A. (1998) *Safety Culture: Keys for sustaining progress.* International Atomic Energy Authority Bulletin, No. 40/2, 1998.

Bishop, P. G. & Bloomfield, R. E. (1995) *The SHIP Safety Case Approach.* SafeComp95, Belgirate, Italy 11-13, pp 437-451, Adelard, London, E3 2DA, England.

Blanchard, B. S. (2008) *System Engineering Management*. John Wiley & Sons, Hoboken, New Jersey, 4th edition.

BP (2007) *The Report of The BP US Refineries Independent Safety Review Panel*. BP Texas City incident, Baker Review, www.hse.gov.uk/leadership/bakerreport.pdf. (18/03/2009).

Breakwell, G. M., Hammond, S. & Fife-Schaw, C. (1995) *Research Methods in Psychology*. Sage Press, London.

Brown, J. A. C. (1980) *The Social Psychology of Industry*. Penguin books limited, Middlesex, England, Reprint with Postscript.

CAA (2004a) *UK-CAA Policy for light UAV systems.* Design & Production Standards Division, Civil Aviation Authority, UK.

CAA (2004b) *Unmanned Aerial Vehicle Operations in UK Airspace – Guidance, Civil Air Publication 722*. (CAP 722), Directorate Airspace Policy, Civil Aviation Authority, UK.

CAA (2002a) *Aircraft Airworthiness Certification Standards for Civil UAVs*. Design & Production Standards Division, Civil Aviation Authority, UK.

CAA (2002b) *An introduction to Aircraft Maintenance Engineering Human Factors for JAR 66, Civil Air Publication 715*. (CAP 715), Human Factors, Aerodrome, Air Traffic and Licensing Standards Division, Safety Regulatory Group (SRG), Civil Aviation Authority, UK.

CAA (1998) *Analysis of Airprox in the UK: Joint Airprox Working Group Report No. 3/97.* Civil Aviation Authority, London, August 1998.

CBI (1990) *Developing a Safety Culture – Business for Safety.* Confederation of British Industry, Loose Article, London CBI.

Cable & Wireless (2006a) *Cable & Wireless Criminal Justice Extranet (CJX) and Secure Communities Network (SCN), Service Information.* Cable & Wireless, Bracknell, Berkshire.

Cable & Wireless (2006b) *Cable & Wireless National Private Circuits, Service Information.* Cable & Wireless, Bracknell, Berkshire.

Campbell, D. T. & Fiske, D. W. (1959) Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin*. Vol. 56, No.2, pp81-105.

Carver, C. S. & Scheier, M. F. (1998) *On the Self-Regulation of Behaviour*. Cambridge University Press, Cambridge.

Checkland, P. (1981) *Systems Thinking, Systems Practice*. John Wiley and Sons, Chichester, UK.

Cheyne, A., Cox, S., Olivier, A. & Tomas, J. M. (1998) Modelling safety climate in the prediction of levels of safety activity. *Work and Stress.* Vol. 12. No.1. pp255-271.

Clarke, S. (1999) Perceptions of organisational safety: implications for the development of safety culture. *Journal of Organisational Behavior.* Vol. 20. pp185-198.

Clarke, S. (1998) Safety Culture on the UK railway network. *Work and Stress.* Vol. 12. No.3. pp285-292.

Clott, A. (2005) *A Route Map for Realising a UAV Systems Industry in the UK; A National Plan.* Unmanned Aerial Vehicle Systems Association (UAVSA), Proposal to the UAVS Trade Association.

Collinson, D. L. (1999) Surviving the rigs: Safety and surveillance on North Sea oil installations. *Organisation Studies.* Vol. 20. No.4. pp579-600.

Cooper, D. (1998) *Improving Safety Culture: A Practical Guide.* Wiley, ISBN 0-471-95821-2.

Cooper, D. (2000) Towards a model of safety culture. *Safety Science*. Vol. 36. pp111-136.

Cooper, D & Philips, X. (2004) Exploratory analysis of the safety climate and safety behaviour relationship. *Journal of Safety Research*. Vol. 35.

Cox, S. J. & Cheyne, A. J. T. (2000) Assessing safety culture in offshore environments. *Safety Science.* Vol. 34. pp111-129.

Cox, S. J. & Flin, R. (1998) Safety Culture: Philosopher's Stone or Man of Straw? *Work and Stress.* No. 12, Vol. 3. pp189-201.

Coyle, I. R., Sleeman, S. D. & Adams, N. (1995) Safety Climate. *Journal of Safety Research*. Vol. 26, Issue 4. pp247-254.

Crystal, D. (1990) *The Cambridge Encyclopaedia*. Cambridge University Press, Cambridge, England, UK.

Cullen, Lord (2001) *The Ladbroke Grove Rail Inquiry*. Part 2 Report. London HMSO.

Cullen, Lord (1996) *The Development of Safety Legislation*. Royal Academy of Engineering and Royal Society of Edinburgh Lecture, Lecture notes, February 12th.

Cullen, Lord (1990) *The Public Inquiry into the Piper Alpha Disaster*. London HMSO.

Davies, J., Ross, A., Wallace, B. & Wright, L. (2003) *Safety Management: A Qualitative Systems Approach.* Taylor & Francis, 11 New Fetter Lane, London.

De Cort, R. (1994) The Development of UK and European Major Hazards Legislation and the Review of the Seveso Directive; The Implications for Industry. *Disaster Prevention and Management.* Vol. 3.

Dedobbeleer, N. & Beland, F. (1998) Is risk perception one of the dimensions of safety climate? *Occupational injury: Risk prevention and intervention*. London, Taylor and Francis.

Defense Science Board (2004). *Unmanned Aerial Vehicle Reliability Study.* Office of the Secretary of Defense, Washington, DC.

Despotou, G. & Kelly, T. (2004) *Extending the Safety Case Concept to Address Dependability*. Proceedings of the 22nd International System Safety Conference, pp 645-654.

Duncker, K. (1945) On problem solving. *Psychological Monographs.* 58(5), No. 270.

Dyer, C. (2000) The Lessons From Sellafield, *Health & Safety Bulletin*. Vol. 287. pp7-14.

Eiff, G. (1998) *Organisational Culture and its Effect on Safety*. 12th Symposium on Human Factors in Aviation.

Emson, R. (2009) *The Admissibility of Expert Evidence in Criminal Proceedings in England and Wales.* The Law Commission, Consultation Paper No.190, Steel House, 11 Tothill St, London.

CEng. (2010) *Academic Standards for CEng Registration.* Engineering Council (UK) website, www.engc.org.uk (4/06/2010).

Evans, A.W. (2005) *Safety Appraisal Criteria*. The 2005 Lloyd's Register Lecture on Risk Management, The Royal Academy of Engineering, 29 Great Peter Street, London.

Fennell, D. (1988) *Investigation into the King's Cross Underground Fire*. Department of Transport. London HMSO.

Fielding, N. G. & Fielding, J. L. (1986) *Linking Data (Qualitative Research Methods).* Sage Press, London, Vol. 4.

Fisli, R. (2005) *Secure Corporate Communications over VPN-Based WANs.* Master's Degree Project, KTH Numerical Analysis & Computer Science, Stockholm, Sweden.

Flin, R., Mearns, K., O'Connor, P. & Bryden, R. (2000) Measuring Safety Climate: Identifying the common features. *Safety Science*. Vol 34. pp177-193.

Flood, R. & Carson, E. (1993) *Dealing with Complexity: An Introduction to the Theory and Applications of Systems Science*. Plenum Press, London, UK.

Garman, E. (2007) *Ranges & Facilities Safety Case Part 2: Goal Structured Notation.* TECS/HSES/PR100/Pt 2/1.0, QinetiQ, Unpublished.

Garman, E. (2006) *Ranges & Facilities Safety Case Volume 7: Risk Criteria for Trials and Risk Management Methodology*. TECS/HSES/PR106/C, QinetiQ, Unpublished.

Gerold, A. (2006) *UAV : Manned and Unmanned Aircraft; Can they co-exist?*. www.aviationtoday.com/military. (18/11/2007).

Gilbreth, F. B. (1911) *Motion Study: A Method for Increasing the Efficiency of the Workman.* D. Van Nostrand Company, New York, NY.

Glendon, A. I. & Litherland, D. K. (2001) Safety climate factors, group differences and safety behaviour in road construction. *Safety Science*. Vol. 39. pp157-188.

Glendon, A. I. & McKenna, E. F. (1995) *Human Safety and Risk Management*. Chapman & Hall, London, UK.

Govier, T. (1992) *A Practical Study of Argument*. Belmont CA, Wadsworth, 3rd edition.

Groenweg, J. (1996) *Controlling the Controllable: The Management of Safety*. DSWO Press, Leiden, 3rd edition.

Guldenmund, F. W. (2000) The Nature of Safety Culture: A Review of Theory and Research. *Safety Science.* Vol. 34. pp215-257.

Haddon-Cave (QC), C. (2009) *An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006*. London HMSO.

Haddon, D. R. & Whitaker, C. J. (2002) *Aircraft Airworthiness Certification Standards for Civil UAVs*. Civil Aviation Authority, UK.

Hale, A. R. (2000) Culture's Confusions. *Safety Science.* Vol. 34. pp1-14.

Harries, L. S. (2009) *A Business Case to Identify Opportunities to Replace an ATSA with an ATCO*. QinetiQ Proprietary, Unpublished.

Harvey, J., Bolam, H. & Gregory, D. (1999) How many safety cultures are there? *The Safety and Health Practitioner*. Vol. 17. No.12. pp9-12.

Heidegger, M. (1962) *Being and time*. SCM Press, London, UK.

Hitchins, D. K. (1992) *Putting Systems to Work*. John Wiley & Sons, Chichester, England, UK.

Hollnagel, E. (2004) *Barriers and Accident Prevention: or how to improve safety by understanding the nature of accidents rather than finding their causes*. Ashgate Publishing Ltd, Aldershot, England, UK.

HSE (2009a) *ND Guidance on the demonstration of ALARP (as low as reasonably practicable).* Health and Safety Executive, T/AST/005 Issue 4 Rev 1, Issued 20th January 2009, London, HMSO.

HSE (2009b) *Guidance on 'as low as reasonably practicable' (ALARP) decisions in control of major accident hazards (COMAH).* Health and Safety Executive, SPC Permissioning/12, London, HMSO.

HSE (2008a) *ALARP "at a glance"*. Health and Safety Executive, ALARP Guide, www.hse.gov.uk/risk/theory/alarpglance.htm, (15/04/2008).

HSE (2008b) *HSC/E Merger Announcement*. Health & Safety Executive, What's new at HSE, www.hse.gov.uk/2008/04/01/hsce-merger-announcement.html, (04/05/2010).

HSE (2006a) *HSE Information Sheet No. 2/2006, Offshore Installations (Safety Case) Regulations 2005 Regulation 12*. Health and Safety Executive, Information Sheet, London, HMSO.

HSE (2006b) *Safety Assessment Principles for Nuclear Facilities.* Health and Safety Executive, London, HMSO.

HSE (2005) *Revision of the Offshore Installations (Safety Case) Regulations 1992 (OSCR).* Health and Safety Executive, London, HMSO.

HSE (2004a) *Thirty years on and looking forward – The development and future of the health and safety system in Great Britain*. Health and Safety Executive, London, HMSO.

HSE (2004b) *Working Together to Reduce Stress at Work, A Guide for Employees*. Information Sheet Misc. 686, Health and Safety Executive, London HMSO.

HSE (2001a) *Reducing risks, protecting people: HSE's decision-making process*. Health and Safety Executive, London, HMSO.

HSE (2001b) *Summary guide to safety climate tools*. Offshore Technology Report 1999/063, Health and Safety Executive, London, HMSO.

HSE (2000) Successful Health and Safety Management. *Health and Safety Series Books, HS(G)65.* Health and Safety Executive, London HMSO.

HSE (1999) Reducing error and influencing behaviour (second edition), *Health and Safety Series Books, HS(G)48.* Health and Safety Executive, London HMSO.

HSE (1993) Advisory Committee on the Safety of Nuclear Installations (ACSNI) Study Group on Human Factors. *Third report: Organising for Safety*. Health and Safety Executive, London HMSO.

HSE (1975) *The Flixborough Disaster: Report of the Court of Inquiry*. Health and Safety Executive, London, HMSO.

IET (2008a.) Independent Safety Assurance (ISA) Key Topic, Promoting the role of Independent Safety Assessor, *The Institution of Engineering and Technology (IET).* www.theiet.org/publicaffairs/isa/index.cfm, 09/05/08.

IET (2008b.) Using competence frameworks for CPD, A guide to using competence frameworks for continuous professional development. *The Institution of Engineering and Technology (IET).* www.theiet.org/careers/cpd/competences/19/02/2008.

Johnson, E. N. (2003) Making UAVs smarter. *Aerospace America*. pp20-22.

Kelly, T. (2008) Are Safety Cases Working? *Safety Critical Systems Club Newsletter*, Vol 17, No.2, pp31-33.

Kelly, T. (2003) *A Systematic Approach to Safety Case Management.* SAE International, 04AE-149, Department of Computer Science, University of York, UK.

Kelly, T. (2001) *Concepts and Principles of Compositional Safety Case Construction.* (Contract Research Report for QinetiQ COMSA/2001/1/1), Department of Computer Science, University of York, UK.

Kelly, T. (1998) *Arguing Safety – A Systematic Approach to Managing Safety Cases.* (PhD Thesis), Department of Computer Science, University of York, UK.

Kelly, T. P. and McDermid, J. A. (2001) A Systematic Approach to Safety Case Maintenance. *Reliability Engineering and System Safety*. Vol 71. pp271-284.

Kelly, T. P. and McDermid, J. A. (1995) Safety Case Patterns - Reusing Successful Patterns. Rolls-Royce Systems and Software Engineering, University Technology Centre, Department of Computer Science, University of York.

Kennedy, R. & Kirwan, B. (1998) Development of a Hazard and Operability-based method for identifying safety management vulnerabilities in high risk systems. *Safety Science.* Vol. 30. pp249-274.

Kirk, S. (2005) *What We Know: Safety Culture*. www.saferhealthcare.org.uk/IHI/Topics /SafetyCulture/WhatWeKnow/published 27 July 2005.
La Franchi, P. (2005) UAVs could revitalise UK industry. *Flight International.*

Lee, T. (1998) Assessment of safety culture at a nuclear reprocessing plant. *Work and Stress.* Vol. 12. No.3. pp217-237.

Lee, T. & Harrison, K. (2000) Assessing safety culture in nuclear power stations. *Safety Science.* Vol. 30. pp61-97.

Lees, F. P. (1996) *Loss prevention in the process industries – Hazard identification, assessment and control*. Butterworth Heinemann, Vol. 3. ISBN 0-7506-1547-8.

Leveson, N. G. (2002) *A New Approach To System Safety Engineering*. Aeronautics and Astronautics, Massachusetts Institute of Technology.

Lindsay, P. R. & Stuart, R. (1997) Reconstruing competence. *Journal of European Industrial Training*. Vol. 21.

Maslow, A. H. (1943) A Theory of Human Motivation. *Psychological Review.* No. 1.

Maxwell, J. A. (1998) Designing a qualitative study. Quoted in L. Bickman & D.J. Rog. *Handbook of Applied Social Research Methods.* Thousand Oaks Press, London, UK.

McCarley, J. S. & Wickens, C. D. (2005) *Human factors implications of UAVs in the National Airspace*. Technical Report AHFD-05-05/FAA-05-01, Federal Aviation Administration, Atlantic City, New Jersey, USA.

McCutcheon, J. E. (1963) *The Hartley Colliery Disaster, 1862*. (With a foreword by The Rt. Hon. Lord Robens of Woldingham, P.C., Chairman, National Coal Board). (Hardback sourced through Mr I McKay, Privately Published).

McDermid, J. & Kelly, T. (2005) *Operational Management and Maintenance*. MSc Safety Critical Engineering, Course Notes, York University, England, UK.

Mearns, K., Flin, R., Gordon, R. & Flemming, M. (1998) Measuring safety climate on offshore installations. *Work and Stress.* Vol. 12. No.3. pp238-254.

Mearns, K., Flin, R., Gordon, R. & Flemming, M. (2001) Human and organisational factors in offshore safety. *Work and Stress.* Vol. 15. No.2. pp144-160.

MoD (2004) *Safety Management Requirements for Defence Systems*. Ministry of Defence, Interim Defence Standard (00-56), Parts 1 (Requirements) & 2 (Guidance), Issue 3, December 2004, London, HMSO.

MoD (1997a) *Handbook of Defence Land Ranges Safety.* Ministry of Defence, Joint Services Publication (JSP) 403, Vol.1. April 1997, London, HMSO.

MoD (1997b) *Requirements for Safety Related Software in Defence Equipment.* Ministry of Defence, Defence Standard (00-55), Parts 1 (Requirements) & 2 (Guidance), Issue 2, August 1997, London, HMSO.

Műnsterberg, H. (1913) *Psychology and Industrial Efficiency*. Boston & New York, Houghton Mifflin Company, Boston, MA.

Myers, C. S. (1921) *Mind and Work: The Psychological Factors in Industry and Commerce.* University of London Press, London, UK.

Myers, C. S. (1909) *A Textbook of Experimental Psychology with laboratory Exercises*. Cambridge University Press, 1st Edition.

NATS (2008) *Human Factors Safety Assurance for Changing ATM Systems.* Article presented in the proceedings of the 16th Safety-critical System Symposium, Bristol, UK, 5th-7th February 2008.

Oxford (1995) Concise English Dictionary, 9th edition, Oxford University Press.

Payne, R. (1996) *The Characteristics of Organisations: Psychology at Work.* Penguin Press, London, UK.

Pearson, K. (1999) *Tolley's survey of senior executives commitment to health and safety (1999 to 2000).* Butterworths Tolley, UK.

Perrow, C. (1984) *Normal accidents: Living with high risk technologies.* Basic Books Inc., New York, USA.

Peterson, D. (1993) Establishing good safety culture helps mitigate workplace dangers. *Occupational Health & Safety.* Vol. 62. No.7. pp20-24.

Pidgeon, N. (1998) Safety culture: Key theoretical issues. *Work and Stress.* Vol. 12. No.3. pp202-216.

Pidgeon, N. & O'Leary, M. (2000) Man-made disasters: Why technology and organisations (sometimes) fail. *Safety Science.* Vol. 34. pp15-30.

Popper, K. (1963) *Conjectures and Refutations: The Growth of Scientific Knowledge.* Routledge, London, UK.

Richards, A. (2006) *Financial and Commercial Analysis of the Air Traffic Control Pan-Ranges Support Contract; Years 1 & 2.* QinetiQ internal report, April 2006, Unpublished.

Richards, G. (2009) Is it a bird, is it a plane? *Engineering & Technology*. Vol. 4, No. 4, pp44-47.

Robens, Lord. (1972) *Safety and Health at Work. The Report of the Robens Committee*. London, HMSO.

Robson, C. (1993) *Real world research: A resource for social scientists and practitioner-researchers.* Blackwell Press, Oxford, UK.

Rowley, P. (2008) *Ranges & Facilities Safety Case: Parts 11 & 26, Aberporth*. QinetiQ Proprietary, Unpublished.

Rundmo, T. (2000) Safety climate, attitudes and risk perception in Norsk Hydro. *Safety Science.* Vol. 34. pp47-59.

Rundmo, T. (1996) Associations between risk perception and safety. *Safety Science.* Vol. 24.

Rundmo, T. (1995) *Experience of risk and safety in Norwegian offshore workers. Changes in risk perception in the period 1990 to 1994.* Conference Paper: Understanding Risk Perception, Robert Gordon University, Aberdeen.

Rundmo, T., Hestad, H. & Ulleberg, P. (1998) Organisational factors, safety attitudes and workload among offshore oil personnel. *Safety Science.* Vol. 29. pp75-87.

Sage, AP. (1992) *Systems Engineering.* John Wiley & Sons, Chichester, England, UK.

Sandom, C. (2002) *Human Factors Considerations for System Safety*. Proceedings of the 10th Safety Critical Systems Symposium, 5th - 7th February, 2002.

SBAC (2005) *UK UAV Industry Opportunities with Boeing*. Sourced from the Society of British Aerospace Companies, 2005. www.defense-aerospace.com. (3/11/2005).

Seymour, J. (2008) New Hartley Colliery Disaster, Extracted from the *Illustrated London News, 1862, January 25th*. No. 1129, Page 81.

Simard, M. & Marchand, A. (1994) The behaviour of first line supervisors in accident prevention and effectiveness in occupational safety. *Safety Science*. Vol. 17. pp169-185.

Skelton, B. (1997) *Process Safety Analysis: An Introduction*. Butterworth-Heinemann Publishing, UK.

Skyttner, L. (2001) *General Systems Theory: An Introduction.* MacMillan Press Ltd, Basingstoke, UK.

Smallman, C. & John, G. (2001) British directors' perspectives on the impact of health and safety on corporate performance. *Safety Science.* Vol. 38. pp227-229.

Taylor, F. W. (1919) *The Principles of Scientific Management*. Harper & Row, New York, NY.

Thales (2004) *The Thales WATCHKEEPER System; The British Solution.* www. thales group.co.uk/Watchkeeper. (11/12/2005).

Thompson, R. C., Hilton, T. F. & Witt. L. A. (1998) Where the safety rubber meets the shop floor: A confirmatory model of management influence on workplace safety. *Journal of Safety Research.* Vol. 29. pp15-24.

Toulmin, S. E. (1958). *The Uses of Argument*. Cambridge University Press, Cambridge, UK.

Tvaryanas, A. P., Thompson, B. T. & Constable, S. H. (2005) *U.S. military UAV mishaps: Assessment of the role of human factors using HFACS*. Human Factors paper presented at the May UAV workshop, Mesa, Arizona, USA.

UCAS. (2010) *So You Want To Be A Doctor?* Widening Access to Medical School: An admissions resource for those applying for medical school in the UK. www.wanttobeadoctor.co.uk/main (4/06/2010).

Varonen, U. & Mattila, M. (2000) The safety climate and its relationship to safety practices, safety of the work environment and occupational accidents in eight wood processing companies. *Accident Analysis and Prevention.* Vol. 32. pp761-769.

Vaughan, G. (2005) *Demonstration of ALARP*. Nuclear Safety Directorate, Technical Assessment Guide, T/AST/005, 2005.

Vesely, W. E. (1987) *Fault Tree Handbook*. Nuclear Regulatory Commission, UK.

Wallace, B., Ross, A. & Davies, J. B. (2003) Applied hermeneutics and qualitative safety data: The CIRAS project. *Human Relations.* Volume 56(5), pp587-607.

Waring, A. (1996) *Practical Systems Thinking.* International Thomson Business Press, London, UK.

Warner, H. (2009) *Ranges & Facilities Safety Case: Parts 15 & 30, Hebrides*. QinetiQ Proprietary, Unpublished.

Weick, K. E. (1987) Organisational culture as a source of high reliability. *California Management Review.* Vol. 29(2), pp112-127.

Weinberg, G. (1975) *An Introduction to General Systems Thinking*. John Wiley & Sons, New York, USA.

Wilde, G. (1994) *Target Risk.* Ontario; PDS Publications, http://pavlov.psyc.queensu.ca /target. (21/10/2008).

Wilkinson, P. (2002) *Safety Cases: Success or Failure?* Seminar Paper 2, National Research Centre for OHS Regulation, The Australian National University, Australia.

Williams, K. W. (2004) *A Summary of Unmanned Aircraft Accident/Incident data: Human Factors Implications*. Technical Report No. DOT/FAA/AM-04/24. Washington, DC: US Department of Transportation, Federal Aviation Administration, Office of Aerospace Medicine, USA.

Williamson, A. M., Feyer, A., Cairns, D. & Biancotti, D. (1997) The development of a measure of safety climate: The role of safety perceptions and attitudes. *Safety Science.* Vol. 25. pp5-27.

Wilson, S. P., Kelly, T. P. & McDermid, J. A. (1995) *Safety Case Development: Current Practice, Future Prospects*. Paper issued by HISE Group, Department of Computer Science, University of York, UK.

Zhou, X. and Weaver, R. (2003) *Improving the Efficiency of Safety Case Development in the Railway Industry - A Feasibility Study*. Rail Safety & Standards Board, 2003.

Zohar, D. (1980) Promoting increased use of ear protectors in noise through information feedback. *Human Factors*. Vol. 22. pp69-79.

BIBLIOGRAPHY

Adams, A. A. & McCrindle, R. J. (2008) *Pandora's Box: Social & Professional Issues of the Information Age*. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, England, 1st edition.

Allan, J. (2002) *Guidance For Applying Cost Benefit Analysis To Safety Decisions In Aviation Projects*. ALTG-ADRP1, MoD Abbey Wood, Bristol, (Loose paper - Unpublished).

Boeing 2707 (2009) *Boeing 2707 SST*. www.Globalsecurity.org/military/systems/aircraft/b2707.htm (18/07/2009).

Bowles, D. S. (2003) *ALARP Evaluation: Using Cost Effectiveness and Disproportionality to Justify Risk Reduction*. Australian National Committee On Large Dams (ANCOLD), Conference on Dams.

Bowman, C. (1998) *Strategy in Practice*. Pearson Education Ltd, Edinburgh Gate, Harlow, Essex, England, 1st edition.

Burns, B. (2004) *Managing Change*. Pearson Education Ltd, Edinburgh Gate, Harlow, Essex, England, 4th edition.

CAA (2002) *Human Factors in Aircraft Maintenance and Inspection*. Civil Air Publication (CAP) 718, Human Factors, Aerodrome, Air Traffic and Licensing Standards Division, Safety Regulatory Group (SRG), Civil Aviation Authority, UK.

Casarosa, C., Galatolo, R., Mengali, G. & Quarta, A. (2004) *Impact of Safety Requirements on the weight of civil unmanned aerial vehicles*. Aircraft Engineering and Aerospace Technology, Vol. 76, No.6, pp.600-606.

Clothier, R., Walker, R., Fulton, N. & Campbell, D. (2007) *A Casualty Risk Analysis for Unmanned Aerial Systems (UAS) Operations over Inhabited Areas*. 12th Australian International Aerospace Congress, 2nd Australasian Unmanned Air Vehicles Conference, 19-22 March, 2007.

Dilthey, W. (2002) *The Formation of the Historical World in the Human Sciences.* Editors; R.A., Makkreel, & Frithjof, R., Princeton University Press, New Jersey, USA.

Dilthey, W. (1996) *Hermeneutics and the Study of History*. Editors; R.A., Makkreel, & Frithjof, R., Princeton University Press, New Jersey, USA.

Eichblatt, E. J. (1989) *Test and Evaluation of the Tactical Missile.* Progress in Astronautics and Aeronautics, Volume 119, American Institute of Aeronautics and Astronautics, Inc., 370 L'Enfant Promenade, SW, Washington, DC, 20024-2518, USA.

Evans, A. W. (2005) *Safety Appraisal Criteria*. The Royal Academy of Engineering and Lloyd's Register Lecture on Risk Management, Lloyd's Register Professor of Transport Risk Management, Imperial College London, 14th April, 2005.

Fleeman, E. L. (2001) *Tactical Missile Design*. American Institute of Aeronautics and Astronautics, Inc., Reston, Virginia, USA.

FSF (2005) *See What's Sharing Your Airspace*. Flight Safety Foundation, Flight Safety Digest, Vol. 24, No. 5, May 2005.

Gadamer, H-G. (1976) *Philosophical Hermeneutics*. Translation; Linge, D.E., California University Press, Berkley, USA.

Garnell, P. (1980) *Guided Weapon Control Systems*. 2nd edition, Pergamon Press Ltd, Headington Hill Hall, Oxford, England, UK.

Hamilton, A. (2001) *Managing Projects for Success; a trilogy*. 1st edition, Thomas Telford Publishing Ltd, 1 Heron Quay, London, England, UK.

Hemsch, J. M. (1992) *Tactical Missile Aerodynamics: General Topics*. Progress in Astronautics and Aeronautics, Volume 141, American Institute of Aeronautics and Astronautics, Inc., 370 L'Enfant Promenade, SW, Washington, DC, 20024-2518, USA.

Hodges, H. A. (1952) *The Philosophy of Wilhelm Dilthey*. Routledge & Kegan Paul Ltd, Broadway House, 68-74 Carter Lane, London, UK.

HSE (2007) *Managing competence for safety-related systems: Part 1 - Key Guidance*. Health and Safety Executive, London, HMSO.

IET (2009) *Safety Audits*. Health & Safety Briefing No. 25, April 2009, The Institution of Engineering and Technology (IET), Michael Faraday House, Six Hills Way, Stevenage, SG1 2AY.

Kennedy, R & Kirwan, B. (1998) Development of a Hazard and Operability-based method for identifying safety management vulnerabilities in high risk systems. *Safety Science.* Vol. 30, pp249-274.

Lee, R. G., Garland-Collins, T. K., Johnson, D. E., Archer, E., Sparkes, C., Moss, G. M. & Mowat, A. W. (1988) *Guided Weapons*. Brassey's Defence Publishers Ltd, 24 Gray's Inn Road, London, England, UK.

Mullins, L. J. (2007) *Management & Organisational Behaviour*. 8th edition, Pearson Education Ltd, Edinburgh Gate, Harlow, Essex, England, UK.

Peebles, L., Wearing, S. & Heasman, T. (2005) *Identifying Human Factors Associated with Slip and Trip Accidents*. Research Report No. 382, Report prepared by System Concepts for the Health & Safety Executive (HSE).

Pettersen, K. A. & Aase, K. (2008) Explaining safe work practices in aviation line maintenance. *Safety Science*. Vol.46, pp.510-519.

Quintana, E. (2009) *The Ethics and Legal Implications of Military Unmanned Vehicles*. Occasional Paper, Head of Military Technology and Information Studies, Royal United Services Institute for Defence and Security Studies.

Reynolds, M. T. (1996) *Test & Evaluation of Complex Systems*. 1st edition, John Wiley & Sons Ltd, Baffins Lane, Chichester, England, UK.

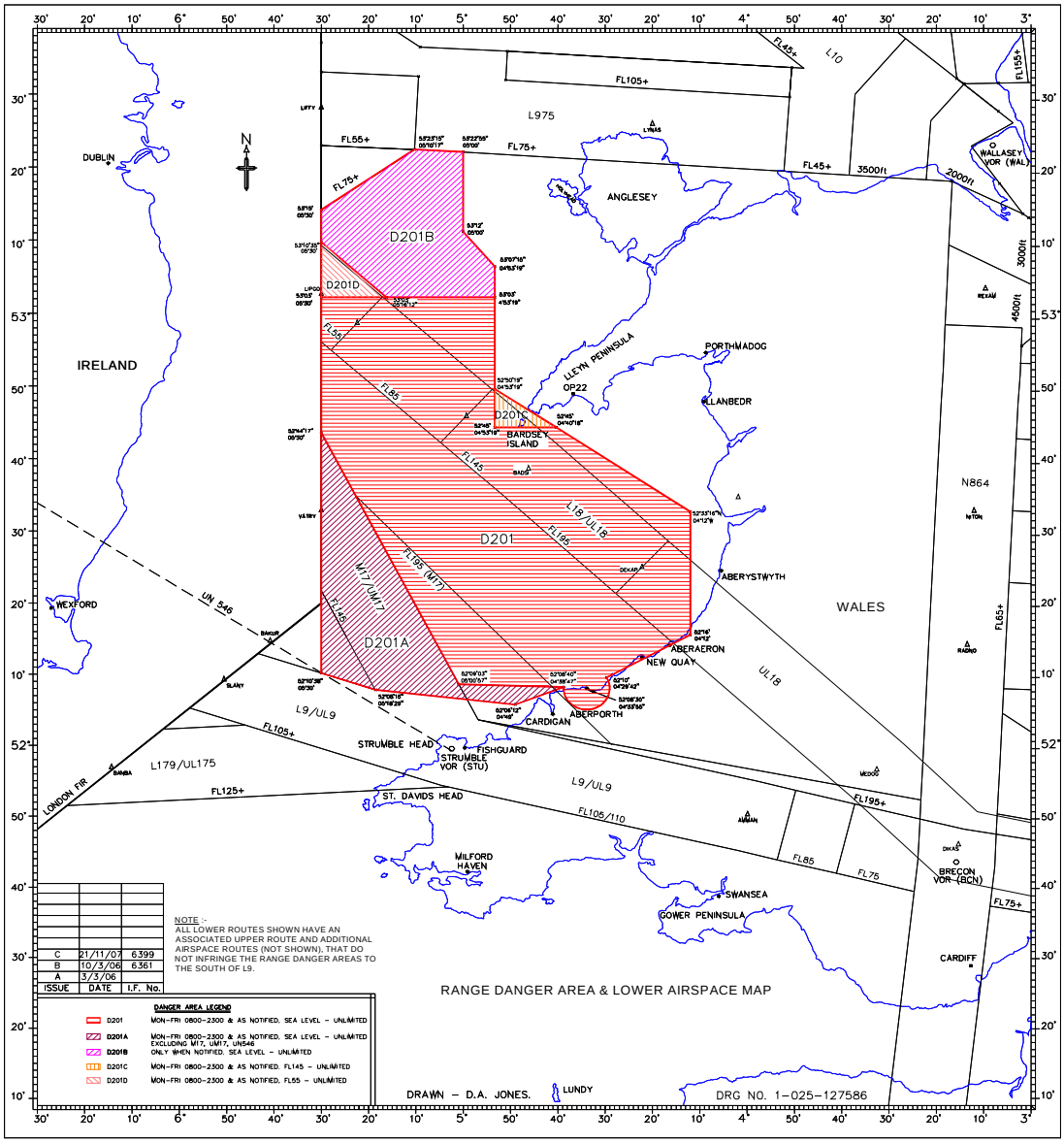
Ricoeur, P. (1974) *The Conflicts of Interpretation: Essays in Hermeneutics*. Translation; Domingo, *et al*, Northwestern University Press, Evanston.

Weibel, R. E. & Hansman, R. J. (2005) *Safety Considerations for Operation of Unmanned Aerial Vehicles in the National Airspace System*. MIT International Center for Air Transportation, Department of Aeronautics & Astronautics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA. Report No. ICAT-2005-1.

Whittaker, C. (2003) *Aircraft Airworthiness Standards for Civil Unmanned Vehicle Systems*. A report issued by the Civil Aviation Authority (CAA) - Safety Regulation Group (SRG), 2nd September, 2003.

APPENDIX A

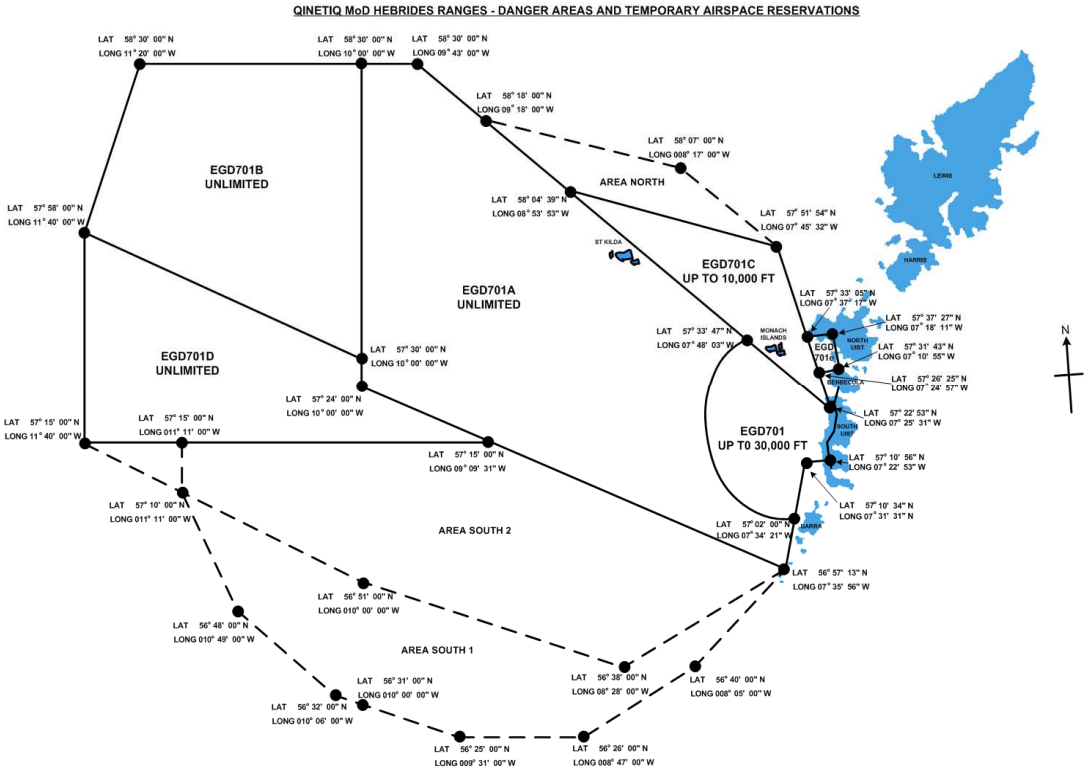
Geographical layout of MoD Aberporth Range Danger Area.



This page left intentionally blank.

APPENDIX B

Geographical layout of MoD Hebrides Range Danger Area



This page left intentionally blank.

APPENDIX C

Regulatory & Statutory Documentation for MoD Air Ranges

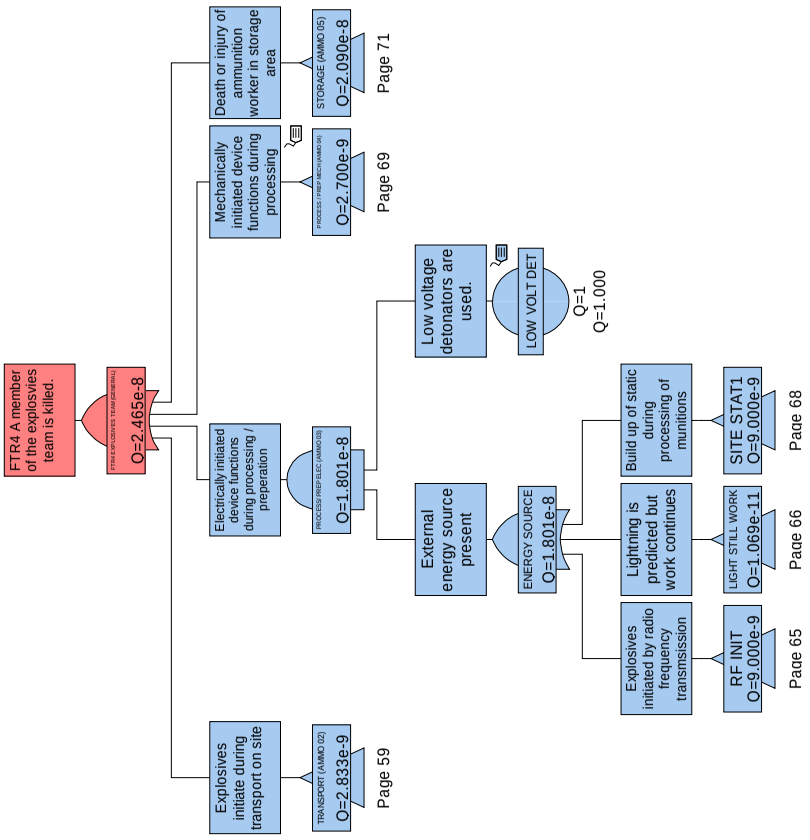
Regulatory Document/Protocol	Descriptor
Joint Services Publication 550 Series.	Military Aviation Regulatory Group. (Edition 1, Issue 5, 1st Nov 06)
Joint Services Publication 403.	Handbook of Defence Land Ranges Safety.
Defence Standard 00-56 (Interim) Parts 1 & 2	Safety Management Requirements for Defence Systems 2004.
Range Standing Orders for the Conduct of Trials.	MOD Aberporth and MOD Hebrides operational documentation.
Manual of Air Traffic Services. Including TESD Air Traffic Control Instructions	MATS Parts 1 & 2 NATS Aberporth and NATS Hebrides operational documentation.
Test & Evaluation Support Division (TESD) Airfields and Ranges (A&R).	MOD Regulator and Airspace sponsor, T&E Operations.
Defence Ordnance Safety Group (DOSG)	MOD Safety Regulator.
Joint Services Publication 440 & 480	Security Configuration & Installation Design Authority (SCIDA), MOD compliance management.
Civil Aviation Authority (CAA)	Specifically Safety Regulatory Group (SRG).
Hazardous Activity Scrutiny Panel (HASP)	QinetiQ internal safety review panel
Civil Aviation Publication (CAP) 670 (Issue 2 inc. amendments 2006)	Air Traffic System (ATS) Safety Requirements.
Civil Aviation Publication (CAP) 722 (Issue 1 inc. amendments 2004)	Unmanned Aerial Vehicle Operations in UK Airspace – CAA guidance.

(Non-exhaustive)

This page left intentionally blank

APPENDIX D

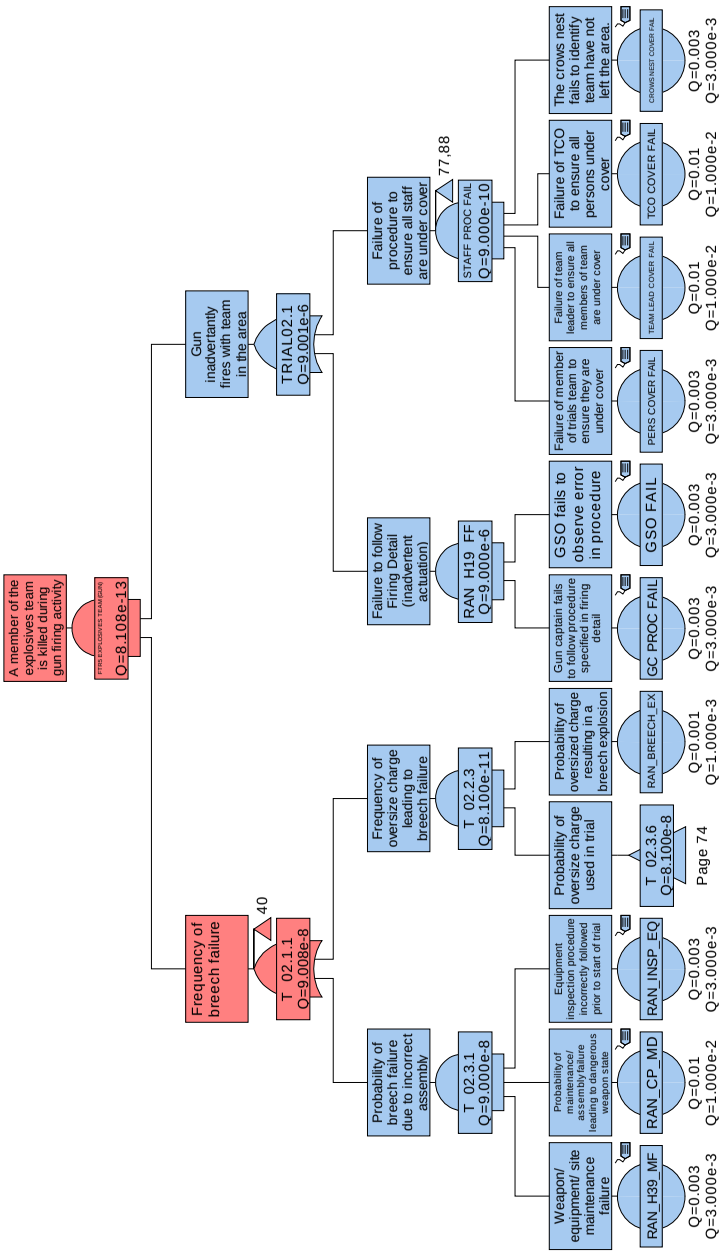
Storage, Transport & Preparation (FTR4)



This page left intentionally blank.

APPENDIX E

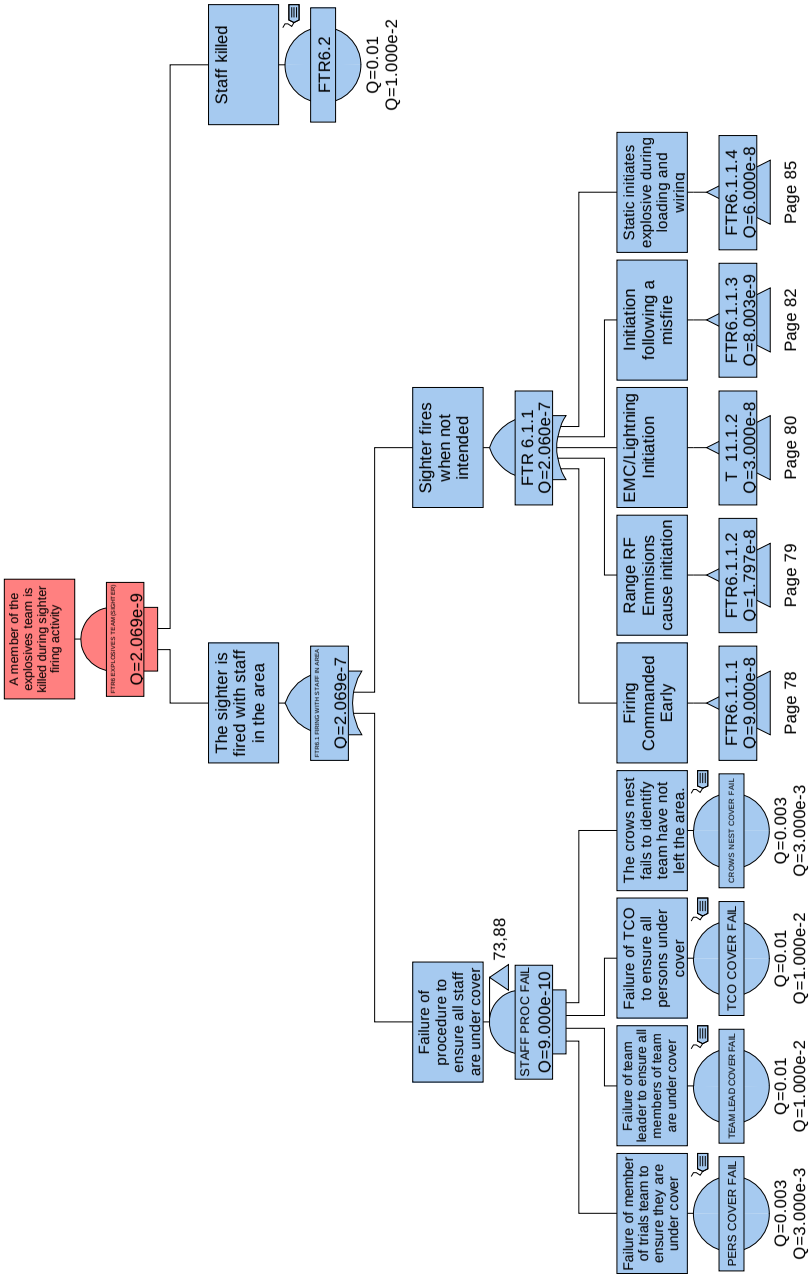
Gun Firing (FTR 5)



This page left intentionally blank.

APPENDIX F

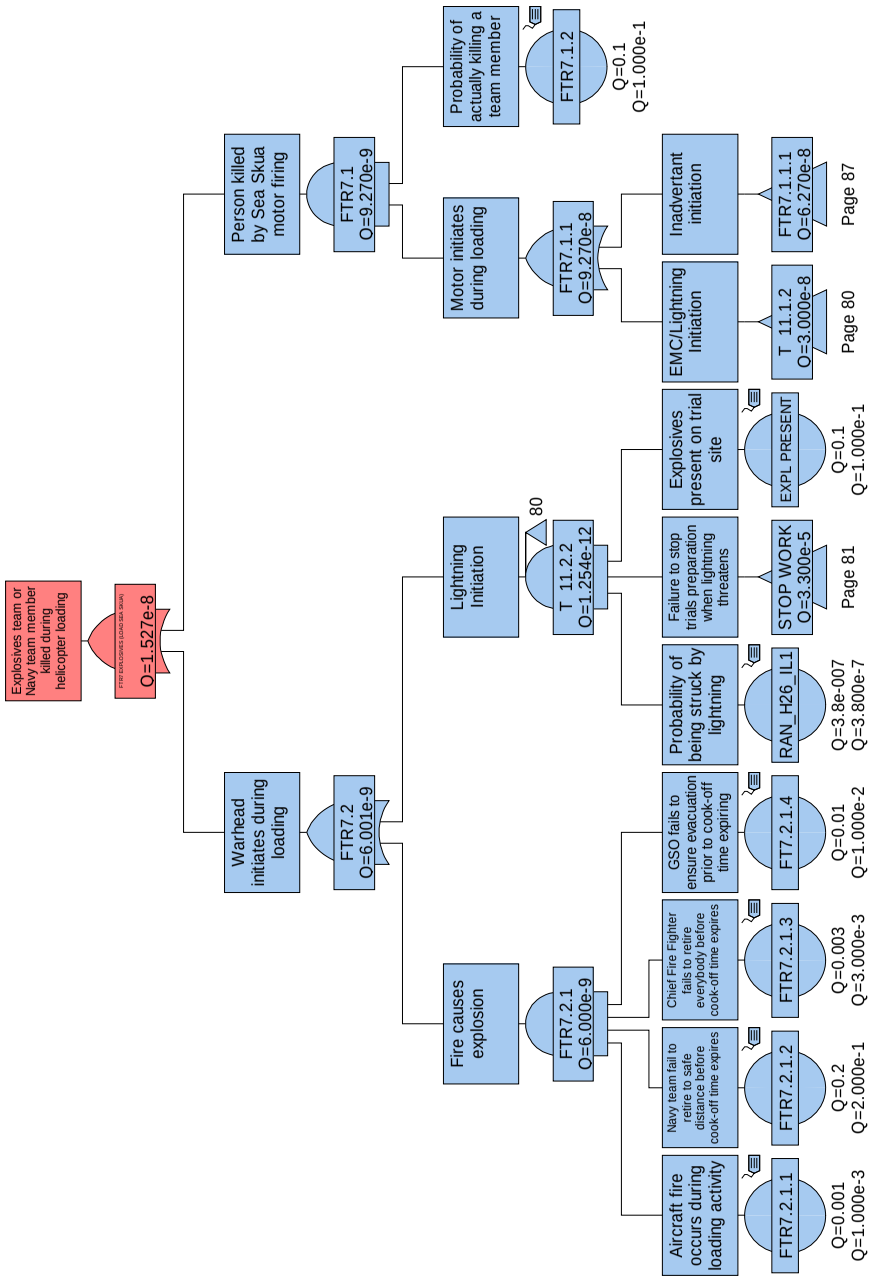
Sighter Rocket Firing (FTR 6)



This page left intentionally blank.

APPENDIX G

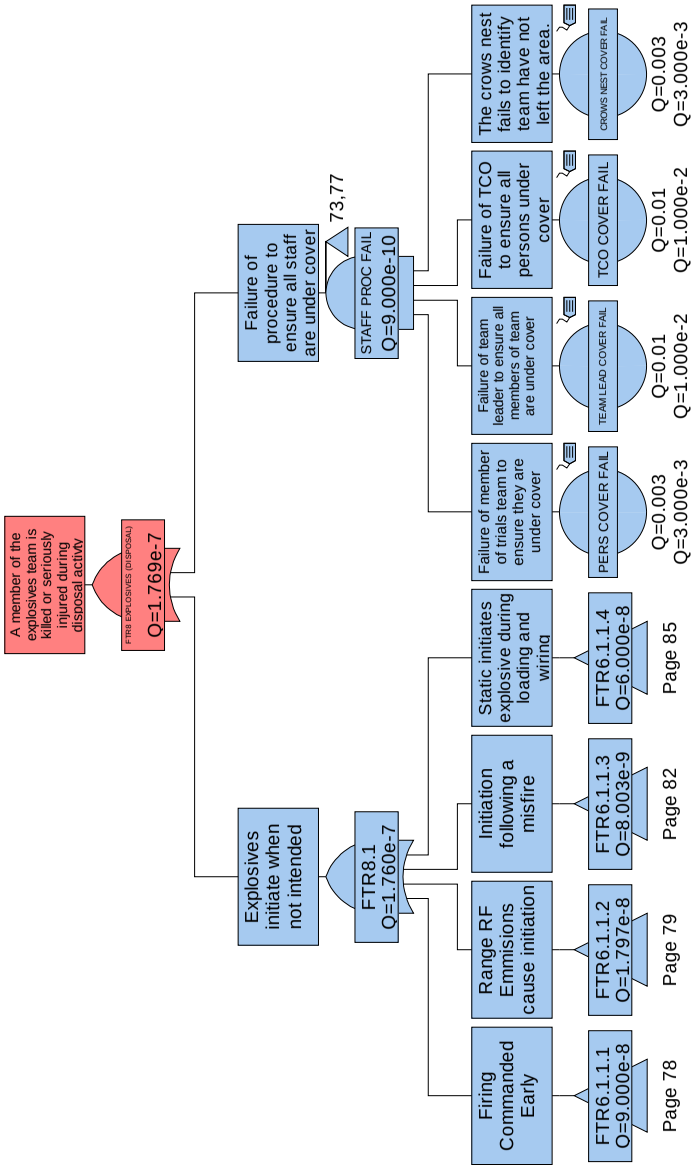
Sea Skua Missile Loading (FTR 07)



This page left intentionally blank.

APPENDIX H

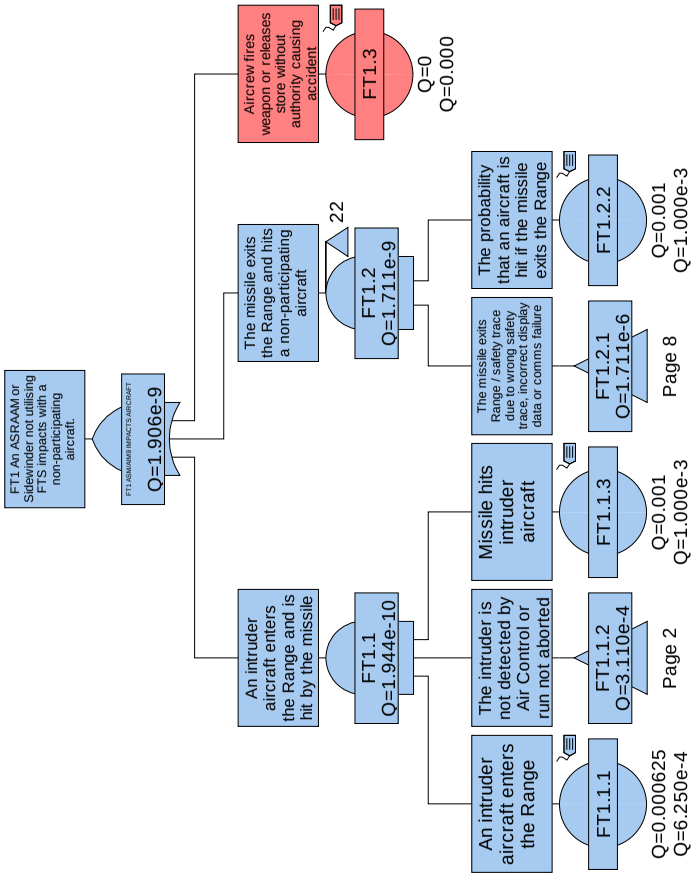
Disposal of unspent OME (FTR 08)



This page left intentionally blank.

APPENDIX I

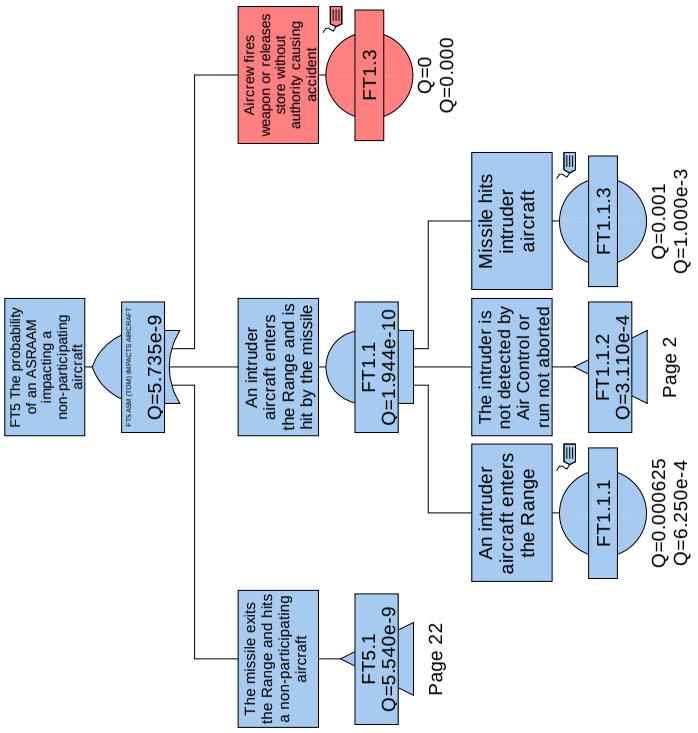
ASRAAM OM / *Sidewinder* AIM 9 strike (FT 01)



This page left intentionally blank.

APPENDIX J

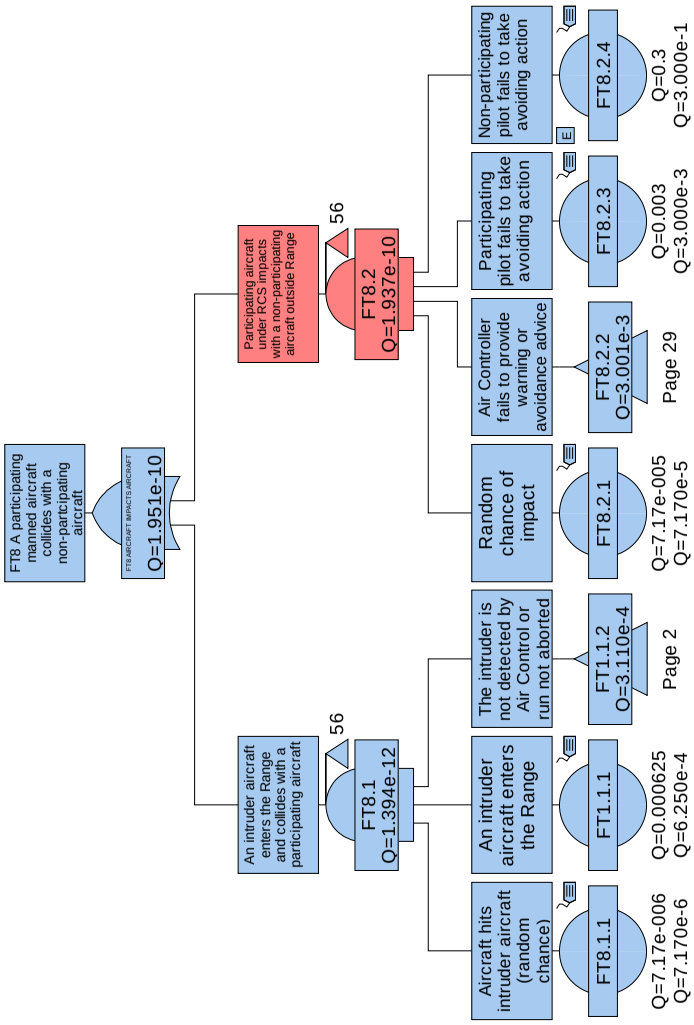
ASRAAM TOM strike (FT 05)



This page left intentionally blank.

APPENDIX K

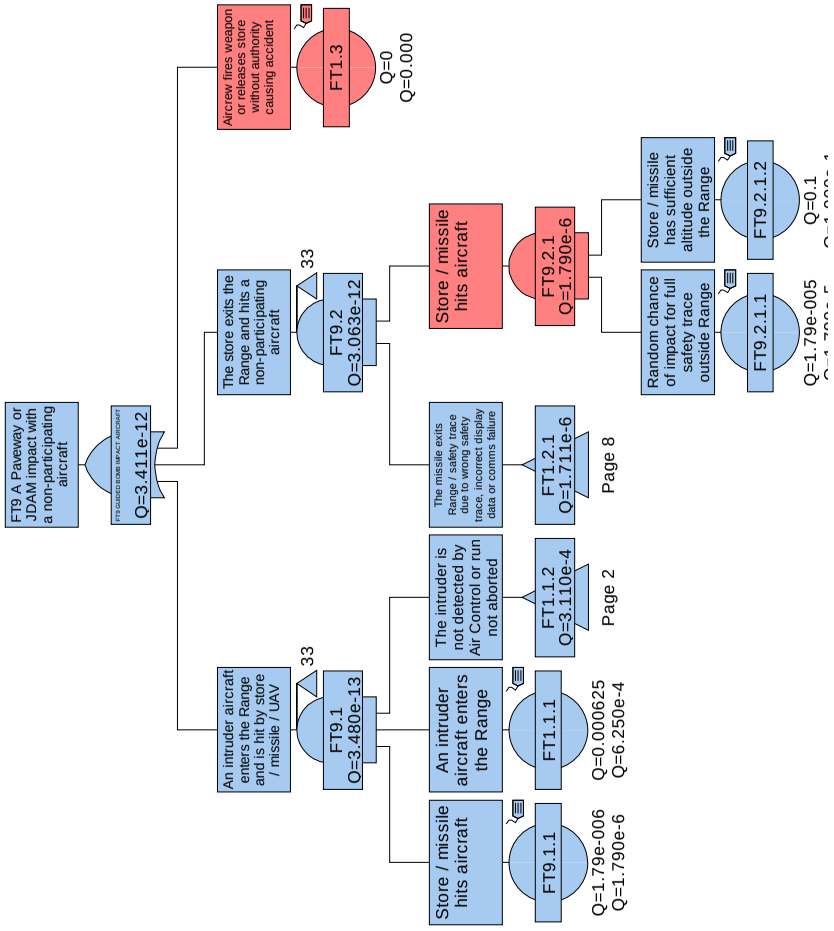
Non-participative aircraft collision (FT 08)



This page left intentionally blank.

APPENDIX L

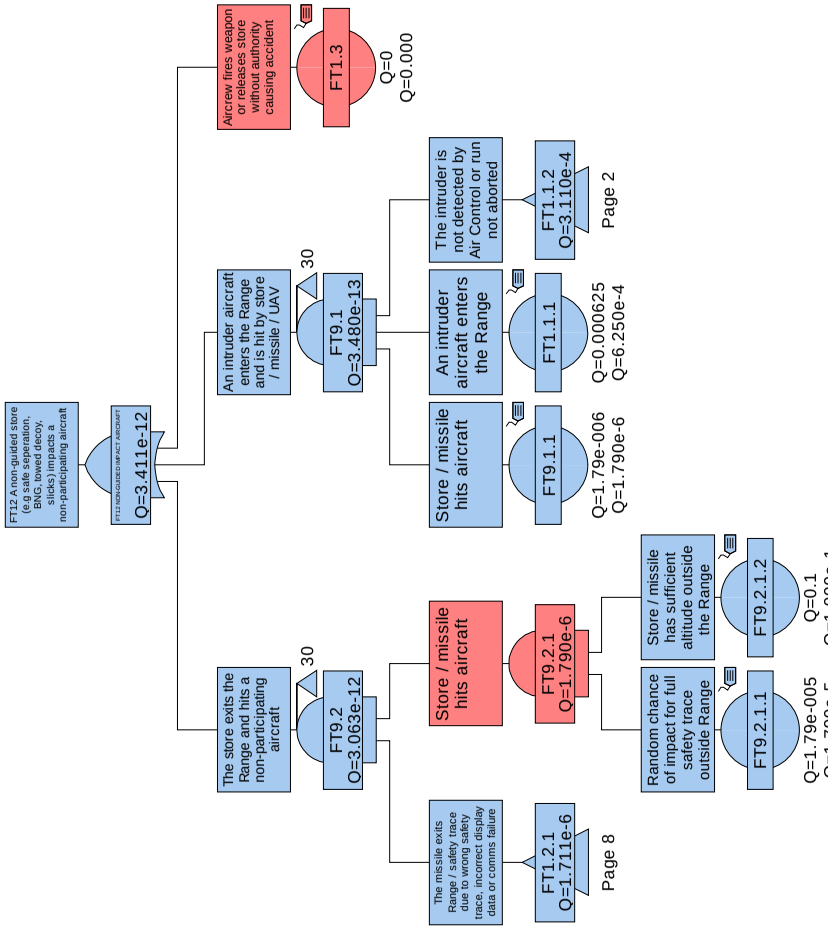
LGB / JDAM strike (FT 09)



This page left intentionally blank.

APPENDIX M

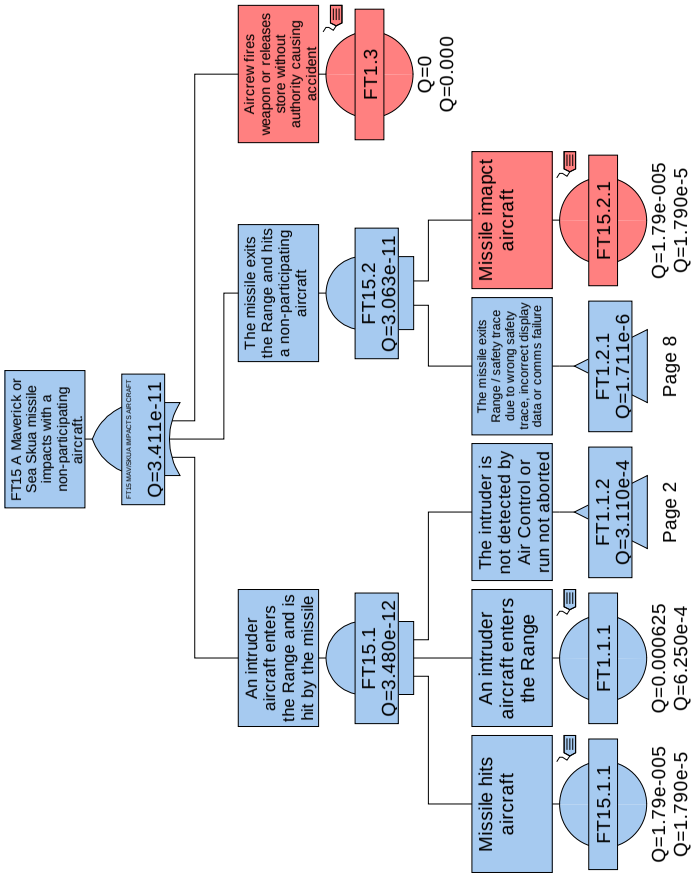
Non-guided store strike (FT 12)



This page left intentionally blank.

APPENDIX N

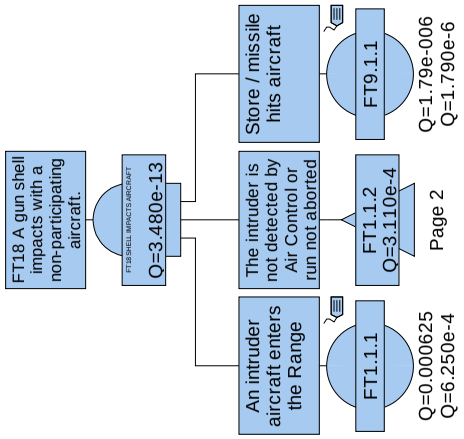
Maverick / Sea Skua strike (FT 15)



This page left intentionally blank.

APPENDIX O

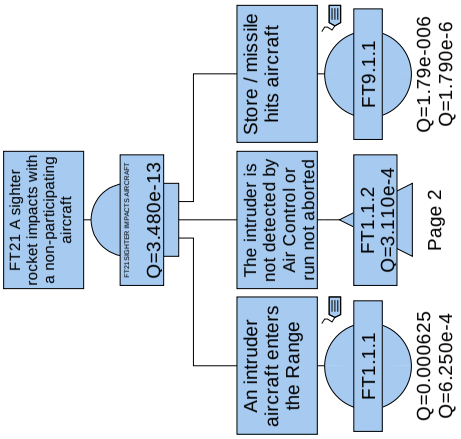
Rangehead Gun Firing (AS90 strike) (FT 18)



This page left intentionally blank.

APPENDIX P

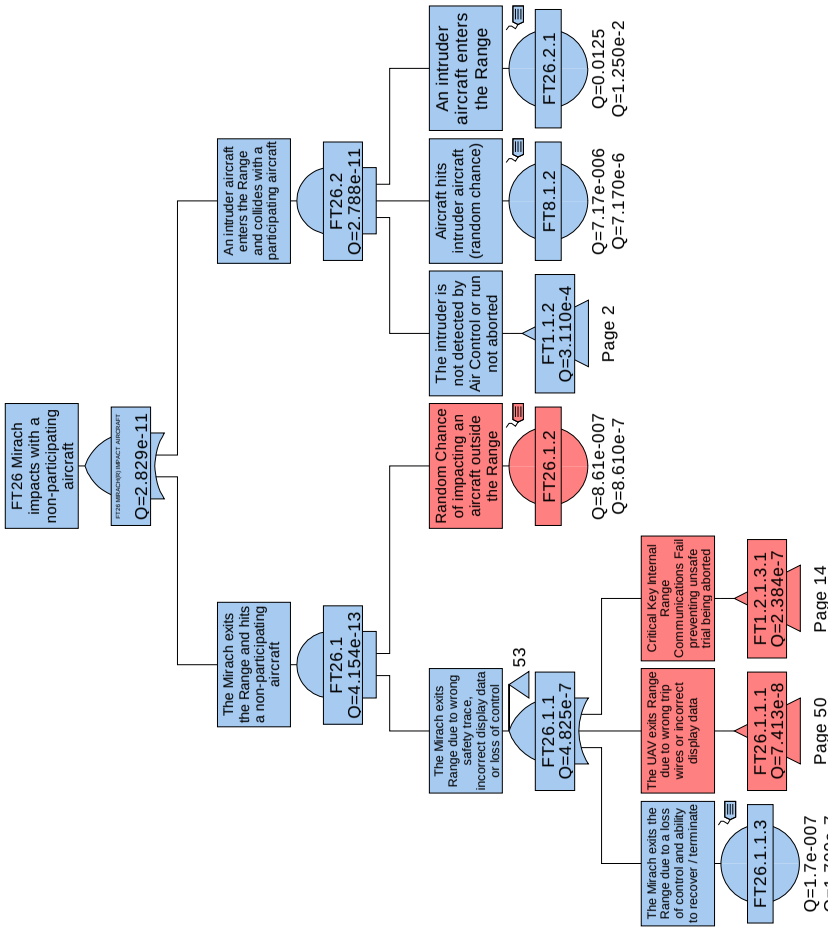
Sighter Rocket strike (FT 21)



This page left intentionally blank.

APPENDIX Q

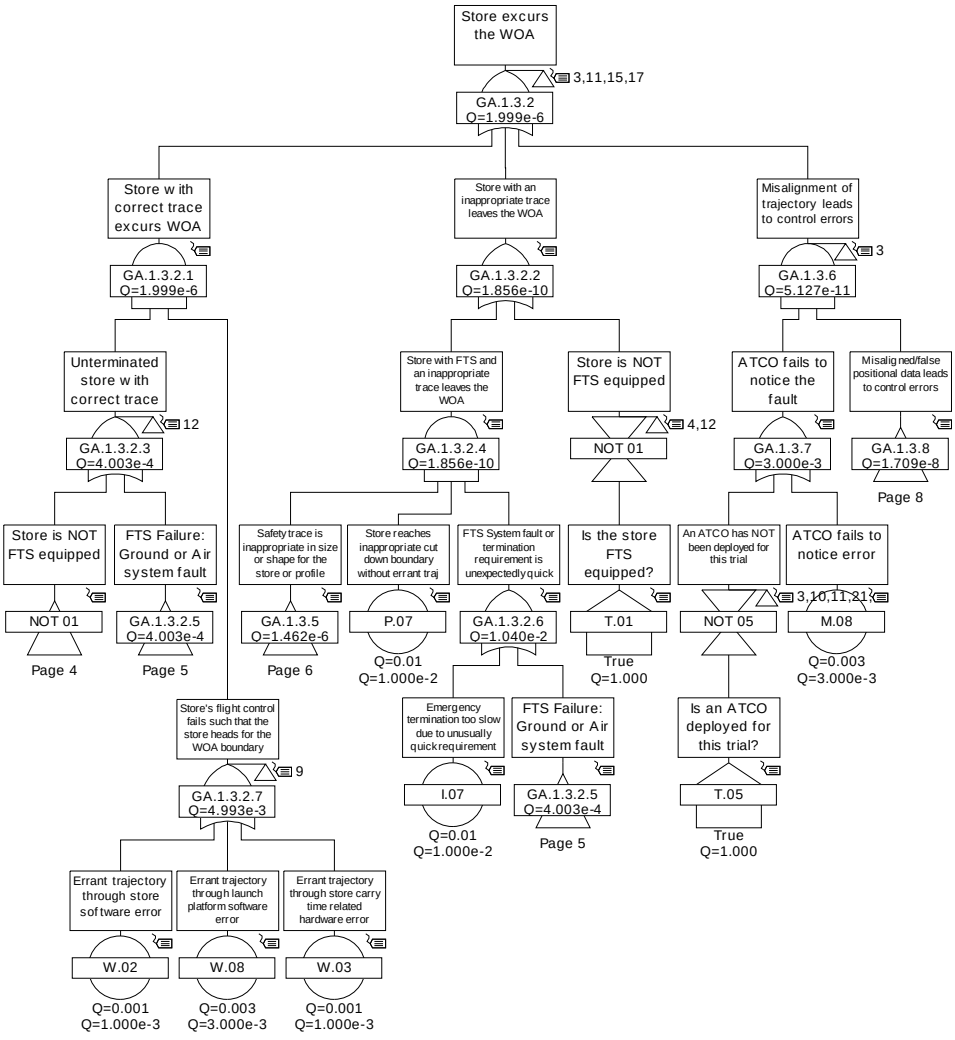
Mirach UAV strike (FT 26)



This page left intentionally blank.

APPENDIX R

Store Breaches the Weapon Operating Boundary (FT B3)



This page left intentionally blank.

APPENDIX S

Competence & Professional Standing of the O&STWG

The Operations and Trials Safety Working Group is primarily assembled from the Operations Controllers (OCs) and the Trial Safety Managers (TSMs) from across the four QinetiQ operated Test & Evaluation (T&E) Air Ranges. Together with representation from the QinetiQ's Combined Aerial Target Service (CATS) the aforementioned form the working group's quorum whilst other Subject Matter Experts (SMEs) are drawn in to enhance its technical abilities on a case-by-case basis. This forum is acknowledged by MoD regulators outside the company as the single and critical mass of competency in Air Range activities within the United Kingdom (UK). Within the company the working group is acknowledged by engineering and technical directors, including other divisions, as the single source of expertise in Air Range activities. The forum gives collective advice to internal projects upon various activities, including peer reviewing of safety cases and safety related activities. The following text attempts to qualify the forum's competence and professional standing within the environment of T&E, including UAV operations.

Experience within the O&STWG.

The working group has a vast amount of experience within the field of T&E. With a typical, collective, annual number of sorties approaching 800 per year across the four sites, combined with individual experiences in T&E approaching 30 years for some members, the forum can claim to have been involved in the planning and execution of over 125,000 T&E trials sorties. From a domain perspective these experiences include, but are not limited to;

- Air to Air activities. (e.g. live and inert weapon releases, combat manoeuvring, etc.)
- Air to Surface activities. (e.g. live and inert weapon releases, platform drops, safe separation trials, special forces equipment releases, etc.)
- Surface to Air activities. (e.g. live and inert weapon, UAV and rocket launches, etc.)
- Surface to Surface activities. (e.g. live and inert weapon releases, etc.)

- Non release activities. (e.g. commercial airline height monitoring, laser designator qualifying and integration trials, satellite tracking, UAV qualifying trials, missile approach warner system qualifying, etc.)

Professional Status and Formal Qualifications within the O&STWG.

The O&STWG consists of individuals who are members of professional institutions and who also hold an array of T&E, engineering and safety related qualifications. In all cases, basic qualifications are heavily augmented by attendance at specialised courses including, but not limited to, tracking and surveillance radar, laser safety, guided weapons, ballistic weapons, explosive safety, radio communication, UAVs, UCAVs and flight termination systems. Many are recognised as leading authorities within the UK's T&E environment.

The table overleaf records the experience, professional status and qualifications of the group. A glossary of professional membership is attached below.

Glossary of Professional Membership within the O&STWG.

APM	Association for Project Management.
CMI	Chartered Management Institute.
IEMA	Institute of Environmental Management & Assessment.
IET	Institution of Engineering & Technology.
INCOSE	International Council on Systems Engineering.
Inst.LM	Institute of Leadership & Management.
IOSH	Institution of Occupational Safety & Health.
RAeS	Royal Aeronautical Society.

Experience, Professional Status and Qualifications of the O&STWG.				
Member	Qualifications	Experience within T&E/ Aerospace	Safety/ Operational Specialist	Professional Membership/Status
A	HNC Mechanical Engineering with Aerospace. Diploma in HS&E	35 years	Yes	MIOSH AIEMA
B	BSc (Biology). Numerous Biochemistry and Nuclear courses.	18 years (+8years Nuclear commissioning RSA & USA)	Yes	MAPM
C	C&G Electronics	35 years	Yes	Nil
D	HNC & BSc Electronics. Part MSc Systems Engineering	5 years	Yes	MIET, INCOSE.
E	C&G (Engineering), Army Aviation, Systems Auditor (various.).	39 years	Yes	MInst.LM, MIET.
F	HNC & BSc Electronics	11 years	Yes	MIET, CMI.
G	C&G (Telecoms)	30 years	Yes	Aff.CMI
H	BA, BSc(Hons), MSc (Safety Engineering)	27 years	Yes	MIOSH, MRAeS.
I	RAF Radar Systems Eng.	34 years	No	FRAeS, MIET, CMI.
J	BA, BSc(Hons), MSc (Safety Engineering)	35 years	Yes	MIET, MRAeS.
K	HNC Electronics. MSc (HS&E Management)	20 years	Yes	Grad.IOSH, AIEMA.
L	HNC Aero Engineering	30 years	No	MAPM
M	Secondary School Education, Qualified Aircraft dispatcher.	23 years	No	MIOSH
N	IOSH Cert.	21 years	Yes	MAPM

This page left intentionally blank.

This page left intentionally blank.

This final page left intentionally blank.