

Failure in Safety-Critical Systems:

A HANDBOOK OF INCIDENT AND ACCIDENT
REPORTING

Chris Johnson

Glasgow University Press

Glasgow University Press,

Publicity Services,
No. 2 The Square,
University of Glasgow,
Glasgow, G12 8QQ,
Scotland.

Copyright ©2003 by C.W. Johnson.

All rights reserved. No part of this manuscript may be reproduced in any form, by photostat, microform, retrieval system, or any other means without the prior written permission of the author.

First printed October 2003.

ISBN 0-85261-784-4.

Contents

1	Abnormal Incidents	1
1.1	The Hazards	2
1.1.1	The Likelihood of Injury and Disease	6
1.1.2	The Costs of Failure	8
1.2	Social and Organisational Influences	9
1.2.1	Normal Accidents?	10
1.2.2	The Culture of Incident Reporting	11
1.3	Summary	19
2	Motivations for Incident Reporting	21
2.1	Why Bother With Incident Reporting?	21
2.1.1	The Strengths of Incident Reporting	21
2.1.2	The Weaknesses of Incident Reporting	25
2.2	Different Forms of Reporting Systems	29
2.2.1	Open, Confidential or Anonymous?	29
2.2.2	Scope and Level	37
2.3	Summary	43
3	Sources of Failure	45
3.1	Regulatory Failures	46
3.1.1	Incident Reporting to Inform Regulatory Intervention	47
3.1.2	The (Continuing) Problems of Regulation	47
3.2	Managerial Failures	49
3.2.1	Latent and Catalytic Failures	50
3.2.2	Incident Reporting and Safety Management Systems	50
3.3	Hardware Failures	52
3.3.1	Acquisition and Maintenance Effects on Incident Reporting	53
3.3.2	Source, Duration and Extent	54
3.4	Software Failures	57
3.4.1	Failure Throughout the Lifecycle	58
3.4.2	Problems in Forensic Software Engineering	62
3.5	Human Failures	64
3.5.1	Individual Characteristics and Performance Shaping Factors	64
3.5.2	Slips, Lapses and Mistakes	73
3.6	Team Factors	76
3.6.1	Common Ground and Group Communication	79
3.6.2	Situation Awareness and Crew Resource Management	82
3.7	Summary	85

4	The Anatomy of Incident Reporting	89
4.1	Different Roles	90
4.1.1	Reporters	90
4.1.2	Initial Receivers	93
4.1.3	Incident Investigators	96
4.1.4	Safety Managers	98
4.1.5	Regulators	100
4.2	Different Anatomies	104
4.2.1	Simple Monitoring Architectures	104
4.2.2	Regulated Monitoring Architectures	105
4.2.3	Local Oversight Architectures	106
4.2.4	Gatekeeper Architecture	107
4.2.5	Devolved Architecture	108
4.3	Summary	109
5	Detection and Notification	111
5.1	‘Incident Starvation’ and the Problems of Under-Reporting	112
5.1.1	Reporting Bias	113
5.1.2	Mandatory Reporting	115
5.1.3	Special Initiatives	117
5.2	Encouraging the Detection of Incidents	119
5.2.1	Automated Detection	119
5.2.2	Manual Detection	127
5.3	Form Contents	135
5.3.1	Sample Incident Reporting Forms	136
5.3.2	Providing Information to the Respondents	138
5.3.3	Eliciting Information from Respondents	142
5.4	Summary	145
6	Primary Response	147
6.1	Safeguarding the System	151
6.1.1	First, Do No Harm	151
6.1.2	Incident and Emergency Management	155
6.2	Acquiring Evidence	157
6.2.1	Automated Logs and Physical Evidence	157
6.2.2	Eye-Witness Statements	161
6.3	Drafting A Preliminary Report	173
6.3.1	Organisational and Managerial Barriers	173
6.3.2	Technological Support	175
6.3.3	Links to Subsequent Analysis	176
6.4	Summary	179
7	Secondary Investigation	181
7.1	Gathering Evidence about Causation	184
7.1.1	Framing an Investigation	184
7.1.2	Commissioning Expert Witnesses	189
7.1.3	Replaying Automated Logs	194
7.2	Gathering Evidence about Consequences	200
7.2.1	Tracing Immediate and Long-Term Effects	201
7.2.2	Detecting Mitigating Factors	204
7.2.3	Identifying Related Incidents	207
7.3	Summary	210

8	Computer-Based Simulation	213
8.1	Why Bother with Reconstruction?	213
8.1.1	Coordination	218
8.1.2	Generalisation	220
8.1.3	Resolving Ambiguity	222
8.2	Types of Simulation	226
8.2.1	Declarative Simulations	228
8.2.2	Animated Simulations	234
8.2.3	Subjunctive Simulations	241
8.2.4	Hybrid Simulations	254
8.3	Summary	257
9	Modelling Notations	261
9.1	Reconstruction Techniques	261
9.1.1	Graphical Time Lines	262
9.1.2	Fault Trees	266
9.1.3	Petri Nets	284
9.1.4	Logic	297
9.2	Requirements for Reconstructive Modelling	314
9.2.1	Usability	314
9.2.2	Expressiveness	322
9.3	Summary	339
10	Causal Analysis	341
10.1	Introduction	341
10.1.1	Why Bother With Causal Analysis?	342
10.1.2	Potential Pitfalls	345
10.1.3	Loss of the Mars Climate Orbiter & Polar Lander	349
10.2	Stage 1: Incident Modelling (Revisited)	352
10.2.1	Events and Causal Factor Charting	353
10.2.2	Barrier Analysis	358
10.2.3	Change Analysis	371
10.3	Stage 2: Causal Analysis	389
10.3.1	Causal Factors Analysis	389
10.3.2	Cause and Contextual Summaries	397
10.3.3	Tier Analysis	405
10.3.4	Non-Compliance Analysis	416
10.4	Summary	421
11	Alternative Causal Analysis Techniques	437
11.1	Event-Based Approaches	438
11.1.1	Multilinear Events Sequencing (MES)	438
11.1.2	Sequentially Timed and Events Plotting (STEP)	447
11.2	Check-List Approaches	455
11.2.1	Management Oversight and Risk Tree (MORT)	455
11.2.2	Prevention and Recovery Information System for Monitoring and Analysis (PRISMA)	469
11.2.3	Tripod	479
11.3	Mathematical Models of Causation	487
11.3.1	Why-Because Analysis (WBA)	487
11.3.2	Partition Models for Probabilistic Causation	501
11.3.3	Bayesian Approaches to Probabilistic Causation	507
11.4	Comparisons	513
11.4.1	Bottom-Up Case Studies	515

11.4.2	Top-Down Criteria	518
11.4.3	Experiments into Domain Experts' Subjective Responses	527
11.4.4	Experimental Applications of Causal Analysis Techniques	530
11.5	Summary	537
12	Recommendations	541
12.1	From Causal Findings to Recommendations	541
12.1.1	Requirements for Causal Findings	543
12.1.2	Scoping Recommendations	546
12.1.3	Conflicting Recommendations	558
12.2	Recommendation Techniques	568
12.2.1	The 'Perfectability' Approach	571
12.2.2	Heuristics	576
12.2.3	Enumerations and Recommendation Matrices	579
12.2.4	Generic Accident Prevention Models	590
12.2.5	Risk Assessment Techniques	596
12.3	Process Issues	605
12.3.1	Documentation	605
12.3.2	Validation	609
12.3.3	Implementation	616
12.3.4	Tracking	619
12.4	Summary	623
13	Feedback and the Presentation of Incident Reports	625
13.1	The Challenges of Reporting Adverse Occurrences	625
13.1.1	Different Reports for Different Incidents	626
13.1.2	Different Reports for Different Audiences	629
13.1.3	Confidentiality, Trust and the Media	632
13.2	Guidelines for the Presentation of Incident Reports	641
13.2.1	Reconstruction	641
13.2.2	Analysis	655
13.2.3	Recommendations	667
13.3	Quality Assurance	679
13.3.1	Verification	679
13.3.2	Validation	697
13.4	Electronic Presentation Techniques	704
13.4.1	Limitations of Existing Approaches to Web-Based Reports	706
13.4.2	Using Computer Simulations as an Interface to On-Line Accident Reports	708
13.4.3	Using Time-lines as an Interface to Accident Reports	710
13.5	Summary	713
14	Dissemination	717
14.1	Problems of Dissemination	717
14.1.1	Number and Range of Reports Published	717
14.1.2	Tight Deadlines and Limited Resources	719
14.1.3	Reaching the Intended Readership	721
14.2	From Manual to Electronic Dissemination	725
14.2.1	Anecdotes, Internet Rumours and Broadcast Media	725
14.2.2	Paper documents	729
14.2.3	Fax and Telephone Notification	734
14.3	Computer-Based Dissemination	735
14.3.1	Infrastructure Issues	736
14.3.2	Access Control	747
14.3.3	Security and Encryption	748

14.3.4	Accessibility	751
14.4	Computer-Based Search and Retrieval	752
14.4.1	Relational Data Bases	754
14.4.2	Lexical Information Retrieval	774
14.4.3	Case Based Retrieval	786
14.5	Summary	796
15	Monitoring	801
15.1	Outcome Measures	817
15.1.1	Direct Feedback: Incident and Reporting Rates	818
15.1.2	Indirect Feedback: Training and Operations	823
15.1.3	Feed-forward: Risk Assessment and Systems Development	826
15.2	Process Measures	832
15.2.1	Submission Rates and Reporting Costs	832
15.2.2	Investigator Performance	835
15.2.3	Intervention Measures	838
15.3	Acceptance Measures	842
15.3.1	Safety Culture and Safety Climate?	844
15.3.2	Probity and Equity	849
15.3.3	Financial Support	851
15.4	Monitoring Techniques	853
15.4.1	Public Hearings, Focus Groups, Working Parties and Standing Committees	854
15.4.2	Incident Sampling	860
15.4.3	Sentinel systems	865
15.4.4	Observational Studies	868
15.4.5	Statistical Analysis	873
15.4.6	Electronic Visualisation	878
15.4.7	Experimental Studies	888
15.5	Summary	897
16	Conclusions	901
16.1	Human Problems	902
16.1.1	Reporting Biases	903
16.1.2	Blame	903
16.1.3	Analytical Bias	904
16.2	Technical Problems	906
16.2.1	Poor Investigatory and Analytical Procedures	906
16.2.2	Inadequate Risk Assessments	907
16.2.3	Causation and the Problems of Counter-Factual Reasoning	908
16.2.4	Classification Problems	910
16.3	Managerial Problems	913
16.3.1	Unrealistic Expectations	913
16.3.2	Reliance on Reminders and Quick Fixes	914
16.3.3	Flaws in the Systemic View of Failure	916
16.4	Summary	918

List of Figures

1.1	Components of Systems Failure	4
1.2	Process of Systems Failure	5
1.3	Normal and Abnormal States	17
2.1	EUROCONTROL's Safety Iceberg	23
2.2	Distribution of Contribution Sources to ASRS	37
2.3	Involvement in Accidents Per Year	38
3.1	Levels of Reporting and Monitoring in Safety Critical Applications	46
3.2	Costs Versus Maintenance Interval	54
3.3	Failure Probability Distribution for Hardware Devices	55
3.4	Cognitive Influences in Decision Making and Control	71
3.5	Cognitive Influences on Group Decision Making and Control	78
3.6	Influences on Group Performance	79
3.7	Levels of Situation Awareness as Causal Factors in ATC Incidents	83
4.1	A Simple Monitoring Architecture	104
4.2	Regulated Monitoring Reporting System	105
4.3	Local Oversight Reporting System	106
4.4	Gatekeeper Reporting System	107
4.5	Devolved Reporting System	109
5.1	Generic Phases in Incident Reporting Systems	111
5.2	Accident and Incident Rates for Rejected Takeoff Overruns	130
5.3	CHIRP and ASRS Publications	131
5.4	Web Interface to the CHSIB Incident Collection	133
5.5	Incident Reporting Form for a UK Neonatal Intensive Care Unit [119]	136
5.6	ASRS Reporting Form for Air Traffic Control Incidents (January 2000)	138
5.7	The CIRS Reporting System [757]	139
6.1	Generic Phases in Incident Reporting Systems	148
6.2	US Army Preliminary Incident/Accident Checklist	152
6.3	Interview Participation Diagram	166
6.4	US Army Incident/Accident Reporting Procedures	176
6.5	US Army Preliminary Incident/Accident Telephone Reports	177
6.6	US Army Aviation and Missile Command Preliminary Incident Form	178
8.1	Imagemap Overview of the Herald of Free Enterprise	229
8.2	Imagemap Detail of the Herald of Free Enterprise	230
8.3	QuicktimeVR Simulation of a Boeing 757	233
8.4	QuicktimeVR Simulation of Lukas Spreaders	233
8.5	VRML Simulation of Building Site Incidents	237
8.6	NTSB Simulation of the Bus Accident (HWY-99-M-H017).	238
8.7	3 Dimensional Time-line Using DesktopVR	240

8.8	Overview of Perspective Wall Using DesktopVR	241
8.9	Detail of Perspective Wall Using DesktopVR	242
8.10	Graphical Modelling Using Boeing's EASY5 Tool	243
8.11	NTSB Simulated Crash Pulse Of School Bus and Truck Colliding	246
8.12	NTSB Simulation of Motor Vehicle Accident, Wagner Oklahoma	247
8.13	Biomechanical Models in NTSB Incident Simulations (1)	248
8.14	Biomechanical Models in NTSB Incident Simulations (2)	249
8.15	Multi-User Air Traffic Control (Datalink) Simulation	253
8.16	EUROCONTROL Proposals for ATM Incident Simulation	255
8.17	US National Crash Analysis Centre's Simulation of Ankle Injury in Automobile Accidents	256
8.18	Integration of MIIU Plans, Models, Maps and Photographs	257
8.19	NTSB Use of Simulations in Incident Reports	258
9.1	Graphical Time-line Showing Initial Regulatory Background.	262
9.2	Graphical Time-line Showing Intermediate Regulatory Background.	263
9.3	Graphical Time-line Showing Immediate Regulatory Background.	264
9.4	Graphical Time-line of Events Surrounding the Allentown Explosion.	265
9.5	Graphical Time-line of the Allentown Explosion.	267
9.6	Two-Axis Time-line of the Allentown Explosion.	268
9.7	Fault tree components.	269
9.8	A Simple Fault Tree for Design.	270
9.9	Simplified Fault Tree Representing Part of the Allentown Incident.	271
9.10	Fault Tree Showing Events Leading to Allentown Explosion	273
9.11	Using Inhibit Gates to Represent Alternative Scenarios	275
9.12	Using House Events to Represent Alternative Scenarios	277
9.13	Fault Tree Showing Post-Explosion Events	279
9.14	Fault Tree Showing NTSB Conclusions about the Causes of the Explosion	280
9.15	Fault Tree Showing Conclusions about Injuries and Loss of Life	283
9.16	Fault Tree Showing Conclusions about Reliability of Excess Flow Valves	284
9.17	Petri Net of Initial Events in the Allentown Incident	286
9.18	A Petri Net With Multiple Tokens	288
9.19	A Petri Net Showing Catalytic Transition.	290
9.20	A Petri Net Showing Conflict	291
9.21	A Petri Net With An Inhibitor Avoiding Conflict.	292
9.22	A Sub-Net Showing Crew Interaction.	294
9.23	A Sub-Net Showing Alternative Reasons for the Foreman's Decision.	296
9.24	High-Level CAE Diagram for the Allentown Incident	311
9.25	Representing Counter Arguments in a CAE Diagram (1)	312
9.26	Representing Counter Arguments in a CAE Diagram (2)	313
9.27	Representing Counter Arguments in a CAE Diagram (3)	314
9.28	High-Level CAE Diagram Integrating Formal and Informal Material	315
9.29	Extended CAE Diagram Integrating Formal and Informal Material (1)	316
9.30	Extended CAE Diagram Integrating Formal and Informal Material (2)	316
9.31	Subjective Responses to Modelling Notations.	317
9.32	Subjective Responses to Logic-Based Reconstruction How Easy did you find it to understand the logic-based model?	319
9.33	Qualitative Assessments Of CAE-Based Diagrams How Easy Did You Find It to Understand the CAE Diagram?	320
9.34	Qualitative Assessments of Hybrid Approach	321
9.35	Allentown Fault Tree Showing Pre- and Post-Incident Events	324
9.36	Cross-Referencing Problems in Incident Reports	325
9.37	Using a Petri Net to Build a Coherent Model of Concurrent Events	327
9.38	Lack of Evidence, Imprecise Timings and Time-lines	329

9.39	Continuous changes and Time-lines	330
9.40	Using Petri Nets to Represent Different Versions of Events	331
9.41	Annotating Petri Nets to Resolve Apparent Contradictions	332
9.42	Representing the Criticality of Distal Causes	334
9.43	Representing the Impact of Proximal Causes	336
9.44	Representing the Impact of Mitigating Factors	337
9.45	Representing Impact in a Causal Analysis	338
10.1	Overview of the Dept. of Energy's 'Core' Techniques	352
10.2	Simplified Structure of an ECF Chart	353
10.3	Components of ECF Chart	354
10.4	High-Level ECF Chart for the Mars Climate Orbiter (MCO)	354
10.5	Angular Momentum Desaturation Events Affect MCO Navigation	355
10.6	High-Level ECF chart for the Mars Polar Lander (MPL)	356
10.7	Premature MPL Engine Shut-Down and DS2 Battery Failure	357
10.8	Integrating the Products of Barrier Analysis into ECF Charts	363
10.9	Process Barriers Fail to Protect the Climate Orbiter	365
10.10	Process Barriers Fail to Protect the Climate Orbiter (2)	366
10.11	Process Barriers Fail to Protect the Climate Orbiter (3)	367
10.12	Technological Barriers Fail to Protect the Climate Orbiter	424
10.13	Technological Barriers Fail to Protect the Climate Orbiter (2)	425
10.14	Integrating Change Analysis into an ECF Chart	426
10.15	Representing Staffing Limitations within an ECF Chart	427
10.16	Representing Risk Management Issues within an ECF Chart	428
10.17	Representing Technological Issues within an ECF chart (1)	428
10.18	Representing Technological Issues within an ECF chart (2)	429
10.19	Using Change Analysis to Collate Contextual Conditions	430
10.20	Integrating Development Issues into an ECF chart (1)	431
10.21	Integrating Development Issues into an ECF chart (2)	431
10.22	Integrating Review Issues into an ECF chart	432
10.23	An ECF chart of the Deep Space 2 Mission Failure	432
10.24	An ECF chart of the Polar Lander Mission Failure	433
10.25	An ECF chart of the Climate Orbiter Mission Failure	434
10.26	NASA Headquarters' Office of Space Science [570]	435
10.27	JPL Space and Earth Sciences Programmes Directorate [570]	436
11.1	Abstract View of A Multilinear Events Sequence (MES) Diagram	439
11.2	An Initial Multilinear Events Sequence (MES) Diagram	443
11.3	A MES Flowchart showing Conditions in the Nanticoke Case Study	444
11.4	A MES Flowchart showing Causation in the Nanticoke Case Study	446
11.5	Causal Relationships in STEP Matrices	448
11.6	STEP Matrix for the Nanticoke Case Study	451
11.7	The Mini-MORT Diagram	456
11.8	A Causal Tree of the Nanticoke Case Study	470
11.9	The Eindhoven Classification Model [841]	474
11.10	Classification Model for the Medical Domain [845]	475
11.11	The Three Legs of Tripod	480
11.12	Tripod-Beta Event Analysis of the Nanticoke Incident (1)	483
11.13	Tripod-Beta Event Analysis of the Nanticoke Incident (2)	485
11.14	Why-Because Graph Showing Halon Discharge	489
11.15	Why-Because Graph for the Nanticoke Alarm	490
11.16	Overview of the Why-Because Graph for the Nanticoke Incident	492
11.17	Possible 'Normative' Worlds for the Nanticoke Incident	493
11.18	Bayesian Network Model for the Nanticoke Fuel Source	511

11.19	Causal Tree from McElroy's Evaluation of PRIMA (1)	532
11.20	Causal Tree from McElroy's Evaluation of PRIMA (2)	534
13.1	Simplified Flowchart of Report Generation Based on [633]	633
13.2	Data and Claims in the Navimar Case Study.	690
13.3	Qualification and Rebuttal in the Navimar Case Study.	691
13.4	More Complex Applications of Toulmin's Model.	693
13.5	Snowdon's Tool for Visualising Argument in Incident Reports (1).	696
13.6	Snowdon's Tool for Visualising Argument in Incident Reports (2).	697
13.7	MAIB On-Line Feedback Page	703
13.8	MAIB Safety Digest (HTML Version)	706
13.9	ATSB Incident Report (PDF Version)	708
13.10	NTSB Incident Report (PDF Version)	708
13.11	Douglas Melvin's Simulation Interface to Rail Incident Report (VRML Version)	709
13.12	James Farrel's Simulation Interface to Aviation Incident Report (VRML Version)	709
13.13	Peter Hamilton's Cross-Reference Visualisation (VRML Version)	710
14.1	Perceived 'Ease of Learning' in a Regional Fire Brigade	742
14.2	The Heavy Rescue Vehicle Training Package	743
14.3	Overview of the MAUDE Relations	755
14.4	The MAUDE User Interface	770
14.5	Precision and Recall	783
14.6	Components of a Semantic Network	788
14.7	Semantic Network for an Example MAUDE Case	788
14.8	Using a Semantic Network to Model Stereotypes	789
14.9	US Naval Research Laboratory's Conversational Decision Aids Environment	792
15.1	Static Conventional Visualisation of SPAD Severity by Year	880
15.2	Static 'Column' Visualisation of SPAD Severity by Year	881
15.3	Static 'Radar' Visualisation of SPAD Severity by Year	882
15.4	Computer-Based Visualisation of SPAD Data	884
15.5	Signal Detail in SPAD Visualisation	886
15.6	Dynamic Queries in the Visualisation of SPAD Incidents	887
15.7	Eccentric Labelling in the Visualisation of SPAD Incidents	888

Preface

Incident reporting systems have been proposed as means of preserving safety in many industries. For instance, the International Civil Aviation Organization (ICAO) recommends their use throughout the aviation industry. Unfortunately, the lack of training material or other forms of guidance can make it very difficult for engineers and managers to set up and maintain reporting systems. There has been a proliferation of small-scale local initiatives, for example within individual departments in UK hospitals. This, in turn, has made it very difficult to collate national statistics for incidents within a single industry.

There are, of course, exceptions to this. For example, the Aviation Safety Reporting System (ASRS) has established national reporting procedures throughout the US aviation industry. Similarly, the UK Health and Safety Executive have supported national initiatives to gather data on Reportable Injuries, Diseases and Dangerous Occurrences (RIDDOR). In contrast to the local schemes, these national systems face problems of scale. It can become difficult to search databases of 500,000 records to determine whether similar incidents have occurred in the past.

This book, therefore, addresses two needs. The first is to provide engineers and managers with a practical guide on how to set up and maintain an incident reporting system. The second is to provide guidance on how to cope with the problems of scale that can arise from successful local and national incident reporting systems.

In 1999, I was asked to help draft guidelines for incident reporting in air traffic control throughout Europe. The problems of drafting these guidelines led directly to this book. I am, therefore, grateful to Gilles le Gallo and Martine Blaize of EUROCONTROL for helping me to focus on the problems of international incident reporting systems. Roger Bartlett, safety manager at the Maastricht upper air space Air Traffic Control center also provided valuable help during several stages in the writing of this book. In particular, he emphasized the importance of identifying the rights of individuals who contribute to the reporting process.

Thanks are also due to Michael Holloway of NASA's Langley Research Center who encouraged me to analyze the innovative mishap reporting procedures being developed within his organization. Mike O'Leary of British Airways and Neil Johnstone of Aer Lingus encouraged my early work on software development for incident reporting. Ludwig Benner, Peter Ladkin, Karsten Loer and Dmitri Zotov provided advice and critical guidance on the causal analysis sections. I would also like to thank Gordon Crick of the UK Health and Safety Executive, in particular, for his ideas on the future of national reporting systems.

I would like to thank the University of Glasgow for supporting the sabbatical that helped me to finish this work.

Chris Johnson, Glasgow, 2002.