TECHNICAL UNIVERSITY OF CRETE

DEPARTMENT OF PRODUCTION ENGINEERING AND MANAGEMENT

DIPLOMA THESIS

APPLYING ACCIDENT ANALYSIS TECHNIQUES (AcciMap – STAMP) TO THE HELIOS AIRWAYS CRASH AT GRAMMATIKO.

Examining Board:

Associate Professor Tom Kontogiannis (Supervisor)

Assistant Professor Elias Kosmatopoulos

Assistant Professor Vangelis Grigoroudis

PAPETTAS ANDREAS I.

JUNE 2009

Acknowledgements

- I thank Mr. Tom Kontogiannis for introducing and guiding me to the social sensitive world of safety engineering.
- The cross-disciplinary undergraduate curriculum at Department of Production Engineering and Management, Technical University of Crete provided a great background in coupling together the disciplines from different levels; from technical to managerial.
- My gratitude to my parents Ioannis and Despo for supporting me (mentally and by funds) in my first academic quest which eventually ends by this work. And of course my younger brothers Michael and Mario for keeping me fit .

To Lambidona and Michael.

Although gone; they are still around.

ABBREVIATIONS

AAIASB	Air Accident Investigation and Aviation Safety Board (Greece)
AMM	Airplane Maintenance Manual
AOC	Air Operator's Certificate
ATC	Air Traffic Control
ATPL	Airline Transport Pilot License
CAA	Civil Aviation Authority of United Kingdom (UK)
CRM	Crew Resource Management
CVR	Cockpit Voice Recorder
DCA	Department of Civil Aviation (Cyprus)
EASA	European Aviation Safety Agency
FCOM	Flight Crew Operations Manual
FDR	Flight Data Recorder
FMS	Flight Management System
ICAO	International Civil Aviation Organization
JAA	Join Aviation Authorities
NVM	Non Volatile Memory
QRH	Quick Reference Handbook
SOP	Standard Operational Procedures
TUC	Time of Useful Consciousness

Table of Contents

Prologue

The Helios Airways crash at Grammatikos was one shocking air disaster with 121 fatalities which implicated several safety issues. The official report by AAIASB [1] resulted in safety amendments by Boeing, the aircraft manufacturer and caused the undergoing Cyprus Department of Civil Aviation full scale reorganization.

For the analysis of the above accident two novel techniques are chosen. The first one , the Rasmussen's framework[28], which will be also referred as AcciMap, provides a series of graphical representation in representing an accident. Applications of this technique in literature are provide by Hopkins (2000) on the 'ESSO Australian Gas Explosion' [10] and by Svedung and Rasmussen (2000) on the 'Transportation of dangerous goods' [23].

The second technique STAMP [16] suggests a control structure in approaching the accident. Applications of this technique are provided by Leveson et al, [15-20], on the 'Ariane 5 Loss', the 'Loss of a Milstar Satellite', a 'Public Water Supply Contamination' accident and others.

Both techniques present a common feature. They view the accident in a hierarchical socio-technical system. This feature was demonstrated by Almeida and Johnson (2004) [2] where the loss of a Brazilian space vehicle was used to investigate the two techniques.

The aims of this work are:

1. To demonstrate that industrial accidents are not only sequence of erroneous events that happened to occur that specific time window (e.g a day or a worker's shift) but final depictions of deficient decision making and inadequate control of an ill designed system in which the accidental flow of events take place.

2. To reveal the features of each technique by comparable analysis and investigate if they complement each other on areas which by definition they are individually deficient.

3. Point out any safety issues not referenced by the official report.

Chapter 1 Introduction to Analysis Techniques

Most approaches in accident analysis are event based. They focus on the sequence of events on that specific day. Of course accidents are resulted from those events. The problem is that one accident (e.g an air crash) can be caused from almost infinite combination of sequenced events. As a result of this, we must not only focus on the chain of events on that specific time window (e.g. a workers shift) but to extend our focus on the preconditions that allowed those events to happen. In this way we can learn how the production system behaves taken into account its complexity from managerial levels to the lower production lines. How a decision taken at the top, affects the bottom levels without the decision maker knowing or is aware of any hazardous interrelation. It is imperative to study and analyze accidents in terms of the systemic and control structure parameter in order to gain more knowledge about the system behavior. Thus two novel techniques are chosen that incorporate those two parameters: The Rasmussen's framework (AcciMap) and the Systems-Theoretic Accident Model and Processes (STAMP).

The official report by AAIASB contained a vast amount of information relevant to the accident. There was a need to cluster that information in a useful format in order to proceed by application of the two techniques. The Rasmussen's hierarchical levels were found to be a useful platform on which facts were recorded on the appropriate level. This resulted to the diagram on Appendix C which I call the "Big Picture" and the associate table of Appendix B which I call "Look up tables". The brackets in the diagram of Appendix C refer to the tables in Appendix B. Thus, all the necessary information required by the two techniques was distilled from Appendices B and C.

The two techniques are first presented as proposed by their authors. In the next chapter the two techniques are used to analyze the aircraft accident of Helios Airways flight HCY522 on 14th of August 2005. In Appendix A all the figures of Chapters 3 and 4 are reprinted for better review by the reader. This work closes with a conclusion chapter discussing the analysis findings. There has been put great effort to make this work self standing for the reader and that is why the techniques are presented just as proposed in the respective papers. In order to provide evidences from the accident report, a "Big Picture AcciMap" is presented in the Appendix C. This "Big Picture" is the mapping of facts from the official investigation report by the Greek Air Accident Investigation &Aviation Safety Board (AAIASB) and its main purpose is to enable the reader (and he/she is greatly encouraged) to experiment with the two techniques using the associated "Look up tables" of Appendix B.

Before the presentation of the two techniques; the cause-consequence-chart will be presented as the representative of the traditional techniques on which the Rasmussen's framework differentiates and later the STAMP technique jumps from the "event based" plane to the "control" plane. The introduction closes with a reference to criteria for the evaluation of accident analysis techniques.

1.1 The cause-consequence-chart [28]

The cause-consequence chart formalism (Nielsen, 1974), has been widely used as a basis for predictive risk analysis (Figure 1-1). These charts represent a set of possible or actual chain of events. Several different potential causes may release a particular hazard source. These causes are therefore connected to this event by "OR" gates. Depending on actions by people in the system, different alternative routes may be taken by the accidental flow. Consequently, "decision switches" are introduced to represent the effect of human intervention in the flow.

A cause-consequence chart represents a class of related, possible accident scenarios and they therefore reflect a complex network of causal trees (reflecting logical necessity of causes in accident release) and the consequent event flow paths (reflecting the temporal order of causal [functional] relations) (Figure 1-1). Since cause and consequence charts are representing possible accidents, they are not true representation of facts in the same sense as the causal trees used to represent the results of post hoc accident investigations. Causes-consequence charts are not intended for allocation of responsibility to individuals but present a design tool and therefore have the nature of hypotheses. The criterion during analysis is completeness, i.e. they include a complete set of the plausible scenarios related to a given hazard source and the related critical event.

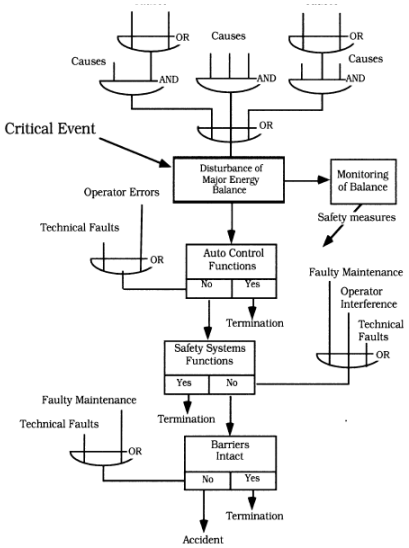


Figure 1-1: The cause-consequence diagram used for generalization from past accidents and for prediction of possible accidents

A cause-consequence chart represents a generalization that aggregates a set of accidental courses of events. The set to include in a cause-consequence chart is defined by the choice of the critical event, which reflects the release of a well-defined hazard source, such as 'loss of containment of hazardous substance', or 'loss of control of accumulated energy'. The 'critical event' connects the causal tree (the logic relation among potential causes) with a consequent event tree (the possible functional and temporal relation among events) explicitly reflecting the switching of the flow resulting from human decisions. The critical event to choose depends upon the purpose.

When dealing with a global safety design within a work place or activity, a set of critical events will be chosen for the analysis. These critical events structure the relevant hazard sources and the protective measures in the most manageable way, e.g. by giving the minimal set of cause-consequence charts, or identifying the most consistent set of risk management strategies.

The concept of critical event and the related definition of a hazard source are basic elements in a taxonomy of hazard sources, work system structure, and risk management strategies which is described by Svedung and Rasmussen (1998) (in Swedish) and by Rasmussen and Svedung (2000). In the cause-consequence chart representation, the focus is still on events and conditions and on decisions directly influencing the causal flow of events. The analyses reflect the focus of most accident committee reports, i.e. the abnormal and unusual events and acts. When the focus is design of improved system safety, not on identifying the guilty person, the problem is to identify those people in the system that can make decisions resulting in improved risk management, given the proper work conditions. This points to decision makers also at the higher social system levels, and leads us to the AcciMap representation.

1.2 Criteria for the evaluation of accident analysis techniques [11]

Previous studies have specified a variety of assessment criteria for accident analysis techniques (e.g. Benner, 1985; Ferry, 1988; Suokas and Pyy,1988) which could be assigned to the following categories:

- Sequential and temporal aspects of the accident scenario i.e. sequence, timing, event dependencies, and levels of representation, etc.
- Aspects of the accident analysis process i.e. coping with unreliable evidence, modeling of assumptions, and encouraging participation,
- Aspects of accident prevention i.e. identifying causal factors at the workplace and management levels, modeling error recovery paths, and devising prevention measures at the management and legislation levels.

In this section, taxonomy of assessment criteria is proposed specifically for accident analysis techniques which aim to expand the traditional system engineering approach and incorporate aspects of human interventions and causal factors at the workplace and management levels. Techniques which perform in-depth investigation of human error mechanisms and analysis of management factors are beyond of our scope.

1.2.1 Sequential and temporal aspects of accident scenarios

Accident analysis techniques are usually judged in terms of the support provided to investigate complex scenarios. Multiple agents may be involved in the accident, taking a number of actions which interact in complex ways. In addition, the events may have different temporal characteristics such as timing and duration. The representation of accident scenarios often produces complicated diagrams which are difficult to use. For this reason, the analysts should be able to represent the accident scenario at different levels of abstraction. The following criteria are proposed to examine the support ordered for analyzing the sequential and temporal aspects of events:

Event sequence. The technique should support analysts in describing and representing the sequence of events/actions that have led to the accident.

Event agent. The graphical representation should facilitate the identification of agents of different events/actions and, if possible, facilitate their grouping in technical, interface, and human agents.

Event dependencies and cascade effect. The technique should support the identification of relationships between the events/actions and examine their dependencies and cascade effects. Dependency refers to the extent that the occurrence of an event/action is dependent upon preceding ones. In addition, the technique should represent cases where the consequences of an event/action are spread upon other areas of the accident scenario.

Modeling the timing and duration. The technique should record both the 'timing' (i.e. when the event happened) and the `duration of the event/action (i.e. how long the event lasted). Special notation may be required when descriptions of timing are imprecise. The duration is also important because we can appreciate cases where operators have to perform many tasks or respond to many events at close time proximity. In other words, the representation of timing and duration may provide a rough estimate of the workload of operators.

Multiple levels of representation. Graphical representations of accidents frequently become unwieldy because of the large number of events/ actions involved and their complex relationships. To simplify the representation, analysts should be able to create 'groups of events' or 'groups of actions' and describe them in more abstract terms; this would enable them to create a multiple level description of the accident scenario.

1.2.2 Aspects of the accident analysis process

Accident analysis is a dynamic process which requires modifications to the representation of accident as additional evidence becomes available. This implies that analysts may have to make assumptions about events which are supported by weak evidence and accommodate different accounts offered by various witnesses. Modeling of assumptions and inconsistencies, therefore, is very important for refining the accident analysis as evidence accrues. In addition, accident analysis techniques should facilitate the co-operation between analysts of different

backgrounds. Therefore, the following three criteria are proposed for assessing the cognitive support provided in the course of analysis:

Modeling assumption. The graphical representation of the accident should offer capabilities for marking events or actions where assumptions are made due to weak evidence. For example, dotted lines can be used for assumed events or assumed actions; these lines can be turned into solid when we become certain that our evidence is reliable at later stages of the analysis.

Modeling inconsistencies. Sometimes, the evidence that we get from the accident data contains inconsistencies or conflicts. This happens because different people offer contradictory accounts of what happened. To resolve this issue, analysts so far have tended to create two or more sequences of events corresponding to different interpretations of what happened. However, it would be desirable to be able to merge all inconsistencies in a single diagram.

Co-operation facilitation. The graphical representation should be comprehensible to all members of the accident analysis team so that it can be used as a common reference framework as well as facilitate their co-operation.

1.2.3 Aspects of accident prevention

The ultimate outcome of the accident analysis is to identify the critical events that have led to the accident and the failures of the agents that gave rise to the critical events. In this sense, the accident analysis aims to identify factors at the technical, workplace and management levels (i.e. the context of work) that should be controlled in order to prevent future accidents or minimize their consequences. Prevention measures, therefore, are tightly linked to the causal factors of the work context. In the past, a lot of emphasis has been placed into the prevention or avoidance of human error. However, this is not always possible in complex systems and attention must also be paid to the error recovery paths that could have prevented errors or minimized their consequences (Kontogiannis, 1999).For this reason, the modeling of error recovery paths should be treated as an additional criterion in the assessment of accident analysis techniques. Therefore, the following criteria can be used for assessing the support provided in the accident prevention process:

Event criticality. The technique should support the judgment of the importance or criticality of the events/actions and their contribution to the accident.

Modeling error recovery. There are very few techniques available for modeling events and information cues that could have helped operators to detect and recover their errors. Kontogiannis (1996) argued that accident analysis should offer capabilities for recording `missing events' (i.e. events that were absent or delayed when operators made their decisions), `misleading events' (i.e. events that over-shadowed others) and `attention-diverting events'.

Modeling the context of work. It has been argued that modeling the timing and duration of events/actions would provide an indication of the workload of operators. However, other things the operators had to do in parallel within their main tasks, could also contribute to their

workload. It would be desirable, therefore, to represent not only the events/actions that were directly involved in the accident, but also other events/actions that undoubtedly affected the workload and perception of operators.

Preventive measures. The graphical representation should facilitate the development of preventive measures and their cost-benefit analysis.

Chapter 2 Accident Analysis Techniques

2.1 The Rasmussen's framework[1]

Svedung and Rasmussen suggest the following graphic formats in their framework for accident analysis:

1. The AcciMap that represents a particular accident scenario. It is based on the classic cause and sequence chart representing the causal flow of events supplemented by a representation of the planning, management and regulatory bodies contributing to creation of the scenarios.
2. The Generic AcciMap, a graph that is created by the aggregation of a set of AcciMaps from a representative set of scenarios from a particular hazard domain. This diagram emphasizes the decision bodies setting the general safety level in the particular hazard domain and serves to identify those decisions bodies that should be subject to studies of their normal work routines.
3. The ActorMap, a graph identifying the various organizational bodies, identified by the Generic AcciMap and individual actors and decision makers involved in work planning and risk management as identified during field interviews together with their respective roles in accident creation. Due to their complexity, this representation tends to be hierarchically ordered in a couple of levels.
4. The InfoMap, a graph representing the information flow among decisions makers during normal activities. The study of the normal information flow servers to identify the communication structure in which the propagation of the information about changes in conditions and requirements will be embedded. It is a general finding that information changes are likely to drop out in the usually very rudimentary communication among experts. Due to the complexity of the information flow network, a hierarchical set of diagrams will be useful also for this type of representation.

2.1.1 The AcciMap representation

The need to include in an analysis decision making during normal work of work planners, managers, legislators and the influence of the stressors found in the modern dynamic society

[1] The Rasmussen's framework as presented by Svedung I and Rasmussen J in Safety Science Vol. 40 pp.397-417.

(Figure 2-1). Decision makers on many levels are planning the landscape determining the flow of the accidental events and their roles should be included in the analysis of accidents and the planning of better risk management.

The focus of this analysis is the control of the hazardous process at the bottom of the socio-technical system. The aim is therefore a vertical analysis across the levels not a horizontal generalization within the individual levels as it is usually found within the various academic disciplines. In this situation it appears that an extension of the cause-consequence chart representation to explicitly include the normal work decisions at the higher levels of Figure 2-1 will be very useful; useful for analysis of past accidents, for identification of decision makers having a potential from improving safety and for communication with the various disciplines relevant for cross-disciplinary co-operation in research and design.

The "AcciMap" representation is proposed to serve these aims and is organized in the following way.

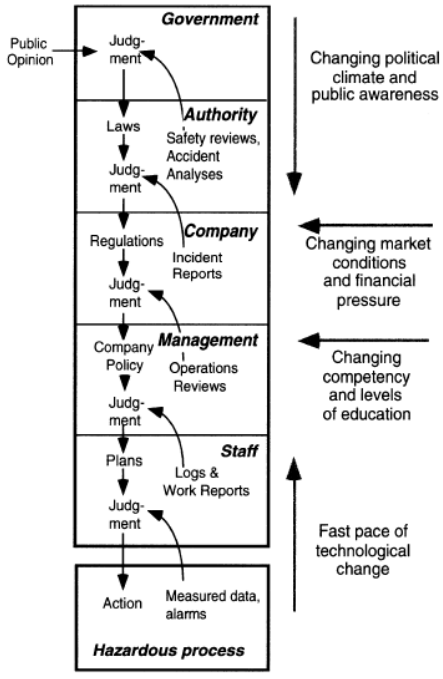


Figure 2-1. The many nested levels of decision making that are involved in risk management and regulatory rulemaking to control hazardous processes.

As in the case with the casual tree normally used to represent the findings from post hoc analysis, the basic AcciMap is developed from analysis of one particular accident case i.e. it reflects one particular course of events. There are however, several basic differences:

1. The AcciMap is aimed at design of improved systems, not at allocation of responsibility. Therefore, the criterion for its development will not be a truthful representation of facts, but representative identification of factors sensitive to improvement, i.e. of all decision makers that could have influenced the flow by a decision different from the past practice.
2. Even if the AcciMap serves to reflect the analysis of only one past accident, the "Decision/Action Box" symbol of the cause-consequence chart in Figure 1-1 is included to represent the decisions and actions that have served to configure the landscape of the accidental flow.
3. In contrast to the conventional cause-consequence chart the analysis for development of an AcciMap should not only include events and acts in the direct dynamic flow of events. It should also serve to identify all decisions markers at the higher level in the socio-technical system of Figure 2-1 that have influenced the conditions leading to accident through their normal; work activities.

For clarity, the presentation of an AcciMap is structured according to the levels of Figure 2-1.The layout and proposes symbols to be used are as in Figure 2-2 :

1. At the bottom there is a level representing the topography of the accident scene: the configuration and physical characteristics of the landscape buildings, equipment, tools, vehicles etc., found at the location and involved in the accident
2. At the next higher level is represented the accident processes i.e. the causal and functional relations of the dynamics flow, described in terms of the cause and consequence chart convention. In the flow "Decision/Action boxes" are included and connected to consequence boxes in cases where the flow has been or could be changed by human(or automated) intervention.
3. At the levels above this the Decision/Action box symbol is used to represent all decision makers that- through decisions in their normal work context- have or could have influenced the accidental flow at the bottom.

In this way, the AcciMap serves to identify relevant decision makers and the normal work situation in which they influence and condition possible accidents. The focus is not the traditional search for 'management errors' and the like. Therefore, the AcciMap representing the conditioning system for one particular accident is well suited as a 'conservation piece' to support discussion with the relevant decision makers.

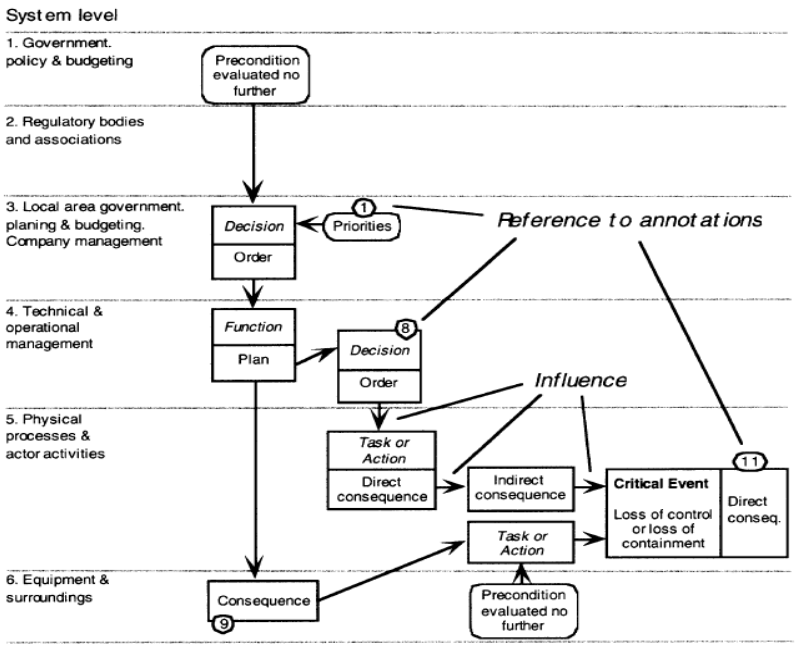


Figure 2-2. An approach to standardize symbols in an AcciMap

2.1.2 The generic AcciMap

The basic AcciMap represents the conditioning system and the flow of events from one particular accident. Suggestion of improvements by changes identified from this map therefore will very likely be ad hoc and, as was done by the cause-consequence chart based on a generic 'critical event', a generalization is necessary based on a set of accident scenarios.

To complete the identification of relevant decision makers, the causal flow at the lowest-but-one level is based on the selection of a 'critical event' defined as discussed for the cause-consequence chart. The model should include all relevant, alternative flow paths following a release of the critical event and related to the prevention and mitigation strategies in place.

This representation at the causal level of the generic AcciMap should be based on a description of the normal, causal flow of activities within which the 'critical event' is embedded. In that way it can form a basis for generalization across several accident scenarios and reflect the influence on the scenarios from the normal work context of decision makers

Since in this analysis one accident scenario is considered, the creation of the generic AcciMap is not possible. Instead the AcciMap can be discussed in its place.

2.1.3 The ActorMap and InfoMap

We consider risk management as an adaptive, closed-loop control function. The various actors and decision makers then have many roles. One is to formulate the goal within their particular

sphere of control and another is to identify the actual state of affairs with reference to this goal. A third role is to act to bring the state of affairs in correspondence with the goal, while making sure that performance is optimal with respect to process criteria such as cost-effectiveness within the boundaries of acceptable performance, as defined by the constraints given by work and safety regulations.

Risk management and safety audit should then serve to evaluate the structure of the communication network and the content of the information to make sure that the closed-loop feedback control is actually effective. Such an evaluation implies an identification of the interacting decision makers (controllers) and their role in the distributed control function.

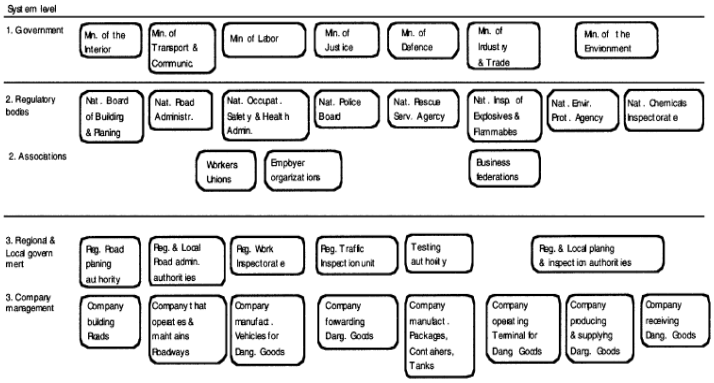


Figure 2-3. An ActorMap identifies the interacting bodies contributing to the landscape in which accidents flow.

A first step is a representation of those organizational bodies that were identified by the generic AcciMap for the work domain in question, i.e. focus on these acting units is derived from accident analyses. Included in this mapping are the information paths and the content of communication that normally connects these controlling bodies. This analysis includes review of legislation, instructional systems, commercial practices when passing orders, goods handling instructions, work plans and orders, etc.(Figure 2-3)

The phase of analysis behind the ActorMap depends on studies of the formal, case-independent communications such as company manuals, annual reports, branch recommendations, legislation, etc. It serves to prepare for a focused and detailed analysis in the field of the communication that actually takes place for a particular case in a system of highly trained professionals

At a level lower, the actual communication to and from each of the relevant bodies is mapped. The representation of this normative, formal communication net will serve as a reference for the detailed analysis of the complex, actual performance.

The co-operating organizational bodies relevant for safety auditing were identified by generalization across accident cases in terms of the generic AcciMap related to a particular work and hazard domain. In contrast, the following identification of the individual decision makers,

their roles, and competence depends on field studies and interviews

During this analysis, the nature of naturalistic, collaborative decision making must be kept in mind. Work performance during familiar work situations is typically based on know-how that has been learned from older colleagues during apprenticeship and refined while learning-by-doing. Decisions by professionals during familiar work are not based on careful situation analysis. Experts are well-synchronized with their work environment and know by heart the options for action that are relevant in a particular situation and only have to make a choice. For this choice they only need information that distinguishes between those few options; in effect, the choice is based on a cue which have been found to correlate to one of these options for action. If the work system conditions change, reliance on the familiar cues will no longer be valid, and even if performance is locally acceptable, unacceptable side effects may propagate through the collaborative network.

This reliance on familiar cue-action correlations has important implications for the co-ordination of co-operative work. Members of a professional team share a professional terminology and vocabulary. During collaborative work messages act as verbal cues to trigger actions by co-operators. The level of explicit formulation of such cues depends on the sender's perception of the receiver's competence and work situation. Familiarity with collaborators' level of competence grows steadily with team training, and messages increasingly get a rudimentary shorthand form.

When mapping the content and form of communication during collaborative work within an organizational body these aspects of professional communication must be carefully considered. First of all, some observation of the interaction within the team may be necessary, because the information rendered by an interview will very likely be rationalizations reflecting the formal messages.

The representation of the form and content of communication between and within the decision-making bodies should describe the following aspects:

1. The structure of the information net: are the information loops required for work control open and intact?
2. How effective is the communication of values, objectives, and performance criteria?
3. Is a feedback loop effective and informing higher management levels about work performance and resource requirement?
4. Is a practice of explicit reporting of changes, disturbances and unusual conditions in place and active also during normal conditions? Is this reporting practice in a form that prompts decision makers to consider likely side-effects of usual practice during less normal conditions?
5. What is done to ensure that basic understanding is maintained and up-dated with regard to work requirements and safety issues, which are likely to degenerate during long routine periods?

The information flow network is very complex, and a hierarchical, graphic representation is

used for clarity. Based on the ActorMap representation of the bodies and individuals involved in setting regulatory boundary conditions, in management and work planning, and in actual production, a normative representation of a consistent closed-loop safety control system is developed. This normative information system is used for a representation of the actual communication found within the particular work place subject to field analysis and audit. That is, the graphic representation will serve to highlight the communication links that are not active or not adequately explicit. The communication links, and its content depend on the hazard source and the configuration of the technical system involved, and a different normative information network may be required for different hazard scenarios.

Due to the fact that the accident's official report did not provide the structure and inmost of any actor identified in order to document the channels of information flow the InfoMap was not possible to be constructed. Instead STAMP treats actors referred to as operators as black boxes and provides the channels that form the control loop between the actors that belong to different hierarchical levels.

2.2 Systems-Theoretic Accident Model and Processes[2]

The hypothesis underlying the new model, called STAMP (Systems-Theoretic Accident Model and Processes) is that system theory is a useful way to analyze accidents, particularly system accidents. In this conception of safety, accidents occur when external disturbances, component failures, or dysfunctional interactions among system components are not adequately handled by the control system, that is, they result from inadequate control or enforcement of safety-related constraints on the development, design, and operation of the system.

Safety then can be viewed as a control problem, and safety is managed by a control structure embedded in an adaptive socio-technical system. The goal of the control structure is to enforce constraints on system development (including both the development process itself and the resulting system design) and on system operation that result in safe behavior. In this framework, understanding why an accident occurred requires determining why the control structure was ineffective. Preventing future accidents requires designing a control structure that will enforce the necessary constraints.

In STAMP, systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control. A system in this conceptualization is not a static design-it is a dynamic process that is continually adapting to achieve its ends and to react to changes in itself and its environment. The original design must not only enforce appropriate constraints on behavior to ensure safe operation, but the system must continue to

[2]STAMP as presented in Safety Science, Vol. 42, No. 4, April 2004, p. 237-270 by Nancy Leveson.

operate safely as changes occur. The process leading up to an accident (loss event) can be described in terms of an adaptive feedback function that fails to maintain safety as performance changes over time to meet a complex set of goals and values.

Instead of defining safety management in terms of preventing component failure events, it is defined as a continuous control task to impose the constraints necessary to limit system behavior to safe changes and adaptations. Accidents can be understood, using this model, in terms of why the controls that were in place did not prevent or detect maladaptive changes, that is, by identifying the safety constraints that were violated and determining why the controls were inadequate in enforcing them.

The basic concepts in STAMP are constraints, control loops and process models, and levels of control. Each of these is now described followed by a classification of accident factors based on the new model and on basic systems theory concepts.

2.2.1 The Central Role of Constraints in System Safety

The most basic concept in the new model is not an event, but a constraint. In systems theory, control is always associated with the imposition of constraints. The cause of an accident, instead of being understood in terms of a series of events, is viewed as the result of a lack of constraints imposed on the system design and on operations, that is, by inadequate enforcement of constraints on behavior at each level of a socio-technical system. In systems theory terminology, safety is an emergent property that arises when the system components interact within an environment. Emergent properties are controlled or enforced by a set of constraints (control laws) related to the behavior of the system components. Accidents result from a lack of appropriate constraints on the interactions.

As an example, the unsafe behavior (hazard) in the Challenger loss was the release of hot propellant gases from the field joint. An O-ring was used to control the hazard, i.e., its role was to seal a tiny gap in the field joint created by pressure at ignition. The design, in this case, did not effectively impose the required constraint on the propellant gas release (i.e., it did not adequately seal the gap), leading to an explosion and the loss of the Space Shuttle and its crew. Starting from here, there are then several questions that need to be answered to understand why the accident occurred. Why was this particular design unsuccessful in imposing the constraint, why was it chosen (what was the decision process), why was the flaw not found during development, and was there a different design that might have been more successful? These questions and others consider the original design process.

Understanding the accident also requires examining the contribution of the operations process. One constraint that was violated during operations was the requirement to correctly handle feedback about any potential violation of the safety design constraints, in this case, feedback during operations that the control by the O-rings of the release of hot propellant gases from the field joints was not being adequately enforced by the design. There were several instances of feedback that was not adequately handled, such as data about O-ring blowby and erosion

during previous shuttle launches and feedback by engineers who were concerned about the behavior of the O-rings in cold weather. In addition, there was missing feedback about changes in the design and testing procedures during operations, such as the use of a new type of putty and the introduction of new O-ring leak checks without adequate verification that they satisfied system safety constraints on the field joints. As a final example, the control processes were flawed that ensured unresolved safety concerns were adequately considered before each flight, i.e., flight readiness reviews and other feedback channels to project management making flight decisions.

Why do design constraints play such an important role in complex systems, particularly software intensive systems? The computer is so powerful and so useful because it has eliminated many of the physical constraints of electromechanical devices. This is both its blessing and its curse: We do not have to worry about the physical realization of our software designs, but we also no longer have physical laws to limit the complexity of these designs-the latter could be called the curse of flexibility (Leveson, 1995). Physical constraints enforce discipline on the design, construction, and modification of our design artifacts. Physical constraints also control the complexity of what we build. With software, the limits of what is possible to accomplish are different than the limits of what can be accomplished successfully and safely-the limiting factors change from the structural integrity and physical constraints of our materials to limits on our intellectual capabilities. It is possible and even quite easy to build software that we cannot understand in terms of being able to determine how it will behave under all conditions: We can construct software (and often do) that goes beyond human intellectual limits. The result has been an increase in system accidents stemming from intellectual unmanageability related to interactively complex and tightly coupled designs that allow potentially unsafe interactions to go undetected during development.

The solution to this problem is for engineers to enforce the same discipline on the software parts of the system design that nature imposes on the physical parts. Safety, like any quality, must be built into the system design. When software acts as a controller in complex systems, it represents or is the system design it embodies or enforces the system safety constraints by controlling the components and their interactions. Control software, then, contributes to an accident by not enforcing the appropriate constraints on behavior or by commanding behavior that violates the constraints. In a batch reactor case, the software needed to enforce the system safety constraint that water must be flowing into the reflux condenser whenever the flow of catalyst to the reactor is initiated. This system behavioral constraint translates to a constraint on software behavior (a software requirement) that the software must always open the water valve before the catalyst valve.

This control model provides a much better description of how software affects accidents than a failure model. The primary safety problem in computer-controlled systems is not software "failure" but the lack of appropriate constraints on software behavior, and the solution is to identify the required constraints and enforce them in the software and overall system design. System engineers must identify the constraints necessary to ensure safe system behavior and

effectively communicate these behavioral constraints to the software engineers who, in turn, must enforce them in their software.

The relaxation of physical constraints also impacts human supervision and control of automated systems and the design of interfaces between operators and controlled processes (Cook, 1996). Cook argues that when controls were primarily mechanical and were operated by people located close to the operating process, proximity allowed sensory perception of the status of the process via direct physical feedback such as vibration, sound, and temperature. Displays were directly linked to the process and thus were essentially a physical extension of it. For example, the flicker of a gauge needle in the cab of a train indicated (1) the engine valves were opening and closing in response to slight pressure fluctuations, (2) the gauge was connected to the engine; (3) the pointing indicator was free, etc. In this way, the displays provided a rich source of information about the controlled process and the state of the displays themselves.

The introduction of electromechanical controls allowed operators to control the process from a greater distance (both physical and conceptual) than possible with pure mechanically linked controls. That distance, however, meant that operators lost a lot of direct information about the process—they could no longer sense the process state directly and the control and display surfaces no longer provided as rich a source of information about it (or the state of the controls themselves). The designers had to synthesize and provide an image of the process state to the operators. An important new source of design errors was the need for the designers to determine beforehand what information the operator would need under all conditions to safely control the process. If the designers had not anticipated a particular situation could occur and provided for it in the original system design, they might also not anticipate the need of the operators for information about it during operations.

Designers also had to provide feedback on the actions of the operators and on any failures that might have occurred. The controls could now be operated without the desired effect on the process, and the operators might not know about it. Accidents started to occur due to incorrect feedback. For example, major accidents (including Three Mile Island) have involved the operators commanding a valve to open and receiving feedback that the valve had opened as a result, when in reality it had not. In these cases, the valves were wired to provide feedback that power had been applied to the valve, but not that it had actually opened. Not only could the design of the feedback about failures be misleading, but the return links were also subject to failure themselves.

Thus, electromechanical controls relaxed constraints on the system design allowing greater functionality. At the same time, they created new possibilities for designer and operator error that had not existed or were much less likely in mechanically controlled systems. The later introduction of computer and digital controls afforded additional advantages and removed even more constraints on the control system design-and introduced more possibility for error. It is this freedom from constraints that makes the design of such systems so difficult. The constraints shaped the system design in ways that efficiently transmitted valuable physical process

information and supported the operators' cognitive processes. Proximity provided rich sources of feedback that involved almost all of the senses, enabling early detection of potential problems. We are finding it hard to capture and provide these same qualities in new systems that use computer controls and displays.

The most basic concept in STAMP is a constraint, rather than an event. Accidents are considered to result from a lack of appropriate constraints on system design. The role of the system engineer or system safety engineer is to identify the design constraints necessary to maintain safety and to ensure that the system design, including the social and organizational aspects of the system and not just the physical ones, enforces them.

2.2.2 Control Loops and Process Models

Instead of decomposing systems and accident explanations into structural components and a flow of events as do most event-based models, STAMP describes systems and accidents in terms of a hierarchy of control based on adaptive feedback mechanisms. Some basic concepts from systems theory are needed here.

In system theory, open systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control. The plant's overall performance has to be controlled in order to produce the desired product while satisfying cost and quality constraints. In general, to effect control over a system requires four conditions (Ashby, 1956):

1. The controller must have a goal or goals (e.g., to maintain the set point),

2. The controller must be able to affect the state of the system,

3. The controller must be (or contain) a model of the system, and

4. The controller must be able to ascertain the state of the system.

Figure 2-3 shows a typical control loop where an automated controller is supervised by a human controller. The dotted lines indicate that the human supervisor may have direct access to system state information (not provided by the computer) and may have ways to manipulate the controlled process other than through computer commands. The human and/or automated controller(s) obtains information about (observes) the process state from measured variables (Condition 4, i.e., feedback) and uses this information to initiate action by manipulating controlled variables (Condition 2) to keep the process operating within predefined limits (constraints) or set points (Condition 1, i.e., the goal) despite disturbances to the process. In general, the maintenance of any open-system hierarchy, either biological or man-made, will

require a set of processes in which there is communication of information for regulation or control (Checkland, 1981).

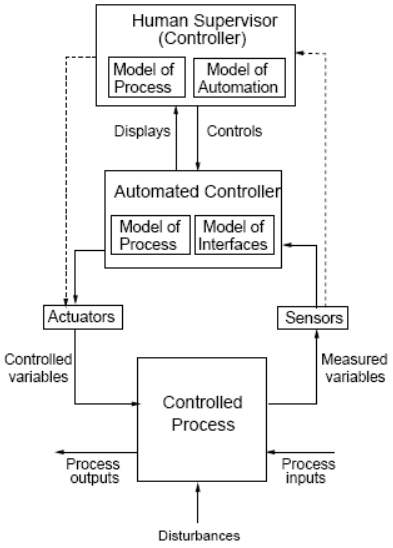


Figure 2-4. A typical control loop and the model process involved.

Control actions will, in general, lag in their effects on the process because of delays in signal propagation around the control loop: an actuator may not respond immediately to an external command signal (called dead time); the process may have delays in responding to manipulated variables (time constants); and the sensors may obtain values only at certain sampling intervals (feedback delays). Time lags restrict the speed and extent with which the effects of disturbances (both within the process itself and externally derived) can be reduced and impose extra requirements on the controller, for example, the need to infer delays that are not directly observable.

Condition 3 says that any controller-human or automated-must contain a model of the system being controlled (Conant and Ashby, 1970). This model at one extreme may contain only one or two variables (such as that required for a simple thermostat) while at the other extreme it may require a complex model with a large number of state variables and transitions (such as that needed for air traffic control). Whether the model is embedded in the control logic of an automated controller or in the mental model maintained by a human controller, it must contain the same type of information: the required relationship among the system variables (the control laws), the current state (the current values of the system variables), and the ways the process can change state. This model is used to determine what control actions are needed, and it is updated through various forms of feedback.

Human controllers interacting with automated controllers, in addition to having a model of the controlled process, must also have a model of the automated controllers' behavior in order to monitor or supervise it (Figure 2-4). Accidents may result from inaccuracies in this mental

model. In the loss of the American Airlines B-757 near Cali, Colombia, the pilots did not understand the model used by the computer for labeling waypoints. In the Nagoya A320 accident, the pilots' mental models of the automation behavior did not match the automation design. unfortunately, surveys and studies are finding that many operators of high-tech systems do not understand how the automation works (see, for example, Bureau of Air Safety Investigation, 1996 and Plat and Amalberti, 2000).

There may, of course, be multiple human and automated controllers in the control loop, and computers may be in other parts of the control loop than shown in Figure 2-4. For example, computers may act as automated decision aids that provide information to the human controller but do not directly issue control commands to the process actuators: If the software provides decision aiding, however, it is indirectly controlling the process and it must contain a model of the process. Common arguments that in this design the software is not safety-critical are not justified-it is still a critical part of the functioning of the control loop and software errors can lead to accidents.

This discussion has been simplified by speaking only of process models. Models will also need to include the relevant properties of the sensors, actuators, and on occasion the environment. An example is the need for an automated controller to have a model of its interface to the human controller(s) or supervisor(s). This interface, which contains the controls, displays, alarm annunciators, etc., is important because it is the means by which the two controller's models are synchronized, and lack of synchronization between the models can lead to system accidents.

2.2.3 Socio-Technical Levels of Control

In systems theory, systems are viewed as hierarchical structures where each level imposes constraints on the activity of the level beneath it that is, constraints or lack of constraints at a higher level allow or control lower-level behavior (Checkland, 1981). Control laws are constraints on the relationships between the values of system variables. Safety-related control laws or constraints therefore specify those relationships between system variables that constitute the nonhazardous system states, for example, the power must never be on when the access door is open. The control processes (including the physical design) that enforce these constraints will limit system behavior to safe changes and adaptations.

Modeling complex organizations or industries using system theory involves dividing them into hierarchical levels with control processes operating at the interfaces between levels (Rasmussen, 1997). Figure 2-5 shows a generic socio-technical control model. Each system, of course, must be modeled to reflect its specific features, but all will have a structure that is a variant on this one.

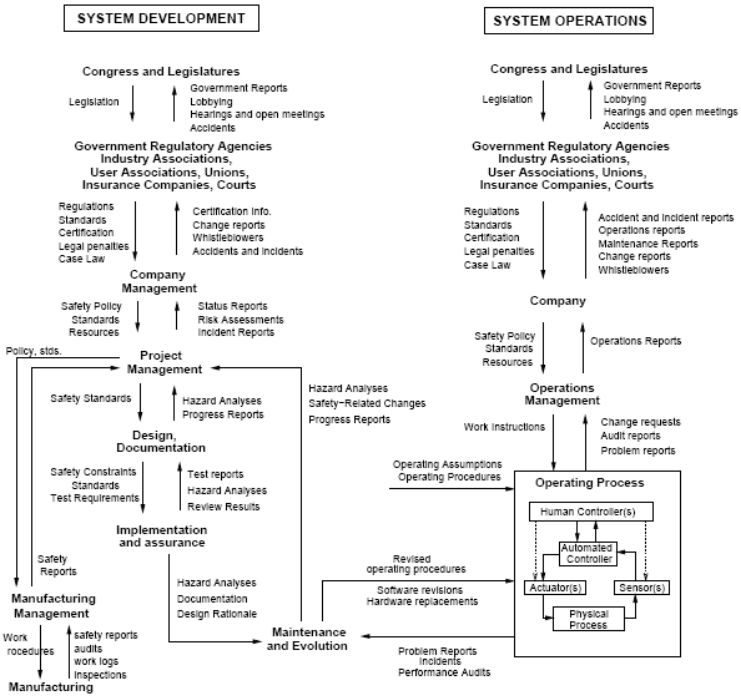


Figure 2-5. General Form of a Model of Socio-Technical Control

The model is similar to the one devised by Rasmussen and Svedung but their model contains only one control structure and the focus is on operations and not development (Rasmussen and Svedung, 2000). The model in Figure 2-5 has two basic hierarchical control structures one for system development (on the left) and one for system operation (on the right) with interactions between them. An aircraft manufacturer, for example, might only have system development under its immediate control, but safety involves both development and operational use of the aircraft, and neither can be accomplished successfully in isolation: Safety must be designed into the system, and safety during operation depends partly on the original design and partly on effective control over operations. Manufacturers must communicate to their customers the assumptions about the operational environment upon which the safety analysis was based, as well as information about safe operating procedures. The operational environment in turn provides feedback to the manufacturer about the performance of the system during operations.

Between the hierarchical levels of each control structure, effective communications channels are needed, both a downward reference channel providing the information necessary to impose constraints on the level below and an upward measuring channel to provide feedback about how effectively the constraints were enforced. Feedback is critical in any open system in order to provide adaptive control. At each level, inadequate control may result from missing constraints, inadequately communicated constraints, or from constraints that are not enforced correctly at a lower level.

The top two levels of each of the two generic control structures are government and general industry groups. The government control structure in place to control development may differ from that controlling operations-a different group at the U.S. Federal Aviation Administration (FAA), for example, is responsible for issuing aircraft type certifications than that responsible for supervising airline operations. The appropriate constraints in each control structure and at each level will vary but in general may include technical design and process constraints, management constraints, manufacturing constraints, and operational constraints.

At the highest level in both the system development and system operation hierarchies are Congress and state legislatures. Congress controls safety by passing laws and by establishing and funding government regulatory structures. Feedback as to the success of these controls or the need for additional ones comes in the form of government reports, congressional hearings and testimony, lobbying by various interest groups, and, of course, accidents.

The next level contains government regulatory agencies, industry associations, user associations, insurance companies, and the court system. Unions may play a role in ensuring safe system operations (such as the air traffic controllers union) or worker safety in manufacturing. The legal system tends to be used when there is no regulatory authority and the public has no other means to encourage a desired level of concern for safety in company management. The constraints generated at this level and enforced on the companies are usually passed down in the form of policy, regulations, certification, standards (by trade or user associations), or threat of litigation. Where there is a union, safety-related constraints on operations or manufacturing may result from union demands and collective bargaining.

In the development control structure (shown on the left), constraints imposed on behavior by government and other entities must be reflected in the design of company safety policy, standards, and allocation of resources. Recent trends from management by oversight to management by insight reflect differing levels of feedback control exerted over the lower levels and a change from prescriptive management control to management by objectives, where the objectives are interpreted and satisfied according to the local context (Rasmussen, 1997). An attempt to delegate decisions and to manage by objectives requires an explicit formulation of the value criteria to be used and an effective means for communicating the values down through society and organizations. The impact of specific decisions at each level on the objectives and values passed down need to be adequately and formally evaluated. While some generic functions will be required at a particular level to avoid accidents, the details about how the functions will be accomplished may be left to the lower levels. New objectives may also be added at each level. Feedback is required to measure how successfully the functions were performed. Several recent aerospace accidents have been partly attributed (in the accident investigation reports) to an inadequate transition from management by oversight to management by insight (Leveson, 2001).

As an example, while government and/or company standards may require a hazard analysis be performed, the system designers and documenters (including those designing the operational

procedures and writing user manuals) may have control over the actual hazard analysis process used to identify specific safety constraints on the design and operation of the system. The design constraints identified as necessary to control system hazards are passed to the implementers and assurers of the individual system components along with standards and other requirements. Success is determined through test reports, reviews, and various additional hazard analyses. At the end of the development process, the results of the hazard analyses as well as documentation of the safety-related design features and design rationale should be passed on to the maintenance group to be used in the change process.

A similar process involving layers of control is found in the system operation control structure (the right half of Figure 2-5). In addition, there will be (or at least should be) interactions between the two structures. For example, the safety design constraints used during development form the basis for operating procedures and for performance and process auditing.

As in any control structure, time lags may affect the flow of control actions and feedback and may impact the efficiency of the control loops. For example, standards can take years to develop or change-a time scale that may keep them behind current technology and practice. In general, the actions of those at the lower levels of the control structure will usually be closer in time to the actual accident than those higher up in the structure (Rosness, 2001). In general, a common way to deal with time lags is to delegate control responsibility to lower levels that are not subject to as great a delay in obtaining information or feedback from the measuring channels. In periods of quickly changing technology, time lags may make it necessary for the lower levels to augment the control processes passed down from above or to modify them to fit the current situation. Accident analysis needs to include the influence of these time lags.

In the next section, general factors leading to accidents are identified by applying the concepts of constraints, basic control loops, and levels of control, as presented in this and the previous two sections.

2.2.4 A Classification of Accident Factors

It was hypothesized earlier that accidents result from inadequate control, i.e., the control loop creates or does not handle dysfunctional interactions in the process-including interactions caused both by component failures and by system design flaws. Starting from this basic definition of an accident, the process that leads to accidents can be understood in terms of flaws in the components of the system development and system operations control loops in place during design, development, manufacturing, and operations. This section presents a classification of those flaws. The classification can be used during accident analysis or accident prevention activities to assist in identifying the factors involved in an accident (or a potential accident) and in showing their relationships. Figure 2-6 shows the general classification.

In each control loop at each level of the socio-technical control structure, unsafe behavior results from either a missing or inadequate constraint on the process at the lower level or

inadequate enforcement of the constraint leading to its violation. Because each component of the control loop may contribute to inadequate control, classification starts by examining each of the general control loop components and evaluating their potential contribution: (1) the controller may issue inadequate or inappropriate control actions, including inadequate handling of failures or disturbances in the physical process; (2) control actions may be inadequately executed, or (3) there may be missing or inadequate feedback. These same general factors apply at each level of the socio-technical control structure, but the interpretations (applications) of the factor at each level may differ.

For each of the factors, at any point in the control loop where a human or organization is involved, it will be necessary to evaluate the context in which decisions are made and the behavior shaping mechanisms (influences) at play in order to understand how and why unsafe decisions have been made. Note that accidents caused by basic component failures are included here. Component failures may result from inadequate constraints on the manufacturing process; inadequate engineering design such as missing or incorrectly implemented fault tolerance; lack of correspondence between individual component capacity (including humans) and task requirements; unhandled environmental disturbances (e.g., EMI); inadequate maintenance, including preventive maintenance; physical degradation over time (wear out), etc. Component failures may be prevented by increasing the integrity or resistance of the component to internal or external influences or by building in safety margins or safety factors.

They may also be avoided by operational controls, such as operating the component within its design envelope and by periodic inspections and preventive maintenance. Manufacturing controls can reduce deficiencies or flaws introduced during the manufacturing process. The effects of component failure on system behavior may be eliminated or reduced by using redundancy. The model goes beyond simply blaming component failure for accidents and requires that the reasons be identified for why those failures occurred and led to an accident.

2.2.5 Inadequate Enforcement of Safety Constraints

The first factor, inadequate control over (enforcement of) safety constraints, can occur either because hazards (and their related constraints) were not identified (1.1 in Figure 2-6) or because the control actions do not adequately enforce the constraints (1.2). The latter may, in turn, result from flawed control algorithms (1.2.1), inconsistent or incorrect process models used by the control algorithms (1.2.2), or by inadequate coordination among multiple controllers and decision makers (1.2.3).

1. **Inadequate Enforcement of Constraints (Control Actions)**
   - 1.1 Unidentified hazards
   - 1.2 Inappropriate, ineffective, or missing control actions for identified hazards
     - 1.2.1 Design of control algorithm (process) does not enforce constraints
       - Flaw(s) in creation process
       - Process changes without appropriate change in control algorithm (asynchronous evolution)
       - Incorrect modification or adaptation
     - 1.2.2 Process models inconsistent, incomplete, or incorrect (lack of linkup)
       - Flaw(s) in creation process
       - Flaws(s) in updating process (asynchronous evolution)
       - Time lags and measurement inaccuracies not accounted for
     - 1.2.3 Inadequate coordination among controllers and decision makers (boundary and overlap areas)

. **Inadequate Execution of Control Action**
   - 2.1 Communication flaw
   - 2.2 Inadequate actuator operation
   - 2.3 Time lag

. **Inadequate or missing feedback**
   - 3.1 Not provided in system design
   - 3.2 Communication flaw
   - 3.3 Time lag
   - 3.4 Inadequate sensor operation (incorrect or no information provided)

Figure 2-6. A Classification of Control Flaws Leading to Hazards.

Inadequate Control Algorithms: Control algorithms may not enforce safety constraints (1.2.1) because they are inadequately designed originally, the process may change and thus they become in adequate, or they may be inadequately modified by maintainers (if they are automated) or through various types of natural adaptation if they are implemented by humans. Leplat has noted that many accidents relate to asynchronous evolution (Leplat, 1987) where one part of a system (in our case the hierarchical control structure) changes without the related necessary changes in other parts. Changes to subsystems may be carefully designed, but consideration of their effects on other parts of the system, including the control aspects, may be neglected or inadequate. Asynchronous evolution may also occur when one part of a properly designed system deteriorates. In both these cases, the erroneous expectations of users or system components about the behavior of the changed or degraded subsystem may lead to accidents. The Ariane 5 trajectory changed from that of the Ariane 4, but the inertial reference system software did not. One factor in the loss of contact with SOHO (SOlar Heliosperic Observatory) in 1998 was the failure to communicate to operators that a functional change had been made in a procedure to perform gyro spin down.

Communication is a critical factor here as well as monitoring for changes that may occur and feeding back this information to the higher-level control. For example, the safety analysis process that generates constraints always involves some basic assumptions about the operating environment of the process. When the environment changes such that those assumptions are no longer true, the controls in place may become inadequate. Embedded pacemakers, for

example, were originally assumed to be used only in adults, who would lie quietly in the doctor's office while the pacemaker was being "programmed." Later they began to be used in children and the assumptions under which the hazard analysis was conducted and the controls were designed no longer held and needed to be revisited.

Inconsistent Process Models: Effective control is based on a model of the process state. Accidents, particularly system accidents, most often result from inconsistencies between the models of the process used by the controllers (both human and automated) and the actual process state (1.2.2). When the controller's model of the process (either the human mental model or the software model) diverges from the process state, erroneous control commands (based on the incorrect model) can lead to an accident-for example, (1) the software does not know that the plane is on the ground and raises the landing gear or (2) it does not identify an object as friendly and shoots a missile at it or (3) the pilot thinks the aircraft controls are in speed mode but the computer has changed the mode to open descent and the pilot issues inappropriate commands for that mode or (4) the computer does not think the aircraft has landed and overrides the pilots' attempts to operate the braking system.

During software development, the programmers' models of required behavior may not match that of the engineers' (commonly referred to as software requirements error), or the software may be executed on computer hardware during operations that differs from that assumed by the programmer and used during testing. The situation becomes more even complicated when there are multiple controllers (both human and automated) because each of their process models must also be kept consistent.

The most common form of inconsistency occurs when one or more of the process models is incomplete in terms of not defining appropriate behavior for all possible process states or all possible disturbances, including unhandled or incorrectly handled component failures. Of course, no models are complete in the absolute sense: The goal is to make them complete enough that no safety constraints are violated when they are used. We have defined (or at least made progress toward defining) what it means for a software model of the process to be complete in this sense (Leveson, 1995) and are working on determining what the human controller's mental model must contain to safely control the process and to supervise automated controllers.

How do the models become inconsistent? First, they may be wrong from the beginning (e.g. incorrect software requirements). In this case, the design of the controller itself is flawed: there may be uncontrolled disturbances, unhandled process states; inadvertent commands of the system into a hazardous state, unhandled or incorrectly handled system component failures, etc.

In addition to not starting with an accurate model, models may become incorrect due to lack of feedback, inaccurate feedback, or inadequate processing of the feedback. A contributing factor cited in the Cali B-757 accident report was the omission of the waypoints behind the aircraft

from cockpit displays, which contributed to the crew not realizing that the waypoint for which they were searching was behind them (missing feedback). The model of the Ariane 501 attitude used by the attitude control software became inconsistent with the launcher attitude when an error message sent by the inertial reference system was interpreted by the attitude control system as data (incorrect processing of feedback), leading to the issuance of an incorrect and unsafe control command.

Other reasons for the process models to diverge may be more subtle. Information about the process state has to be inferred from measurements. For example, in the TCAS II collision avoidance system, relative range positions of other aircraft are computed based on round-trip message propagation time. The theoretical control function (control law) uses the true values of the controlled variables or component states (e.g., true aircraft positions). However, at any time, the controller has only measured values, which may be subject to time lags or inaccuracies. The controller must use these measured values to infer the true conditions in the process and, if necessary, to derive corrective actions to maintain the required process state. In the TCAS example, sensors include on-board devices such as altimeters that provide measured altitude (not necessarily true altitude) and antennas for communicating with other aircraft. The primary TCAS actuator is the pilot, who may or may not respond to system advisories. The mapping between measured or assumed values and true values can be flawed.

In addition, the control loop must necessarily include time lags, such as that between measuring values and receiving those values or between issuing a command and the actual process state change. Pilot response delays are important time lags that must be considered in designing the control function for TCAS or other aircraft systems as are time lags in the controlled process (the aircraft trajectory) caused by aircraft performance limitations. Delays may not be directly observable, but may need to be inferred. Depending on where in the feedback loop the delay occurs, different models are required to cope with the delays (Brehmer, 1992): dead time and time constants require a model that makes it possible to predict when an action is needed before the need arises while feedback delays require a model that allows prediction of when a given action has taken effect and when resources will be available again. Such requirements may impose the need for some type of open loop or feed forward strategy to cope with delays.

To summarize, process models can be incorrect from the beginning (where correct is defined in terms of consistency with the current process state and with the models being used by other controllers) or they can become incorrect due to erroneous or missing feedback or measurement inaccuracies. They may also be incorrect only for short periods of time due to time lags in the process loop.

Inadequate Coordination Among Controllers and Decision Makers: When there are multiple controllers (human and/or automated), control actions may be inadequately coordinated (1.2.3), including unexpected side effects of decisions or actions or conflicting control actions. Communication flaws play an important role here.

Leplat suggests that accidents are most likely in boundary areas or in overlap areas where two or more controllers (human and/or automated) control the same process (Leplat, 1987). In both boundary and overlap areas, the potential exists for ambiguity and for conflicts among independently made decisions.

When controlling boundary areas, there can be confusion over who is actually in control (which control loop is currently exercising control over the process), leading to missing control actions. The functions in the boundary areas are often poorly defined. For example, Leplat cites an iron and steel plant where frequent accidents occurred at the boundary of the blast furnace department and the transport department. One conflict arose when a signal informing transport workers of the state of the blast furnace did not work and was not repaired because each department was waiting for the other to fix it. Faverge suggests that such dysfunctioning can be related to the number of management levels separating the workers in the departments from a common manager: The greater the distance, the more difficult the communication, and thus the greater the uncertainty and risk.

Coordination problems in the control of boundary areas are rife. A Milstar satellite was lost due to inadequate attitude control of the Titan/Centaur launch vehicle, which used an incorrect process model based on erroneous inputs in a software load tape. After the accident, it was discovered that nobody had tested the software using the actual load tape-everyone assumed someone else was doing so (Leveson, 2001). In this case, system engineering and mission assurance activities were missing or ineffective, and a common control or management function was quite distant from the individual development and assurance groups. A factor in the loss of the Black Hawk helicopters to friendly fire over northern Iraq as that the helicopters normally flew only in the boundary areas of the No-Fly-Zone, and procedures for handling aircraft in those areas were ill-defined (Leveson, Allen, and Storey, 2002). Another factor was that an Army base controlled the flights of the Black Hawks while an Air Force base controlled all the other components of the airspace. A common control point once again was high above where the accident occurred in the control structure. In addition, communication problems existed between the Army and Air Force bases at the intermediate control levels.

Overlap areas exist when a function is achieved by the cooperation of two controllers or when two controllers exert influence on the same object. Such overlap creates the potential for conflicting control actions (dysfunctional interactions among control actions). In Leplat's study of the steel industry, he found that 67 percent of technical incidents with material damage occurred in areas of co-activity, although these represented only a small percentage of the total activity areas. In an A320 accident in Bangalore, India, the pilot had disconnected his flight director during approach and assumed that the co-pilot would do the same. The result would have been a mode configuration in which airspeed is automatically controlled by the auto throttle (the speed mode), which is the recommended procedure for the approach phase. However, the co-pilot had not turned off his flight director, which meant that open descent mode became active when a lower altitude was selected instead of speed mode, eventually contributing to the crash of the aircraft short of the runway (Sarter and Woods, 1995). In the

Black Hawks' showdown by friendly fire, the aircraft surveillance officer (ASO) thought she was responsible only for identifying and tracking aircraft south of the 36th parallel while the air traffic controller for the area north of the 36th parallel thought the ASO was also tracking and identifying aircraft in his area and acted accordingly.

2.2.6 Inadequate Execution of the Control Action

A second way for constraints to be violated in the controlled process is if there is a failure or inadequacy in the reference channel, i.e., in the transmission of control commands or in their execution (actuator fault or failure). A common flaw in system development is that the safety information gathered or created by the system safety engineers (the hazards and the necessary design constraints to control them) is inadequately communicated to the system designers and testers.

2.2.7 Inadequate or Missing Feedback

The third flaw leading to system hazards involves inadequate feedback. A basic principle of system theory is that no control system will perform better than its measuring channel. Important questions therefore arise about whether the controllers or decision makers (either automated or human) have the necessary information about the actual state of the controlled process to satisfy their objectives. This information is contained in their process models and updating these models correctly is crucial to avoiding accidents (1.2.2). Feedback may be missing or inadequate because such feedback is not included in the system design (3.1), flaws exist in the monitoring or feedback communication channel (3.2), the feedback is not timely (3.3), or the measuring instrument operates inadequately (3.4).

The ActorMap (Figure 3-1) shows all relevant actors involved directly or indirectly in the accident. Directly only actors from Levels 5 (and 6) are involved. That is something expected since actors like the flight crew and maintenance/ground engineer are those whose actions were constituents in the accidental chain of events. But how the distant upper levels actors are involved since the accident is well documented to be caused from Level 5 events?

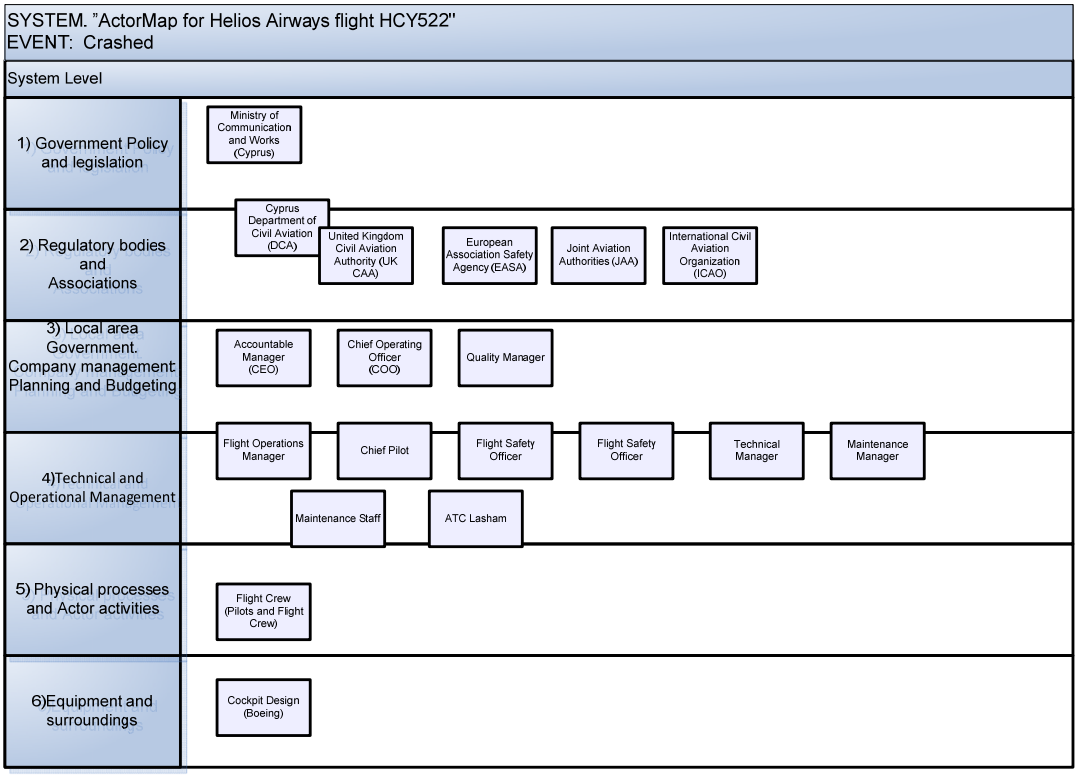
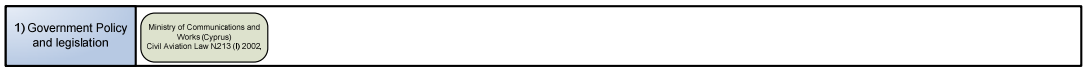


Figure 3-1. ActorMap showing the accident actors.

The AcciMap will reveal those relationships. How the upper decision making (or lag of decision making) shaped the preconditions of this accident.

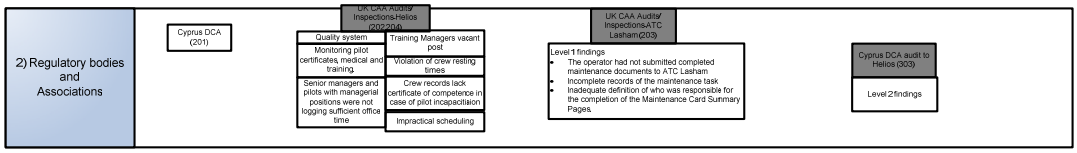
Usually an accident analysis starts by individually presenting the direct events that form the causal chain. In analyzing the AcciMap a different approach will be attempted. Analysis will commence from Level 1.

3.1 Level 1 the Government Policy and Legislation .



In the Republic of Cyprus the Ministry of Communications and Works provides the legislation and budget of the Cyprus Department of Civil Aviation (Cyprus DCA). The Law 213(I)/2002-last amendment 2004, transfer of regulations from the JAA to EASA – is the Aviation Law of the State, based on which the Cyprus DCA conducts its oversight duties. The budget and resources provided by the state will have a negative impact on how the Cyprus DCA is structured and staffed.

3.2 Level 2 the Regulatory Bodies and Associations.



3.2.1 The Cyprus Department of Civil Aviation

The Cyprus DCA as stated before is responsible for fulfilling the State's responsibility under the Convention of International Civil Aviation (also known as the Convention of Chicago). These responsibilities include the licensing of operational personnel, the certification of aircraft, air operators and maintenance organizations.

Several audits (from ICAO, JAA, EU and a Private Firm) revealed severe deficiencies in Cyprus DCA [201][3]. There was insufficient and inadequately trained and qualified staffing of the DCA. Also the organizational structure and record keeping was another obstacle in performing its oversight duties. These deficiencies are attributed to the fact that the necessary resources from the state (ministry) were not provided. The DCA was just a ministry department; it had limited authority due to legislation and limited effectiveness due to understaffing (both in numbers and qualification) in carrying out its duties.

Due to above incapacitation and in order to accomplish, the Cyprus DCA contracted with the United Kingdom's Civil Aviation Authority (UK CAA). UK CAA carried out on behalf of Cyprus DCA inspections required by the ICAO and EU.

[3] Numbers in [] refer to table items of Appendix B

3.2.2 The UK CAA

Based on contraction the UK CAA had an advisory role and had no legal authority to enforce any actions concerning inspection findings. This was also clarified to a letter sent from UK CAA to the Minister of Communication and Works. The letter also underlined the fact that for any operator's audit findings the responsibility and decision rests to DCA for the implementation of any corrective actions. Also the philosophy of this collaboration was to train the Cyprus DCA staff and prepare them to perform these inspections without the support of UK CAA. The Cyprus DCA instead of gaining advantage of exchange of technical knowledge, due to its own deficiencies, in reality delegated its oversight duties to UK CAA. The Cyprus DCA seemed to accept UK CAA's audits reports without any criticism and even forwarded them to the operator (in the case of Helios) without any comments or even a signature.

Nevertheless the audits provided the frame in which the operator (Helios Airways) and its maintenance contractor (ATC Lasham) operated. Helios Airways audits reports [202,204] uncovered deficiencies in vital areas. In the level of management the operator seem to have repeated deficiencies in areas of:

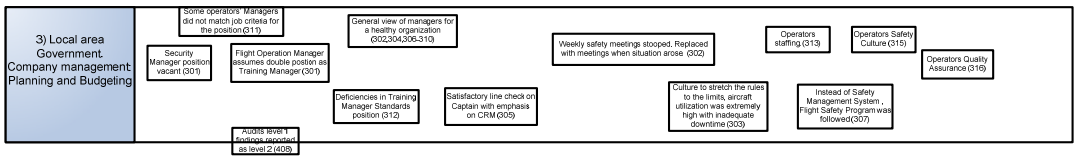
1. Staffing managerial position with competent personnel
2. Quality System and Assurance
3. Updating Training Manuals
4. Monitoring and updating training files, as well as several flight crew certificates.
5. Crew Scheduling and resting times.
6. Pilots with managerial positions were not logging sufficient office times.

The audit of July 2004 stated that "The lack of operational management control is now unacceptable as there is evidence of flight safety being compromised" , the more alarming "Aircraft Inspection/ Facilities and Organization Inspection characterized as symptomatic of a lock of operational management control which had resulted in pilots being cleared to operate public transport flights without the necessary competence etc" and finally "Crew records lacked certificate of competence in case of pilot incapacitation".

The UK CAA also audits ATC Lasham, the maintenance contractor of the operator[203]. The audits revealed a continued problem concerning maintenance. In fact this was a Level 1 finding at which Helios Airways (JAR OPS) Maintenance Management approval and AOC will be suspended. The problem was that the operator failed to submit to ATC Lasham (the maintenance contractor) completed maintenance documentation. Also ATC Lasham failed to acquire this documentation and quit efforts after several trials. Surprising is the fact that those findings were temporarily set to Level 2 and those critical findings were cleared later by a meeting between the UK CAA inspector ,the Technical Manager of ATC Lasham and the Operator.

From the above audits, the initiation of proposing several action plans to the critical situations from the oversight authority, in this case the Cyprus DCA is clearly absent. Although the UK CAA alerted several times the Cyprus DCA.

3.3 Level 3 Local area Government, Company Management Planning and Budgeting.



In Level 3 the management of the operator in this case Helios Airways is examined.

In addition to the audit findings the operator suffered from deeper deficiencies. To begin with the qualifications of some managers did not correspond to those required by job descriptions [311]. Added to that there was a vacant Security Position and the Training Manager's position that came up in several audits was assumed by the Flight Operations Managers. Also there was a general view of some managers that a healthy organization existed with a conductive environment of safety and quality [302-306,310]. Only the Chief Operating Officer had a different opinion [303] as it seem to him that there was a culture of fear where people were encouraged to stretch the rules to the limits. He found aircraft utilization to high with inadequate down time and that schedules were extremely tight and that was evidence that flight times were manipulated to bring them into limits.

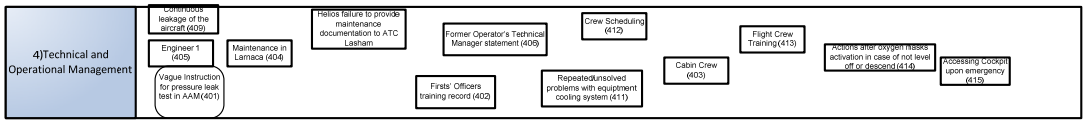
As far as the working environment concerns, the management believed that a 'friendly' management was conducted on the other hand there were complaints from employees e.g characterized the Accountable Manager as unapproachable with little concern for safety and well being of the company employees [311]. The working environment was shaped also by the fact that were seasonal employees with contract, this might gave them the feeling that were not important for the company and discouraged them to be conductive in team spirit, an essential precondition for safety[313]. The multicultural spectrum of employees in the operator gave some rise to unofficial complaints mostly related to the fact that different cultures have different perceptions about characters [313]. Due to unofficial complaints the accident's captain was put on a line check with emphasis on CRM giving satisfactory results.

The deficiencies in the Training Manager Standards position (often vacancies, assumed by another manager) are of key importance in the accident[312]. It is associated with the incapability of monitoring crews training files and give remedies to any arising issues. Such an example is the repeated comments in First's Officers records concerning omissions in check lists and SOP's in non normal circumstances.

The Quality assurance [315] was ill too. After the audit findings, eventually a Quality Manager was appointed. There is no evidence that internal management evaluation was taking place or corporate manuals were updated. In the case of Quick Reference Handbook the Flight Operations Manager incorporated only important to his judgment updates issued by the manufacturer. The After Takeoff Checklist was not revised as "AIR COND & PRESS…ON" and "PACKS…..AUTO" from "AIR COND & PRESS….SET".

Finally the Safety Culture [314] existed in the operator, apart from stretching the rules and replacing weekly safety meetings with meetings when needed [302], was laid through manuals and through the Flight Safety Program [307]. It is not clear if operator met those standards that were described as reactive instead of proactive and did not point out clearly the role of management in ensuring and maintaining safe operations of the company.

3.4 Level 4 Technical and Operational Management.



In level 4 the Technical and Operational Management is examined.

The Line Maintenance in Larnaca was found to have deficiencies concerning maintenance documentation [407] also a line audit by ATC Lasham in June 2005 found deficiencies concerning manpower planning, processing matters , documentations material and equipment management [404]. The high rate of personnel change over did not favor the good setting of a proactive management. Also there is a question if the personnel were receiving the required refreshers courses by the MME. Engineer 1 who was responsible for the unscheduled maintenance was not aware of such courses.

Concerning the maintenance that took place before the accident flight due to a vague instruction in AMM [401] the pressurization mode selector was left to the MAN position. Also the relevant tests were not documented or even carried out as prescribed. In addition the aircraft suffered from repeated leakages [409] and problems with equipment cooling system [411]. Maintenance actions were of no remedy.

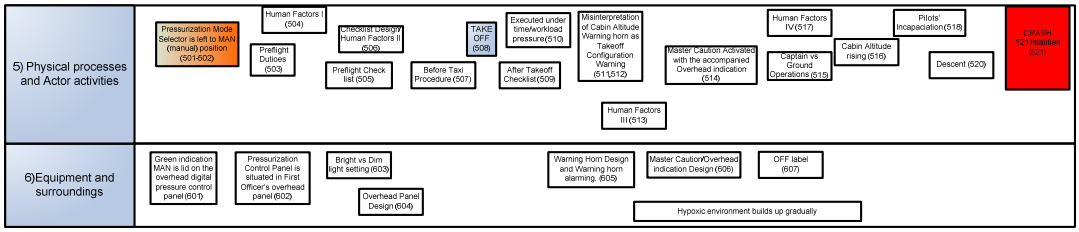
The above are results of the degeneration of the managerial and auditors levels. Since maintenance documentation is not provided to the maintenance contractor and since the oversight authority is unable to take measures; there is not other way to secure that maintenance is done accordingly to the required standards.

Another impact of the same degeneration (associated with Training Manager position deficiencies and lack of training monitoring mechanism) is that Firsts Officers' training record goes unnoticed since there is continue failure to monitor flight crew certificates and training

[402,403,413]. Concerning the accident in audit of June 2004 one finding stated that Crew records lack certificate of competence in case of pilot incapacitation. Also cabin crew training syllabus included only rapid decompression situations. Thus the crew was not trained to recognize gradual loss of pressure as in the case of the accident. In addition they were no instructions for actions after oxygen activation in case of not level off or descend and accessing cockpit upon emergency [414-415].

The vague instruction let the pressurization selector in MAN position, this the point were Level 4 connects to the causal events sequences in Level 5 and 6. Also the unnoticed First Officers omissions with checklists and SOP's as well as the tendency to overreact in non-normal situations will affect greatly the chain of events. Since such omissions will be made during the before and after takeoff check lists and a non normal situation will be resulted. Also there will be a question of how effective the CRM line check was on captain since the events suggested that he failed to implement such CRM, also the last safeguard against pilots incapacitation is dropped due to inadequate training. Level 5 and Level 6 present these events.

3.5 Level 5 Physical processes and Actor activities and Level 6 Equipment and Surroundings



The pressurization mode selector is left to MAN position from the previous pressure leak test [501-502]. The associated green indication MAN lids on the pressurization panel [601-604]. The before take off checklists and duties [503-505-507] are coupling with the hurried manner that are being executed (since scheduling is tight, there is a need to meet departure times), human factors concerning repeated tasks [504-506] and the First Officers' tendency for checklist omissions [402] results to the take off of the plane with the pressurization selector on MAN position. The after take off checklist [509] which is executed under workload pressure and in conjunction again with Firsts Officers omissions on checklists, the selector remains on MAN position although pressurization is the first item to check on after take off list. Just after FL100 Cabin Altitude warning is sounded and is misinterpreted as Takeoff configuration warning due to the fact that the sound is the same [511,512,606]. The warning horn still sounds creating a stress environment in addition Master Caution/Overhead [514] is activated and because is not canceled for 52 s from the two events that happened and could activate Master Caution the one goes unnoticed. Since the passenger oxygen indication is situated at the aft overhead panel it seems that captain concentrated on the equipment cooling OFF lid indications the other event

that activated Master Caution. Meantime hypoxic conditions are prevailing. The Captain seems to be preoccupied with the equipment cooling and loses valuable time in trying to troubleshoot this symptom with the Ground Engineer [515,517,607]. Cabin altitude is rising until hypoxia prevails and pilots' incapacitation is resulted. Aircraft continues flight through the Flight Management System. Due to inadequate training and lack of instructions the cabin crew doesn't respond in the passengers oxygen mask activation and in the fact that the aircraft is not leveling off or descending. If that training was available the Flight Attendant in descent phase [520] would have entered cockpit in time [415] and follow Pilots' Incapacitation Procedures. The plane eventually crashed due to fuel starvation resulting 121 fatalities [521]. From the above the AcciMap (Figure 3-2) for the accident is constructed.

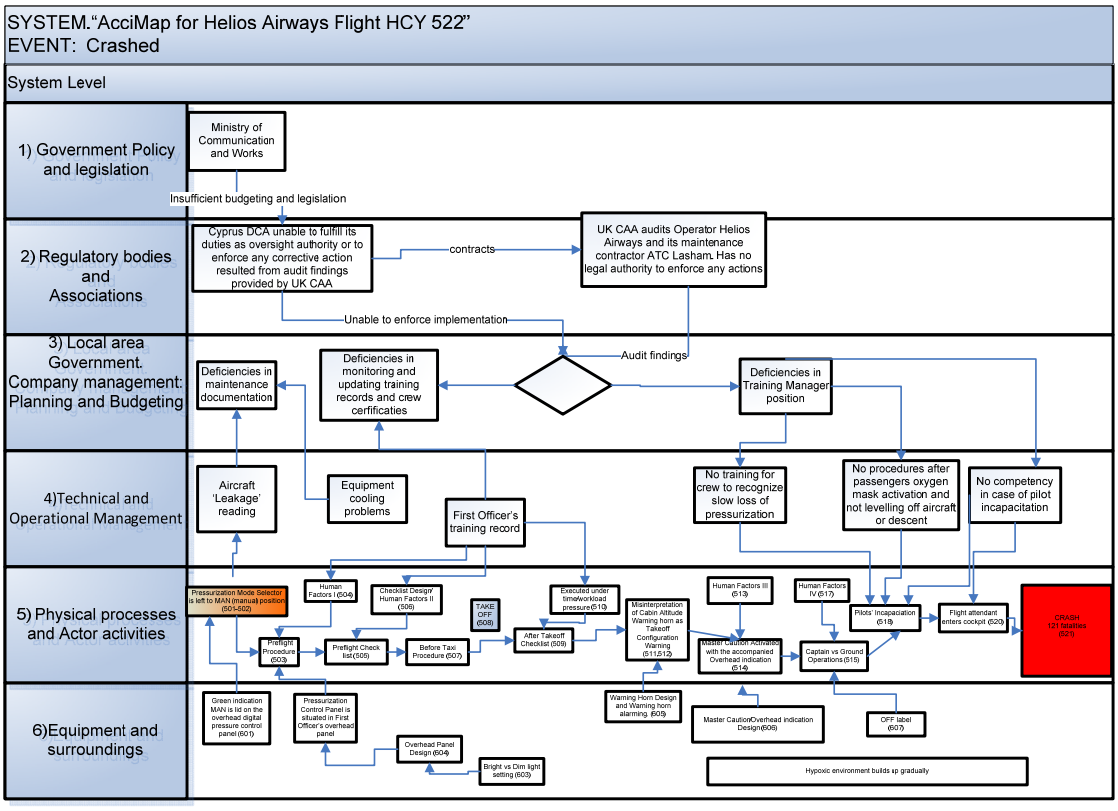


Figure 3-2. The AcciMap of Helios Airways crash

Chapter 4 Analysis using STAMP

STAMP treats accidents as a control failure. In other words an accident is caused from a failure of a system to enforce the predefined safety constraints. Predefined is the key word here. We cannot expect from our system to enforce safety constraints that we have not provided through design. A system may be broken down to various subsystems which have system properties on their own. A failure in a sub system, or a hazard release, might migrate through the rest of the subsystems, causing the whole system to collapse. This collapse in the case of our study is called an accident. Thus STAMP investigates how ill defined are safety constrains in the constituent subsystems or how ill those constraints are enforced allowing the hazard migration.

STAMP is implemented through the following steps:

1. First in STAMP the hierarchical structure is defined (Figure 4-1).

2. Secondly the physical process under control is defined.

3. Thirdly Operators at different control levels are investigated in the context of:
   - Safety Requirements and Constraint
   - Context in which Decision is made
   - Inadequate Control Actions
   - Mental Model Flaws

4. The Dynamic (Adapted) Structure is then presented.

5. The System (Behavioral) Dynamics model is constructed.

4.1 The Physical Process under control:

The Physical Process under control as far as this accident concerns is to provide human sustained and a comfortable environment for both passengers and flight crew in order to perform their duties. As aircraft climbs ambient pressure drops since air gets ‘thinner’ and this condition does not favors the human sustained environment. Thus pressurization of the aircraft is needed. Pressurization is achieved by properly handling the aircraft. In other words the pilots control the pressurization system provided by the aircraft manufacturer through an interface- the pressurization control panel- and the relevant instructions in the relevant manuals.

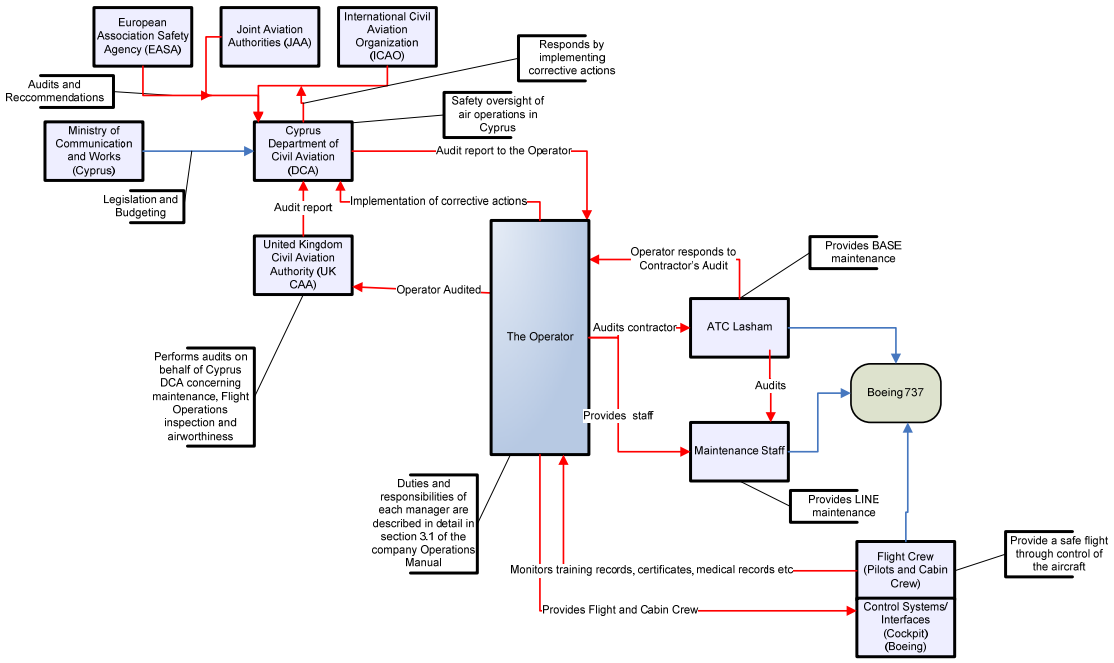


Figure 4-1. The system's control structure.

4.2 Hazard Source:

During an unscheduled maintenance in the morning prior flight, the pressurization mode selector was left to MAN position. The relevant AMM instruction for the pressure leak test requested that aircraft to be restored to its original position without explicitly requesting that the mode selector should be placed to AUTO position. Also the ground engineer who performed the maintenance did not brief the Captain of the flight on any of his actions performed in the flight deck.

4.3 The Operational Line controllers/operators (Figure 4-2).

4.3.1 The Manufacturer: Boeing

At this first level of control structure the aircraft manufacturer is involved in the design of the pressurization system panel, the design of checklists/manuals and several warnings and the instructions in the Aircraft Maintenance Manual.

The instruction in the AMM for the pressure leak test did not included an action of returning the pressurization mode selector to AUTO although for the test required the selector to be placed in the MAN position. Thus the instruction "Put the Airplane Back to its Initial Condition" effectively does not serve the safety constraint that it was meant to. Since pressurization is critical in a

flight and since such tests take place on the flight operating grounds there should be an explicit instruction for the selector to be in AUTO position after test was completed. This explicit recall for AUTO position is not found even in the checklists for preflight procedure and after takeoff.

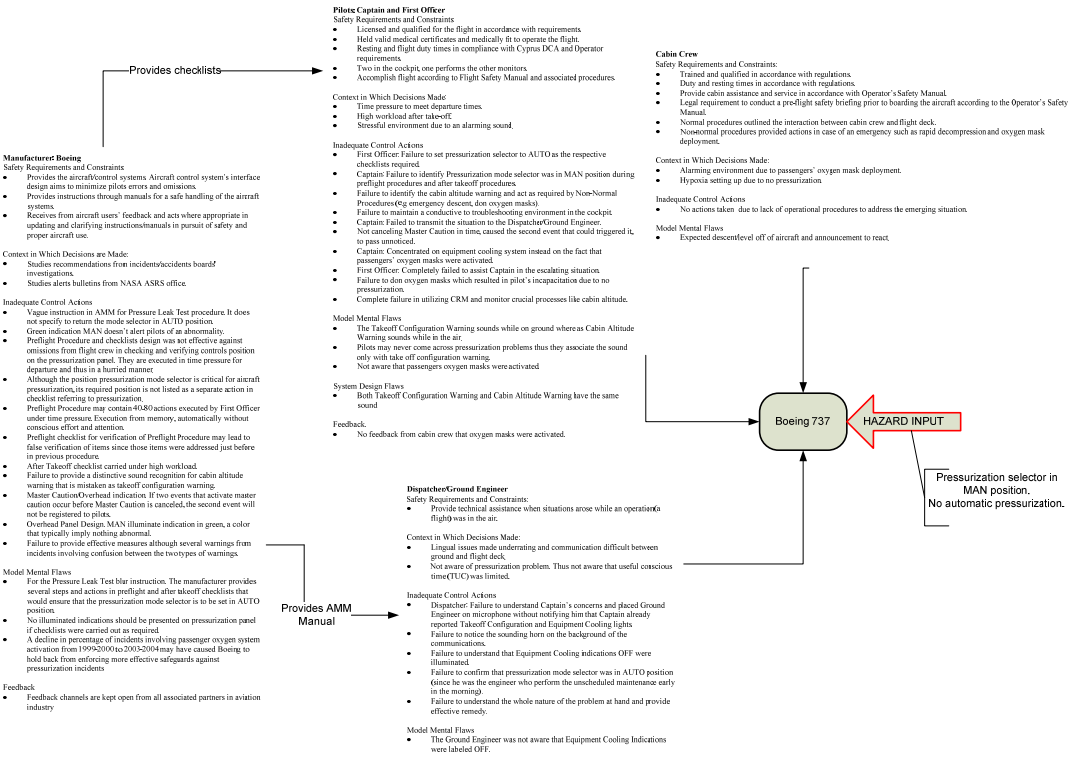


Figure 4-2. Operational Line Control Structure

Although these checklists were by design to ensure that the aircraft will be properly set for flight independent of any prior maintenance. Coming to the Preflight Procedure the First Officer needs to perform between 40 and 80 actions under the pressure to meet departure time and having the captain waiting for the checklist. Thus execution of actions is done automatically from memory and empirical rules from the topology of panels favoring omissions. Also assumptions might take place since the mode selector is rarely not in AUTO position. In fact only in the case that pilots need to fly the plane in manual pressurization the selector is turned to MAN. In the Preflight Checklist the item 12 of 25 concerns pressurization panel: "AIR COND & PRESS…. _PACK(S), BLEEDS ON SET". This action combines two systems, air condition and pressurization in which the first two responses concern the former and only one concerns the latter-pressurization. In fact the SET confirmation refers to eight different actions performed in Preflight Procedure and in the end First Officer's SET response verifies only that landing and cruise altitudes are properly set. The very first thing in After Takeoff list is to check the pressurization system setting. But after take off the pilots have a high workload in concurrent tasks (e.g retracting landing gear and flaps, monitoring climb, ATC communication). Managing concurrent tasks might lead to insufficient attention devotion to some of the tasks performed. As it is obvious that manufacturer intention was to ensure that pressurization is set properly by

the repeated references to set and verify the selector position, the position remained false even after takeoff. The checklists and preflight procedure failed in this case to enforce the safety constrain of ensuring that aircraft is properly configured for flight. Up to this point the failure is attributed to effect of human performance factors under the conditions prevailing in the enforcing of the constraint. Due to high work load (Preflight Procedure contains 40 to 80 actions) under the time pressure to meet departure times and executing tasks without conscious effort. After takeoff; management of concurrent tasks let to the slipping off the selector in wrong position. The above human factor performance and conditions in carrying out checklists should be considered in the design of such procedures. Of course there are other disturbances that amplified the above but there are also compensation factors that failed in this occasion.

Further on, the illuminating green indication MAN on the pressurization panel went unnoticed by the pilots although no illumination under normal settings should be visible. This failure of another safeguard is merely due to the human factor performances described above and more specifically to the being bias on something that you don't expect to see is left unnoticed. In addition green color is not alarming, is not connected with anomalies and may be this is another reason of not paying the necessary attention to it.

The design of the cabin altitude warning of having the same sound with another warning that is not relevant to altitude effects cancels its effectiveness by practice. The intention of the manufacturer was that takeoff configuration warning sounds only on the ground thus there is no possibility to be confused with altitude warning sounding in the air, above 10 000 ft. This intention is countered by flight practice. Pilots are not likely to experience a cabin pressurization problem during their career thus the specific horn sound for most of them is associated with the takeoff configuration. Another safeguard provided by design was the cabin altitude cut button "ALT HORN CUT OUT" which halts the annoying horn sound which may develop stress. In order to use that button the crew needed first to understand that the problem is associated with cabin altitude rising which in the case of accident they did not.

The design of the Master Caution/Overhead indication is another major safety barrier. It directs pilots' attention to illuminated information on the overhead panel. The constrained imposed by this tool were countered by the fact that only one event could trigger the Master Caution/Overhead indication while it was already lid. As it happened in the case of the accident, due to the fact the master caution was not cancelled for about 52 sec, two event occurred that were able to trigger it. Thus only the first event would be noted to the pilots from this warning tool. Of course the second event would have its presence on the overhead panel but it was not noted to the pilots through master caution. Here the placement on the overhead panel of the two information may had played a role. The equipment cooling system indication are further ahead in relation to PASS OXY ON light which is situated in the aft over head panel notifying pilots that passengers oxygen masks are deployed. Thus the captain concentrated on equipment cooling problem rather on oxygen mask deployment which would had given him critical clues for

the pressurization problem. Again these safety constraints ineffectiveness's are also coupled by other safeguard failures discussed further down.

The last safety inadequacy that can be attributed to the manufacturer is its slow response to feedback given from several incidents concerning the confusion with cabin altitude warning horn. Some remedial actions were taken such as revised checklists, the immediate don of oxygen by pilots and steps in ensuring the air condition settings. A decline in percentage of incidents involving passenger oxygen system activation from 1999-2000 to 2003-2004 may have caused Boeing to held back from enforcing more effective safeguards against pressurization incidents. After the accident and recommendations by Greek AAIASB, two warning lights indicators that read "TAKEOFF CONFIG" and "CABIN ALTITUDE" are installed in the front cockpit panel and provide indication along with sounding horn. This is a decisive step by manufacturer and FAA in safeguarding against confusion between the two warnings.

From the above analysis we have seen a failure of following checklists and procedures provided by the manufacturer as safety barriers mainly due to human factors performance. As a consequence we look now at the operators or the human controllers whose one of their duties was to carry out those procedural tasks. Together with the pilots the cabin crew made up the controllers on board during flight. The pilots were also assisted by a ground engineer through in a case of unexpected occurrences.

4.3.2 The Pilots: Captain and First Officer

The Captain and First Officer are examined jointly, as one component although they are two different individuals. This is because their duties during flight can be interchanged. The core philosophy of having two pilots is that the one carries out the task and the other is monitoring that the task is carried out properly. So the two human controllers in the cockpit is the first safety barrier identified. In addition pilots are qualified, in our days holders of a university degree and licensed. The license is obtained after training and several flight hours. The Air Transport Pilot License (ATPL) is issued in accordance with JAR-FCL and they are of different categories and ratings. They are also valid for specific time and require renewal. These are other constraints ensuring the capability of the pilots to fly a plane. The accident pilots were licensed and qualified and held medical certificates as regulations required. They also past through Operator Proficiency Test, Line Check, Recurrent Training in STD and CRM training during 2005. All these qualifications should balance out those human factor performance deficiencies described previously when carrying procedural settings and checklists verifications. At this point the Firsts Officer's training records reveal deficiencies in carrying out standard operations procedures. The First Officer violated the safety constraints set by the checklists. The Captain also failed to verify when calling the checklists that settings were as required. Thus there is a double failure by the two controllers in configuring properly the aircraft. This failure persisted even after take off although the first thing to check was the pressurization. Flight crew procedures are described in Flight Crew Operations Manual (FCOM). The above duties and tasks are under Normal Procedures. According to Area Responsibility the pressurization section of the

Overhead Panel was in responsibility of the First Officer, while the aircraft was on the ground and Pilot Monitoring while the aircraft was in the air.

In the situations followed there was failure from both to identify the correct identity of the warning horn. They misinterpret it as takeoff configuration warning as their reaction reveals. As discussed previously although the sound is connected to two different warnings, one sounding while on ground (takeoff configuration) and the other one while in air (cabin altitude warning). The fact that the warning was misinterpreted, gave failure to another safety constraint. Non-Normal Procedures (according to Quick Reference Manual) provides precise actions in case of cabin altitude warning horn sounds and in addition the Operator's Standard Operating Procedures Manual required that the flight crew should don oxygen masks. Cabin altitude warning horn continued to sound in the cockpit causing stress and distraction from resolving the problem. This is another failure by the pilots to maintain an environment that would help in piecing out messages from the aircraft. It is not clear from the report if a universal button existed for canceling all types aural warnings or if that warning horn could only be canceled by pressing the ALT HORN CUTOUT button. For the second case the pilots needed to identify first that they were dealing with pressurization problem in order to use that button.

The deterioration of the situation revealed that at least the last CRM tests proved to be ineffective. The Captain failed to transmit the situation to the ground mainly due to the environment described above, to lingual problems since he was called to describe an emergency situation in English- not his mother tongue language and to the fact that cabin altitude was rising and hypoxia was prevailing as time passed. Also both pilots failed to notice that oxygen masks were deployed as the overhead sign illuminated mainly because of the fact that equipment cooling illuminations also triggered by master caution were far ahead in the overhead panel. The fact of not canceling master caution for about 52 seconds caused a second event that triggered it to pass unnoticed. Oxygen mask deployment would be a crucial hint to the pilots of the source of the problem and would immediately react by don oxygen masks and start immediate descent to reach a flight level below 14 000 ft. Instead the Captain concentrated on Equipment Cooling system maybe because he was aware of associated write-ups in aircraft's technical log .

Since pilots during the whole sequence of warnings and overhead illuminations never considered a pressurization problem, hypoxia prevailed as aircraft continue its ascent and flight through Flight Management System.

Pilots' incapacitation is the result of all the above violations of safety barriers such as procedures and checklists provided by the operating manuals, misinterpretation of warning horn and overhead indications and failure to resolve the problem even with the aid of the Dispatcher/Ground Engineer.

4.3.3 Cabin Crew

Apart from the pilots in the cockpit the aircraft is staffed with another group of crew. The cabin crew among the duties of cabin service had a legal requirement to conduct a pre-flight safety briefing prior to boarding the aircraft according to the Operator's Safety Manual. Thus the cabin crew was another safety barrier in ensuring a safe flight. The briefing included exchange of flight information between the Captain and the Senior Cabin Attendant as well as assigning emergency exits and duties to individual cabin crew members. Communication guidelines and communication establishment between cabin crew and the cockpit were also provided in the Safety Manual. Specifically under Normal Operations required that flight deck must be called every 20 minutes via the interphone and that all communications (normal and non-normal checks) are to be made through interphone system to maintain a high standard of security. Also below flight level 10 000 ft , Climb and/or Descent the cabin crew shall avoid disturbing the Flight Deck and the flight deck door shall remain locked throughout all phases of flight until engine shutdown. The last requirements were due to security reasons but communication between flight deck and cabin was clearly required. Under Non-normal procedures of the Safety Manual, in the event of an emergency the Cabin Chief immediately contacts the cabin crew for instructions Also it stated that since two emergencies can't be alike the aircrew must use common sense and be prepared to modify standard procedures in the interest of safety. There were procedure regarding rapid decompression, accompanied with physical characteristics and effects. Among the actions provided the cabin crew should remain seated until the aircraft had leveled off. When the aircraft has leveled to a safe altitude the captain must notify the Senior Cabin Attendant by making a specific announcement. As a subsequent action after the aircraft has leveled off, the Senior Cabin Attendant is to check/report to the flight deck. Procedures for dealing with pilot incapacitation were also provided. For situation of Suspected Dual Pilot Incapacitation the Senior Cabin Attendant was instructed to bang on the flight deck door and if no reply was received to use the emergency access panel to enter the flight deck. It is clear that none of the above were conducted by the cabin crew. Some cabin crew members stationed at the front (Chief Cabin attendant) could hear the warning horn and added to the fact that oxygen masks were deployed the crew should react. But the procedures required the crew to remain seated until aircraft is leveled off and, the aircraft was still climbing, the Chief Cabin Attendant would expect an announcement calling him to the flight deck and informing the rest that is safe to remove the oxygen mask. No such announcement was made and there were no procedures covering this emerging situation. Thus it was left to the initiatives of the crew members to improvise in such cases as they were trained. Also the cabin crew's procedures and training included rapid decompression situations. It seems that the cabin crew was never considered with the case of slow loss of pressurization, thus they couldn't detect the physical symptoms associated and consequently its detection. Conclusively the lack of procedures covering the situation of oxygen mask deployment-no descent / level off-no announcement and the lack of training considering in gradual loss of pressure (or no pressurization) let the cabin crew inactive in those crucial limited minutes.

4.3.4 Dispatcher/Ground Engineer

The capability of the flight deck to communicate with the operator's ground operations was the last safety defense provided in resolving emergency situations that concerned the aircraft systems. In this case, after the Captain had reported Takeoff Configuration warning and Equipment Cooling lights the Dispatcher due to Captain's accent failed to understand his concerns and placed the Ground Engineer without briefing him on what was already reported. Due to the fact that the Ground Engineer was not aware that indications concerning Equipment Cooling were labeled OFF, at Captain's report that cooling lights were off he did not comprehend that OFF indications were illuminated as a result of the low density air sensed by the equipment cooling detectors. Thus the Captain's statement did not make sense to him as the natural states of those indications were off. The Ground Engineer ask Captain to verify that pressurization mode selector was in AUTO position but the Captain's reply seem that he was not worrying about pressurization and asked the location of the associated with equipment cooling circuit breakers. The Ground Engineer also did not hear the sounding horn at the background of communications something that would identify as cabin altitude warning since the aircraft was in the air The language difficulties seemed to prolonged the ineffective dialogues at a expense of limited consciousness time due to cabin altitude rising. Communication difficulties can also be the result of hypoxic symptoms that started to develop after passing the 14 000 ft. It seems that lingual issues inactivated the safety constraints that could be imposed by the ground operations

The look at the ground operations bring us to the end of the first level operator analysis. By now it is obvious how one switch remained in the wrong position, although is situated in a clear visual position just above First Officer in the overhead panel. How the many safety barriers failed to impose the prescribed safety constraints and consequently the failure to keep the physical process (lower pressure as aircraft ascends) under control (pressurization). The main factor that can be retrieved from the above analysis is that those safety barriers were designed in a static structure whereas events in real life are dynamic and a system tends to adapt in such situations. The dynamic adapted structure of the system will be presented further down in the analysis.

4.4 The Managerial Control Structure (Figure 4-3)

The sources of those ill designed safety barriers should be investigated. For example the lack of cabin crew procedures in case of oxygen mask deployment and not having aircraft descending. The focus turns now to the upper level operators which are:

- The Operator's Management (Management)
- The Operator's Staff (Staff)
- The Maintenance Contractor (Maintenance)

4.4.1 The Operator's Staff

The Operator's staff had a multinational composition and its official language of communication was English. Multinational teams have issues of different perception due to their different cultural background. The accident's Captain who was German was seen by some Cypriot's colleagues who were Mediterranean as unfriendly or authoritative due to his direct manner of conductive the SOP's or his unwillingness to deviate from typical procedures. None of the non-

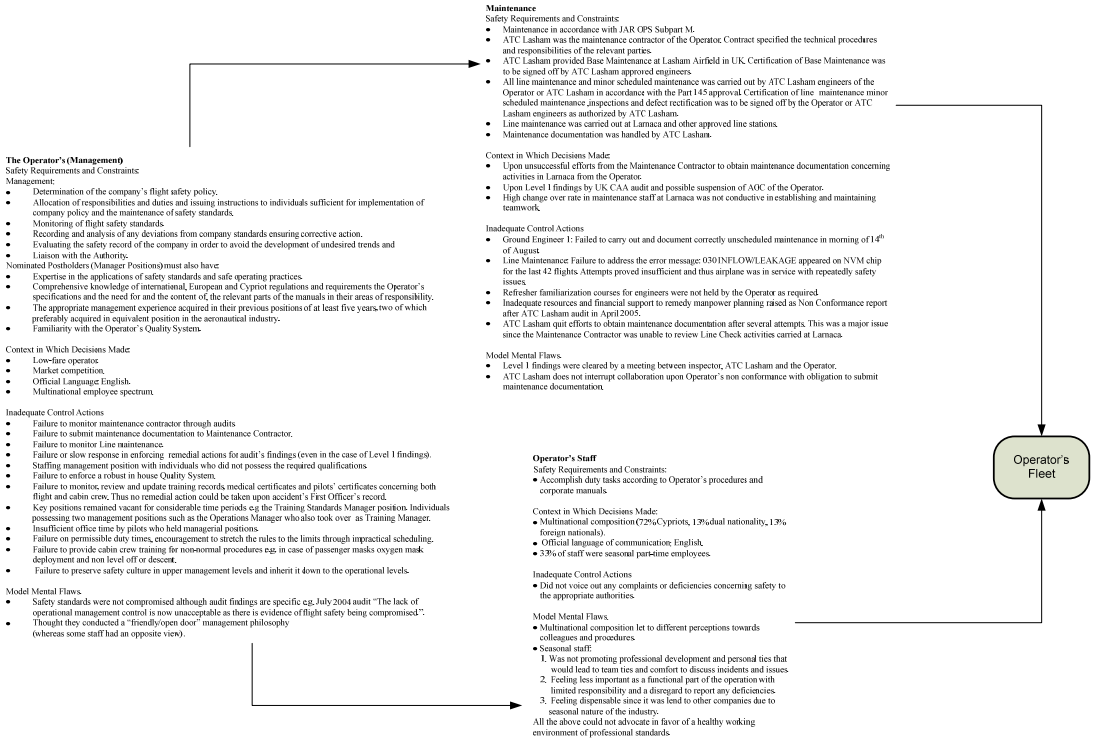


Figure 4-3. The Managerial Control Structure

Cypriots colleagues expressed any difficulties with the specific Captain. Thus different perception towards collogues could lead to weak work climate. Another issue concerning work climate was the fact that a 33% of staff was seasonal thus part time. This could let the staff feeling not important in the operational cycle thus with limited responsibility and no commitment in reporting incidents or deficiencies. Also it was not conductive in building team bonds and developing team procedures since teams were changing in composition. This might meant changing duties as well thus loss of continuity in their job. In addition to that the Operator's practice to lend employees to other companies due to seasonal character of the industry might let them feel dispensable which is not conductive to an enthusiastic work psychology. All the above might conducted to the fact that although they were suspicious or had facts at hand that safety was compromised within the Operator there was no report of that to the appropriate authorities such as Cyprus DCA or the General Prosecutor.

4.4.2 The Maintenance Contractor

ATC Lasham was the maintenance contractor of the Operator in order to comply with JAR OPS Subpart M. The relevant responsibilities and procedures were described in the contract. ATC Lasham provided Base Maintenance, performed in UK at Lasham airfield according to the approved maintenance program and including C checks. Certification of Base Maintenance was to be signed by ATC Lasham approved engineers in accordance with ATC Lasham company procedures.

Line checks and minor scheduled maintenance was performed in Larnaca (and other approved stations) and carried out by ATC Lasham authorized engineers of the Operator or ATC Lasham Engineers in accordance with Part 145 approval. Certification of line maintenance, minor scheduled maintenance, inspection and defect rectification was to be signed off by the operator or ATC Lasham Engineers as authorized by ATC Lasham. It is clear that although the Operator could hire engineering staff they all needed to be authorized by ATC Lasham according ATC MOE (Maintenance Organization Exposition).

ATC Lasham raised a Non-Conformance report concerning manpower planning at Line Maintenance after an audit in April 2005. The main response to that report was that there was an agreement with Cyprus Airways to provide 'as and when required' to cover line maintenance peak requirements. Despite the above effort management proved inadequate to provide for the necessary resources and financial support.

ATC Lasham, after audits of 2004 and 2005, was found not to have maintenance documentation for Line Maintenance carried at Larnaca. This was a contractual obligation and the finding was of Level 1. ATC Lasham attempted many times to obtain that documentation put the Operator would not provide it. ATC Lasham after several efforts quitted but that was a major issue since the Maintenance Contractor could not review or monitor the maintenance carried at Larnaca.

Added to the above, the engineer who performed the unscheduled maintenance documented it incompletely. There were nine write-ups related to the Equipment Cooling system from June to August 2005. This was the system that preoccupied the accident's Captain from concentrating on other pieces of information in order to piece out the pressurization problem. Also there were for 42 flights from NVM a fault message "030 INFLOW/LEAKAGE" which indicated continuous leakage of the aircraft (low inflow or high outflow from fuselage). For the above there were unsuccessfully attempts by maintenance to provide solution but remained unsolved. An aircraft with continuous technical problems was left to operate compromising safety.

Another issue that prevailed in maintenance was the fact of high change over rate in maintenance staff at Larnaca which was not conductive in establishing and maintaining teamwork (issues of multinational teams were discussed under staffing). Many of the maintenance staff was contracted through agencies and due to this change over they missed the familiarization refresher courses that should be held by the Operator but seemed not to take actually place.

4.4.3 The Operator

The Operator should have been the stronger safety enforcer. Yet he remains ill, inadequate not only to enforce new constraints that would allow him to operator with greater safety but also to monitor, in response to several audits, several organic procedures within its organization.

The audits provided diachronic deficiencies of the operator in areas of

1. Inadequate Quality System

The issue of an in-house Quality System was first appeared in a 2003 audit. Due to the absence of such a system the Operator was unable to identify several findings that eventually appeared on audits such us : deficiencies in areas of updating Operation Manuals training files and compliance with the recording of scheduled and permissible duty and rest times. Deficiencies in monitoring pilots certificates and medicals and training. Pilots with managerial duties did not log in sufficient office time. All the above would appear almost in every audit and even in the case that such findings were clear they would re-appear in later audits.

2. Inadequate Operational Management Control

The July 2004 audit concluded that a lack of operational management control resulted in pilots being cleared to operate public transport flights without the necessary competence. The audit contained findings such as management pilots had inadequate office duty time. Incomplete review of training records , days off violations for employees, and cabin crew records lacked certificates of competence for pilot incapacitation.

3. Vacancies in key management positions. Management Positions staffed with personnel whose qualifications did not match the job description.

Such as the Training Manager post which was vacant from June 2004 until March 2005. At the time of the accident Flight Operation Manager assumed the responsibilities of Training Manager as well. This position's periodic vacancy seemed to had greatly effected negatively training standards within the operator. In addition to the above some management positions were staffed by individuals who either did not have the required qualifications or did not possess managerial competence.

4. Failure in monitoring and documenting maintenance.

Audits stated that the Operator never audited its maintenance contractor concerning its standards and obligations. Also failed to document properly line maintenance tasks and submit them to the maintenance contractor. Such failure let to the repeated leakages of the accident aircraft and equipment cooling since remedial actions were not effective. Another example was the inconsistencies by the ground engineer in carrying out and documenting the maintenance actions performed.

5. Safety within the operator.

Safety meetings were held when needed. The operator did not provide the newly contracted engineers at line check with the required refresher courses. The accident's First Officer's record revealed some deficiencies but since there was no system in monitoring

training files there was no way to provide remedial actions for the recorded deficiencies. Thus all the issues described above combined together reveal that safety was compromised although if they are seen independently do lead to the same confusion.

The safety culture of the operator is clearly seen at audits taken to extend his AOC for the accident aircraft. The operator seemed under pressure and proceeded piecewise in typically submitting the necessary manuals to meet the initiation date instead of providing a solid presence with all necessary paperwork suggesting that everything had been prepared in time giving safety a high consideration.

Also absence of quality assurance contributed equally to the above environment. The most stunning example was the Flight Operations manager was updating only those Quick Reference Handbook revisions issued by the manufacturer which were considered important to him. In other words the safety barrier provided by the manufacturer of updating checklists after investigation boards' recommendations, were under conditional judgment of the Flight Operations manager.

Conclusively the Operator failed, to enforce all the required safety constraints, to respond in all of its managerial duties and more importantly failed to address audits findings (even of Level 1) which were eventually inherited to the operational level leading up to the accident.

4.5 The Regulatory Authority-Oversight Control Structure (Figure 4-4)

The last group of operators involved is the oversight operators. Those operators have the task ensure that safety constraints are enforced both managerial and operational level. This group of Operators involves:

1. Cyprus Department of Civil Aviation (Cyprus DCA)/
2. United Kingdom Civil Aviation Authority (UK CAA)
3. International Oversight Organizations for flight and maintenance operations (ICAO,JAA,EASA)

4.5.1 The Cyprus Department of Civil Aviation/ Ministry of Communications and Works (Government).

The Cyprus DCA operates as a department within the Ministry of Communication and Works. Therefore is governed by certain bureaucratic procedures as in all public departments. The Cyprus DCA has the task to fulfill the states' obligations under the Chicago Convention. The state's expectation were inversely proportional to the provisions for the Department. Insufficient funding let to insufficient staff in relation to actual workload. Staff employed was also not expertise in their posts and that is because job descriptions were not available. In addition the DCA/Safety Regulatory Unit had even more organic problems such as the mission strategy of each of its sections (Operations, Airworthiness and Licensing), processes and standard procedures were not officially documented. Key functions such as issuance and

validation of air transport pilot licenses, issuance and record keeping of certificates were not performed.

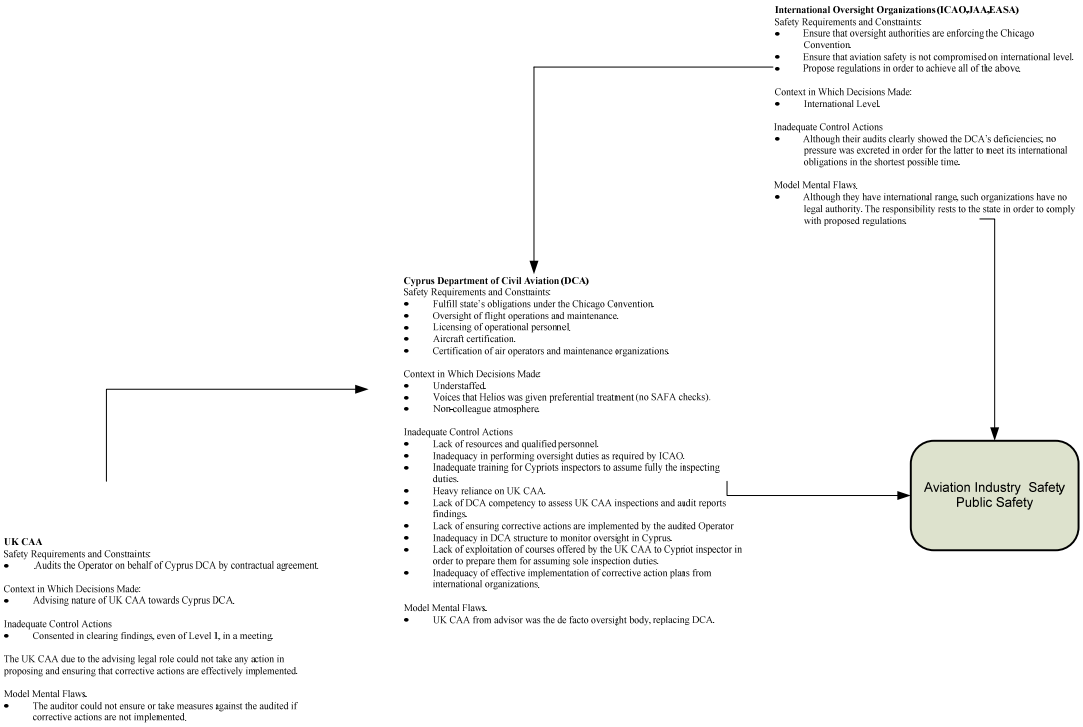


Figure 4-4. The Regulatory Authority /Oversight Control Structure

Also inspections were not accomplished as required by schedule due to lack qualified personnel. Thus to fulfils the oversight task, the department relied on external resources (such as the UK CAA). But even when CAA provided the audit reports DCA had no expertise to assess them and take appropriate actions-thus the Operator under audit continue to present same deficiencies as in previous audits. The other inadequacy due to government provisions was legislation. The DCA director did not had the authority to establish a flight operations inspections as an ICAO audit states. Thus the DCA instead of being the major constraint enforcer protecting public safety, it was reduced to an amputated department whose only action was to forward audit findings from UK CAA to the Operator without ensuring an effective response.

4.5.2 The UK CAA

The UK CAA was the contractual auditor on behalf of Cyprus DCA in order for the latter to accomplish its oversight duties. Legally CAA was just an advisor to DCA something that was clearly specified in a letter to the Minister of Communication and Works stating that it was DCA's responsibility to ensure that the audited has responded to audit's findings. Thus CAA was reluctant even to clear Level 1 findings by just a meeting. The CAA although the de facto oversight body for the Operator conducted audits and revealed many deficiencies and

recommended actions which unfortunately were not adopted. The CAA seemed to acknowledge the situation in DCA and offered regulation courses to Cypriot inspectors and also audits were conducted in conjunction with DCA staff preparing them for the field. Unfortunately the deficiencies described previously were dominant in the department.

4.5.3 The International Oversight Organizations (JAA,ICAO,EASA)

Their task is to maintain a high level aviation safety by auditing and propose regulations in international level. In the case of the Cyprus DCA although their audits showed the department's deficiencies in both safety oversight capability and organizational structure, the necessary pressure to DCA or the state's government was not imposed. Thus leaving a state's oversight body in deficiency could compromise aviation safety on international level. It is imperative for such organizations to impose the necessary pressure and measures to ensure that a state's aviation oversight authority meets and maintains the required standards of safety within its jurisdiction.

Finally the adapted control structure of the system is presented in Figure 4-5. As there was no implementation of corrective actions the feedback loops were eliminated thus the system operated as an open system, without any feature to reset it in the design structure of Figure 4-1. Thus deficiencies were free to migrate down the operational line and cause an accident.

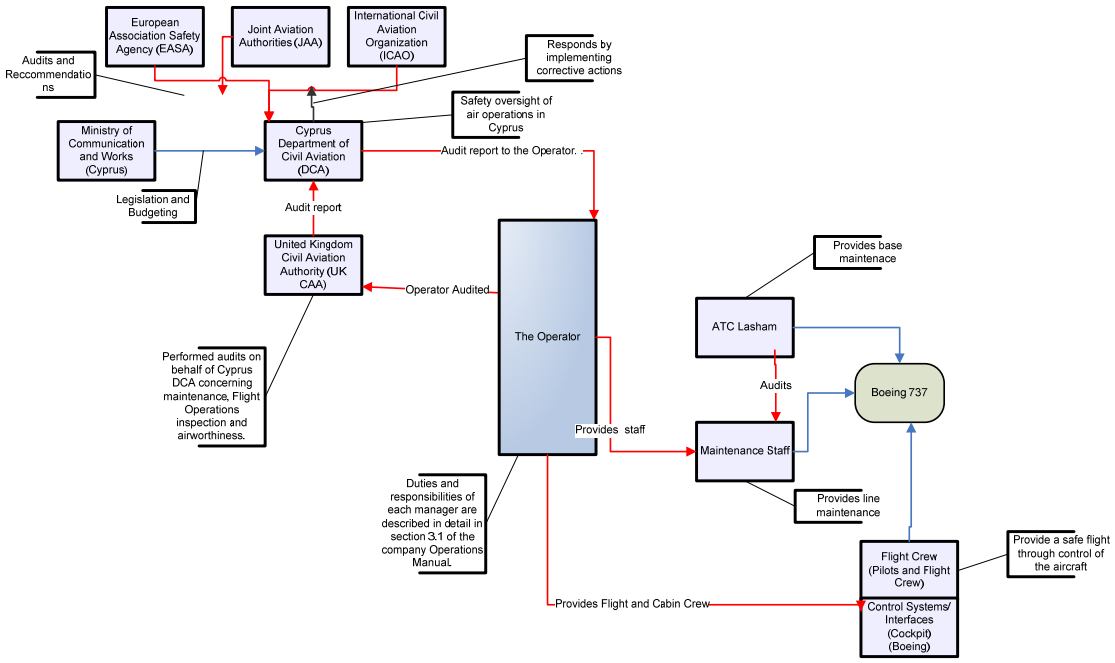


Figure 4-5. Adapted Control Structure showing the missing feedback loops

4.6 Modeling System (Behavioral) Dynamics

The analysis or prevention of accidents requires an understanding not only of the static structure of the system but also of the changes to this structure over time (the *structural dynamics*), but also the dynamics behind these changes (the *behavioral dynamics*). A way to model and understand the dynamic process behind the changes to the static control structure and why it changed over time, potentially leading to ineffective controls and unsafe behavior or hazardous states, is presented.

The approach proposed uses the modeling techniques of *system dynamics*. The field of system dynamics, created at MIT in the 1950's by Jay Forrester, is designed to help decision makers learn about the structure and dynamics of complex systems, to design high leverage policies for sustained improvement, and to catalyze successful implementation and change. Drawing on engineering control theory and the modern theory of nonlinear dynamical systems, system dynamics involves the development of formal models and simulators to capture complex dynamics and to create an environment for organizational learning and policy design.

Modeling the entire systems' dynamics is usually impractical. The challenge is to choose relevant subsystems and model them appropriately for the intended purpose. STAMP provides the guidance for determining what to model when the goal is risk management.

In the analysis lines with arrows between the variables represent causality links, with a positive polarity meaning that a change in the original variable leads to a change in the same direction in the target variable. Similarly, a negative polarity means that a change in the original variable leads to a change in the opposite direction of the target variable. According to systems dynamics theory, all the behavior dynamics of the system, despite their complexity, arise from two types of feedback loops positive (reinforcing) and negative (balancing). In system dynamics terms, degradation over time of the safety control structure, as represented by reinforcing loops, would lead inevitably to an accident, but there are balancing loops, such as oversight, that control those changes. It was found helpful to draw the system dynamics on the Rasmussen's hierarchical structure although it is not originally proposed. This enabled us to show the diffusion and spread of control throughout the system.

Figure 4-6 shows the system dynamics model for the accident system. Starting from the far left at Level 5 the 'Risk of inadequate control of the aircraft' is identified. This is reinforced by the 'Risk of confusion with warnings and panel design", with the 'Risk of improper configuration of the aircraft' and the 'Risk of electromechanical problem'' whereas 'Applicable flight operations and emergency procedures' and 'Effective crew training' act as balancing flows.

The ‘Risk of improper configuration of the aircraft’ receives balancing flows from ‘Monitoring training records’ and ‘Effective crew training’ whereas the ‘Risk of electromechanical problem’ receives reinforcing flow from ‘Risk of ineffective maintenance’ which in turn receives reinforcing flow from ‘Failure for required aircraft maintenance documentation’. It is clear that the only balancing flow concerning maintenance comes from the ‘Maintenance contractor expertise’’ which also balances the ‘Managerial inadequacy in implementing corrective actions’ which in turn receives balancing flow from ‘Statutory oversight’ and a reinforcing flow from ‘Managers’ qualifications incompatible with job descriptions’.

‘Statutory oversight’ receives a reinforcing flow from ‘UK CAA expertise’ and a negative flow from ‘Government legislation and budgeting inadequacies’ which reinforces “Cyprus DCA understaffing and insufficient expertise’ which also provides negative flow on ‘Statutory oversight’.

A ‘Quality Assurance System’ would provide a balancing flow to managerial inadequacy and a reinforcing flow in ‘Monitoring training records’. An effective Training Manager would reinforce ‘Effective crew training’ and ‘Applicable flight operations and emergency procedures’.

From analysis it is obvious that the reinforcing flows of risk and inadequacies prevailed the balancing and prevention flows and thus the accident resulted.

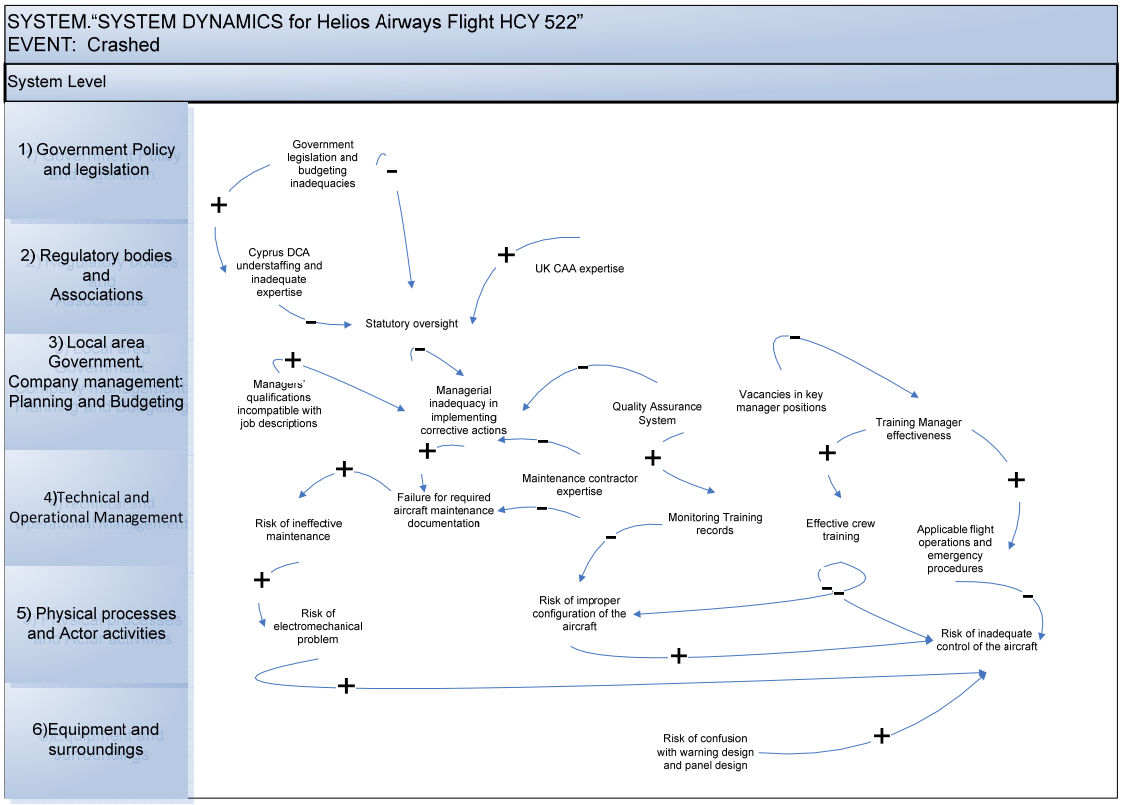


Figure 4-6. System Dynamics model.

Chapter 5 Conclusion Analysis

5.1 Causes

The causes of the accident can be classified into 3 levels: 'Direct, Latent and Contributing factors.'

Direct causes include 1) the non-recognition that the cabin pressurization mode selector was in the MAN position during the execution of Preflight Procedure, Before Start checklist and After Takeoff checklist. 2) The non identification of the aural and visual warnings and the reasons triggering them in conjunction with the continuation of the climb which resulted in 3) incapacitation of the flight crew due to hypoxia.

Latent causes include 1) the Operator's deficiencies in organization, quality management and safety culture as documented in audit reports. 2) The Regulatory Authority's inadequacy in executing its oversight duties and responsibilities in order to ensure the safety of aviation operations and its failure to respond in deficiencies traced in various audits. Also such causes include 3) the inadequacy of Crew Resource Management (CRM) application by the flight crew and 4) the manufacture's inadequate actions with regard to modification of aircraft systems and guidance to the crews.

The contributing factors to the accident include 1) the omission by the ground engineer to return the pressurization mode selector to AUTO after unscheduled maintenance on the aircraft. 2) The lack of specific procedures for cabin crew procedures to address the situation of loss of pressurization, passenger oxygen masks deployment in conjunction with the continuation of the climb 3)The ineffectiveness of international aviation authorities to enforce implementation of corrective action plans after relevant audits.

The above causes and contributing factors are not independent. For example the ineffectiveness of international aviation authorities in enforcing corrective actions is directly connected to the Regulatory Authority's (Cyprus DCA) inadequacy in executing it's oversight duties. Also CRM which is designed to be a remedy action it's inadequacy in application turned to be a cause contributor. Assigning the above causes in a hierarchical structure such as below, we can see an interesting pattern.

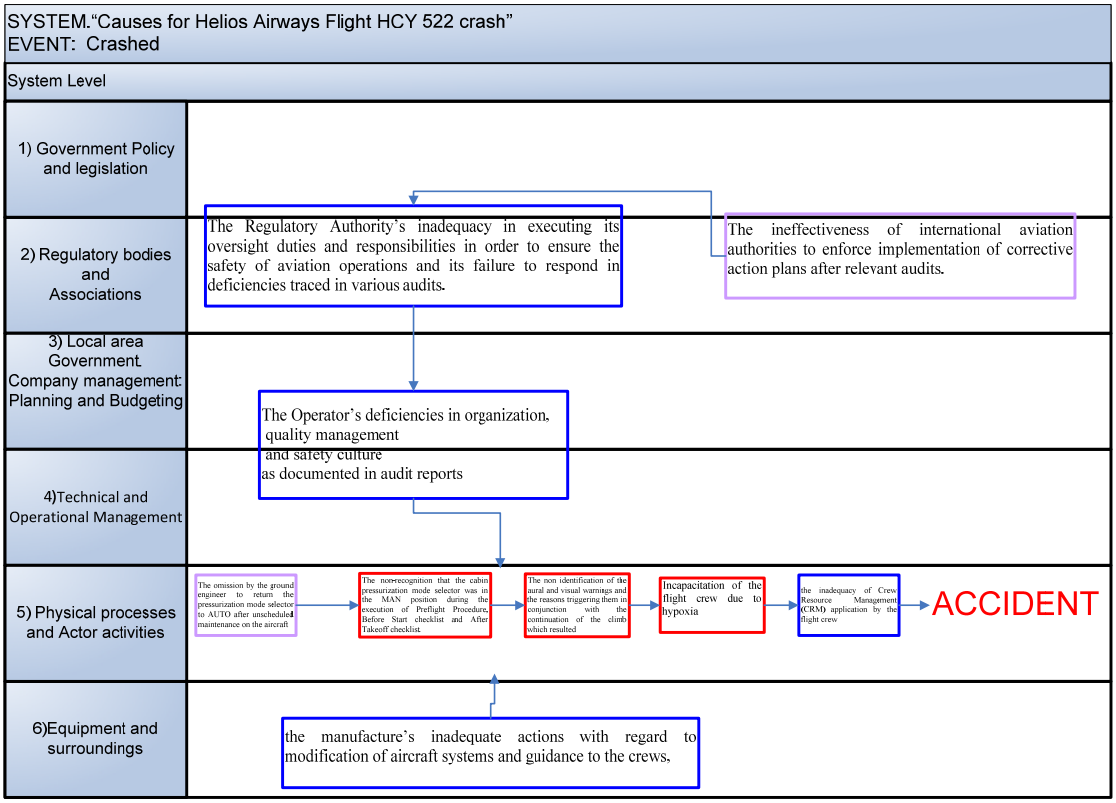


Figure 5-1. Mapping of causes onto Rasmussen's Hierarchical Structure

Figure 5-1 shows an interesting pattern. A contributing factor in the Authorities level gave rise to a latent cause in the same level which in turn gave rise to a latent's cause in the Managerial level. This latent cause in the Managerial level combined with the latent cause in the Manufacture's level created the preconditions of the accident. The direct causes are sparked from an omission in the Line Operational level and after failure (3) of a safety tool (CRM), to confront them the flow lead to the accident. The same flow is illustrated in more detail in the AcciMap which enabled us to see the reasons behind those causes.

5.2 Actions taken after recommendations by AAIASB

Several recommendations were made by the AAIASB to all associate parts. Boeing responded by:

- Introducing New Normal Procedures, thus New Normal Checklists

Old Normal Checklists (Pre 2005)	New Normal Checklists (2005 onwards)
BEFORE START FLIGHT DECK PREPARATION. . . . . . COMPLETED LIGHT TEST . . . . CHECKED OXYGEN & INTERPHONE . . . . CHECKED YAW DAMPER. . . . . .ON NAVIGATION TRANSFER AND DISPLAY SWITCHES . . . . . . AUTO & NORMAL FUEL . . . . . . ._____KGS & PUMPS ON GALLEY POWER . . . . .ON EMERGENCY EXIT LIGHTS. . . . . .ARMED PASSENGER SIGNS. . . . . .SET WINDOW HEAT . . . . .ON HYDRAULICS . . . . NORMAL **AIR COND & PRESS. . . . . .___ PACK(S),** **BLEEDS ON, SET** AUTOPILOTS . . . . . . DISENGAGED INSTRUMENTS . . . . .X-CHECKED AUTOBRAKE. . . . . .RTO SPEED BRAKE . . . . . . DOWN DETENT PARKING BRAKE . . . . .SET STABILIZER TRIM CUTOUT SWITCHES. . . . . NORMAL WHEEL WELL FIRE WARNING . . . . CHECKED RADIOS, RADAR, TRANSPONDER & HUD . . . . .SET RUDDER & AILERON TRIM	PREFLIGHT Oxygen . . . . . . Tested, 100% NAVIGATION transfer and DISPLAY switches . . . . . . NORMAL, AUTO Window heat . . . . On **Pressurization mode selector. . . . . .** **. . . . . AUTO** Flight instruments . . . . . . Heading___, Altimeter___ Parking brake . . . . .Set Engine start levers . . . . CUTOFF

FREE & ZERO PAPERS. . . . . .ABOARD	
FMC/CDU. . . . . .SET	
N1 & IAS BUGS. . . . . .SET	

Table 5-1. Old and New Normal Checklists

In the new normal checklists there is an explicit requirement of 'Pressurization mode selector. . . . . AUTO' instead of 'AIR COND & PRESS. . . . . .___ PACK(S), BLEEDS ON, SET'. Also new normal checklists are shortened including only critical tasks, those which are related mostly to safety. Changes made minimize the number of tasks to be accomplished during taxiing. The aim is to improve situational awareness and reduce missed radio calls & runways incursions. Responsibilities have been redistributed to better align them with the roles the pilots are performing. Items have been re-sequenced to minimize workload at critical times and have retained only those items which are necessary for crew to perform.

- After FAA's AD, AFM Emergency or Non-Normal Procedures sections revised to include :

WARNING HORN - CABIN ALTITUDE OR CONFIGURATION

Condition: An intermittent or steady warning horn sounds:

In flight an intermittent horn indicates the cabin altitude is at or above 10,000 feet.

On the ground an intermittent horn indicates an improper takeoff configuration when advancing thrust levers to takeoff thrust.

In flight a steady horn indicates an improper landing configuration.

If an intermittent horn sounds in-flight:

OXYGEN MASKS AND REGULATORS . . . . . ON, 100%

CREW COMMUNICATIONS. . . . . ESTABLISH

Do the CABIN ALTITUDE WARNING OR RAPID DEPRESSURIZATION checklist.

If an intermittent horn sounds on the ground:

Assure proper airplane takeoff configuration.

If a steady horn sounds in-flight:

Assure proper airplane landing configuration.

After FAA's AD, Boeing upgraded configuration panel to include (2) warning level indicators that read "TAKEOFF CONFIG" and "CABIN ALTITUDE". These warning level lights provide a visual indication to both pilots simultaneous with the aural intermittent horn for cabin altitude and takeoff configuration alerts.

By the above actions Boeing addressed the issues of checklist design and warning horn confusion.

As far as Cyprus DCA concerns, it undergoes a reorganization phase in order to proceed as an independent authority meeting its oversight duties and organizational standards as required now by EASA (replacing JAA).

5.3 Results of methods used in analysis.

Under Causes section, the causes indentified by the official report were listed. Both AcciMap and Stamp revealed almost the same issues but in different depiction. The AcciMap shows the flow of flaws down the hierarchy where as STAMP shows how those flaws affected the control capability of each actor at the respective control level. STAMP also enables us to incorporate the context in which decision was made. Different decisions are made under stress and different under 'calmed conditions'. For example both the Captain and the Ground Engineer were working on the same situation, but the Captain was under pressure to solve a climaxing situation as more and more warning lights were illuminating and under the stressful sound of the warning horn. Thus the Ground Engineer who had the 'luxury' of ground 'peace' should have insisted on confirmation of the position of pressurization selector. Both methods raised issues of human factor performance, CRM failure, work climate and behavior. STAMP also due to the control-loop ability has in addition identified that effective oversight is a necessity and also how institutional outsourcing can be severe to safety. Each issue is now discussed individually:

5.3.1 Human factor performance

Since there was no mechanical failure to cause the accident, human nature must be investigated since humans were the only figures present. They are referred to as Actors in AcciMap and as Operators or Human Controllers in STAMP. In Level 5 human factors infiltrated in the execution of critical actions. Such factors were:

5.3.1.1 Expectation Bias – 'Look without seeing'

This is human vulnerability where if you a certain arrangement is not expected, is ignored and it treated as if it was the expected one. This vulnerability surfaced when performing lengthy habitual tasks as in the case of Preflight Procedure and checklist verification. This can lead to

omissions since it is expected that everything will be in their normal position. This can apply to the pressurization mode selector where is always set to AUTO position. The only case to be in MAN position is if the pilots deliberately have to fly the aircraft in manual pressurization due to a system problem.

5.3.1.2 Execution from memory-Automation Expectation

Humans execute tasks from memory usually for time economy. Such skill is acquired by performing certain duties numerous times until they become habits. This is has a positive gain for long list actions that are time consuming and time pressured. For example, Preflight Procedure may contain 40 to 80 actions and the pressure to meet departure times. Nevertheless there is a negative side as well. Such actions are executed automatically. This means that they are void of conscious and attention and sensitive to assumptions which lead to omissions.

5.3.1.3 Declarative Memory and Muscle Memory

Declarative Memory is the type of memory that stores facts and events whereas muscle memory is that skeletal muscle activity that becomes essentially automatic with practice. Both of these memories associated the onset sounding horn with the throttles and that was a strong (false) indication to the pilots that they were dealing with a takeoff configuration problem.

5.3.1.4 Stress

Stress in this case refers to the consequences of the failure to perceived threat. A loud and annoying horn would signify such threat. The sound of the warning horn (that was never canceled) could create such an environment in conjunction with the fact that any action taken by the pilots failed to address the situation as more warnings were illuminating the overhead panel.

5.3.1.5 Preoccupation with one task

Preoccupation is the absorption of an individual's attention. During the crucial moments of flight while warning lights were flickering on the overhead panel the Captain was preoccupied by the Equipment Cooling system. His attention was absorbed by a symptom by a symptom, instead of being concentrated in troubleshooting the source of the warning horn. In addition gradual hypoxia can be identified as a contributor to preoccupation since ti affects decision making by degrading the ability to think.

5.3.2 Crew Resource Management (CRM)

It is apparent that the pilots committed many errors in the accident flight. As in every system with many degrees of freedom such as the flight operation, many errors occur but very rarely superpose to result in an accident due to the many safety barriers incorporated in the system. CRM training and procedures is such a barrier and has as a goal the elimination of individual errors through communication and teamwork.

The ICAO Human Factors Training Manual (DOC 9683) states: (Part 1, paragraph 1.4.25) *"Crew coordination is the advantage of teamwork over a collection of highly skilled individuals. Its prominent benefits are:*

• *an increase in safety by redundancy to detect and remedy individual errors; and*

• *an increase in efficiency by the organized use of all existing resources, which*

improves the in-flight management."

(Part 1, paragraph 1.4.26) "*The basic variables determining the extent of crew coordination are the attitudes, motivation, and training of the team members. Especially under stress (physical, emotional, or managerial), there is a high risk that crew coordination will break down. The results are a decrease in communication (marginal or no exchange of information), and increase in errors (e.g. wrong decisions), and a lower probability of correcting deviations either from standard operating procedures or the desired flight path …".*

(Part 1,paragraph 1.4.27) *"The high risks associated with a breakdown of crew coordination show the urgent need for Crew Resource Management training, … This kind of training ensures that:*

• *the pilot has the maximum capacity for the primary task of flying the aircraft*

and making decisions;

• *the workload is equally distributed among the crew members, so that excessive*

workload for any individual is avoided; and

• *a coordinated cooperation - including the exchange of information, the support*

of fellow crew members and the monitoring of each other's performance - will

be maintained under both normal and abnormal conditions."

(Part2, paragraph 2.2.9) "*CRM is a widely implemented strategy in the aviation community as a training countermeasure to human error. Traditionally, CRM has been defined as the utilization of all resources available to the crew to manage human error."*

Checklist discipline is a basic a element in CRM. It is an application of both teamwork and a control loop unit since one pilot performs the check while the other pilot confirms to ensure that the required actions have been performed as required.

The failure of the pilots to carry out the checklists properly resulted in leaving the pressurization mode selector to manual position. This is a case of poor CRM application since the pilot responsible to set the pressure failed and the pilot who monitor the proper pressurization setting failed as well. There was inadequate CRM when the warning horn was not silenced and pilots did not don their oxygen masks. The contact of ground operations was a good CRM step although other factors prevailed and eliminated it. From the events of the accident flight it seemed that the teamwork factor was not implemented. Of course the CVR does not provide

any insight for those crucial moments, but it seems that pilots acted individually. The team approach compensates the fact that if one participant performs less than required the others would compensate that inadequacy. Short falls of performance are recorded in First Officer's training record thus the team formed with Captain would mitigate those probable deficiencies. Also to utilize all resources the Captain should be aware of his Firsts Officer's record comments, something which he was not. The pilots are not the only resources in the flight. The cabin crew has its gravity as a safety resource. It was not possible to determine the actions of the cabin crew during oxygen mask deployment but due to lack of procedures to address the specific situation arose, poor CRM would have been expected.

To illustrate the cabin crew significance in CRM, the Boeing 737-548 Irish incident will be referred where the application of proper CRM compensated the errors provided by individuals. In this incident the air conditioning packs were switched off and thus pressurization never achieved. During climb and while the pilots were carrying the After Takeoff list the senior cabin attendant entered the cockpit and reported that she was experiencing problems with her ears that prompted the pilots to carry out the relevant non-normal checklist and made the relevant actions. They proceeded to climb but since there was alerted with a situation, one pilot felt the need for oxygen and used his mask as he noted that cabin altitude was rising. At this time the senior cabin attendant entered again the flight deck and notify the pilots that passengers had ears problems, that the cabin was very cold and that that there was some mist in the aft cabin and later she reported that passengers oxygen masks were deployed causing the pilots to level the aircraft (they were about FL141) and after request they landed at the departure airport. The investigation board AAIU in the report stated that: *"The continued persistence by the [Senior cabin attendant] in keeping the flight crew informed of the cabin situation was a major factor in ensuring the safe outcome of this serious incident."*

Both the pilots and cabin crew received CRM training during 2005. The reasons for not enforcing CRM practices in the accident flight must be looked up in the illness of management to monitor training and also to provide training since the key position of the Training Manager was vacant for a considerable time.

5.3.3 Work climate and behavior.

Several factors and management practices affected the work climate and employees behavior within the operator. To begin with the management had the opinion that a friendly and open door management philosophy was enforced. On the contrary, some employees expressed an opposite view concerning the Accountable Manager who was characterized as unapproachable with little regard for safety and only interested in profitability, This distant views show that management was not aware of the opinion of its own employees. Efficiency within a business is directly linked to an employee's satisfaction from his work. An unsatisfied employee will not enforce full commitment to his duties and therefore there will be shortfalls of performance. Such shortfalls may affect safety as well.

The employment practice of part-time seasonal staff had a negative impact on employees' psychology. They might felt indispensible for the company, not too important and thus they felt no need to offer something beyond their assigned tasks. They wouldn't feel necessary to report or to discuss any deficiencies to their superiors. In addition the constant changing of staff let the staff in new groups all the time, limiting them to become teams and develop the associate trust between them and thus the comfort to discuss all issues, including safety. CRM techniques do not apply only to flight crews but also to any team in the production line. Thus the part-time seasonal practices limited staff from developing teamwork, a base element in a pro-active safety system.

5.3.4 Institutional Outsourcing

Outsourcing is a subcontracting a process to a third party company. Such decision is made for cost issues (lowering cost) or du to the fact that the third party possesses a high level of competency in the specific process.

In the case of study, the UK CAA as the third party company and the process outsourced in effect are the oversight duties of Cyprus DCA. The reason for such decision was not an issues of lowering cost but because of insufficient budgeting and mainly because of inadequate competency with in Cyprus DCA.

The issue in this case, is that although UK CAA's competency was proven by conducting the audits, there were no legal provisions to for the CAA to ensure that audit's findings would be met with the appropriate corrective actions and their implementation.

From the analysis is obvious that effective oversight is a necessity in all levels. From monitoring training records to the level of auditing the air operator or even the oversight agency like the DCA from international oversight organizations.

There are elemental processes that cannot be decomposed into sub processes and such a process is the state's oversight duty. Thus if such a process is necessary to be outsourced the necessary authority for full scale oversight should be outsourced too.

Still there is the question if sensitive state's duties such as the public safety can be outsourced. This can be an issue of further study on how outsourcing implicates safety issues.

5.4 Assessment of the accident analysis techniques

At this point the analysis techniques will be assessed against the criteria described in *section 1.2.*

5.4.1 The Rasmussen's framework

Rasmussen's framework scores high in the group of sequential and temporal aspects of the accident scenario criteria. The AcciMap supports te analyst in describing and representing the

sequence of events and actions that have led to the accident (Level 5), whereas the ActorMap identifies the agents (actors) of different event or actions and facilitate their grouping in technical (Level 6) and human agents (Level 1-5). The AcciMap, through its hierarchical structure, supports the identification of events and actions and the examination of their cascade effects. Also the hierarchical feature provides the dependencies of preceding events whereas consequences can spread in different hierarchical levels. The Rasmussen's framework is found deficient in recording timing. Only Level 5 recorded events in a time flow whereas the upper levels are recorded in a more abstract time manner. Nevertheless workload of the actors can be incorporated in Level 5 as a factor, as in the case of preflight, before takeoff and after takeoff procedures and checklists. Finally the multilevel representation is one of the prime features by Rasmussen's framework The AcciMap is nothing else than a multilevel event and action representation with their complex relationships. In the analysis also 'groups and actions' where identified; such identification on the "Big Picture' diagram of Appendix C enabled us to construct the AcciMap (Figure 3-2).

Concerning the aspects of accident analysis process, the Rasmussen's framework receives a high score. The modeling of assumptions with dotted lines can be enabled by AcciMap. In fact the Level 5 flow of events are assumptions based on the Board's human performance expertise due to the fact that the CVR had only 30 minutes recording capability. Thus dotted lines could be used instead of solid ones. In addition, modeling of inconsistencies such as conflicts is also possible by constructing a Conflict Map (Almeida and Johnson 2004). Finally co-operation facilitation is enabled by providing a hierarchical level platform on which different analysts can referred to, providing a systemic grouping of findings.

The last group of accident criteria concerns accident prevention. Since accident analysis aims to identify the events that have let to the accident, the Rasmussen's framework again provides such tools. Concerning event criticality, the AcciMap supports the judgment for the importance or criticality of events and actions and their contribution to the accident. In addition modeling error recovery or failure of such recovery was greatly illustrated in AcciMap. Delayed events such as not canceling the master caution warning, mislead events such as the equipment system cooling which mislead the Captain to believe that he was dealing with a system cooling problem instead of pressurization and other types of events were illustrated in the analysis through AcciMap. Also due to the fact that in Level 5, factors such as Human Performance factors are included support the modeling of work context; revealing latent factors that had side effects on the main causal flow of events. Finally by zooming on each event or group of events provided by AcciMap we can develop proactive measures for stopping the causal flow.

5.4.2 The STAMP

STAMP receives a low score in the group of sequential and temporal aspects of the accident scenario criteria since it is not an event based framework. Nevertheless STAMP provides a multilevel representation of control structures.

Concerning aspects of accident analysis process, STAMP would score relative high since it has provisions for modeling of assumptions between the different control structure levels as well as modeling of inconsistencies through input (events) against constraints which are violated/ Also co-operation facilitation is enabled through the fact that different control structures and constraints can be proposed by different analysts which at the end can be superposed to provide a more extensive control structure.

Finally for the group of aspects of accident prevention STAMP is unable to detect event criticality or modeling error recovery through events. On the other hand it is capable in modeling the context of work in which decisions was made and also provides the means to propose preventing measures through constraints.

It is quite obvious that the criteria treat unfairly the STAMP by their events based design. Thus new criteria are needed that incorporate the control nature of the techniques so that control based techniques can be objectively assessed.

5.5 Event Vs Control domain. (Almeida and Johnson 2004, p.3)

Rasmussen's models on information flow and in the end a chain of event is included. This 'chain of event' feature resemble the traditional time techniques in which particular incidents develop over time. For this reason proponents of STAMP (or those from the school of 'control') widely criticized Rasmussen's models because they often encourage analyst to focus closely on particular instances of 'human error' rather than at the context that makes those errors more likely.

In the analysis presented in this work, STAMP seemed to complement AcciMap and vice versa. There is indeed a flow of information in any operations but there are also controllers who regulate that flow. Constraints set by STAMP will be violated by events that can demonstrated by AcciMap in the causal flow towards an accidents.

It can be said that these two techniques are bonded by a property of duality. After all the design issue is "given the inputs and outputs design the system", thus inputs and outputs are events provided by Rasmussen's framework and the system design requires constraints that are provided by STAMP.

Nevertheless, human are more familiar in assessing events and people involved in the operational processes level seek to understand what actions lead to the accident or incident whereas the higher managerial and oversight levels are more concerned (or should be) if the necessary safety provisions (constraints) were enforced.

Conclusively, both ‘event and control’ domains should be examined in analysis. The first would reveal the human nature in the accidental flow and the second the systemic behavior in respect to that accidental flow.

5.6 Further suggestions for study and development

Two techniques were used to analyze an industrial accident. It is interesting to study how each technique behaves if it is used to analyze different accidents from the same domain. Thus the Generic AcciMap could be constructed.

Also these techniques analyzed an accident from the industrial domain. It will be equally interesting to see how they will behave if an incident from the social domain is chosen such as the suspension of educational and research processes in the Greek universities; an incident that often occurs.

The above brings out the essence of a pro-active safety society. The accident must be avoided, and to do so the incident prior the accident should be carefully analyzed. Usually before major industrial accidents several non fatal incidents ring the hazard bell and in the case of Flight HY522 there were numerous such bell rings.

Bibliography

[1] AAIASB., 2006, Aircraft accident report: Helios Airways Flight HCY522 BOEING 737-31S at Grammatiko, Hellas on August 2005, Ministry of Transport and Communication, Hellenic Republic.

[2] Almeida I.M., Johnson C.W., 2004. Extending the borders of Accident Investigation: Applying Novel Analysis Techniques to the Loss of Brazilian Space Programme's Launch Vehicle VLS-1 V0.3

[3] Ashby, W.R., 1956. An Introduction to Cybernetics, Chapman and Hall, London.

[4] Benner Jr., L., 1985. Rating accident models and investigation methodologies. Journal of Safety Research 16, 105-126.

[5] Brehmer, B., 1992. Dynamic Decision Making: Human Control of Complex Systems, Acta Psychologica, Vol. 81, pp. 211–241.

[6] Checkland, P., 1981. Systems Thinking, Systems Practice, John Wiley & Sons, New York

[7] Conant, R.C., W.R. Ashby, W.R., 1970. Every good regulator of a system must be a model of that system, International Journal of System Science, 1:89–97, 1970.

[8] Cook, R.I., 1996. Verite, Abstraction, and Ordinateur Systems in the Evolution of Complex Process Control, 3rd Annual Symposium on Human Interaction with Complex Systems (HICS '96), Dayton, Ohio.

[9] Ferry, T.S., 1988. Modern Accident Investigation and Analysis 2nd Edition. Wiley, New York.

[10]Hopkins A.,2000, An AcciMap of the ESSO Australian Gas Plant Explosion, Australian National University.

[11]Kontogiannis T., Vrassidas L., Marmaras N., 2000, A comparison of accident analysis techniques for safety-critical man-machine systems, Elsevier.

[12]Kontogiannis, T., 1996. Stress and operator decision making in coping with emergencies. International Journal of Human - Computer Studies 45, 75-104.

[13]Kontogiannis, T., 1999. User strategies in recovering from errors in man machine systems. Safety Science 32, 49-68.

[14]Leplat, J. 1987. Occupational accident research and systems approach, In: Rasmussen, J., Duncan, K., Leplat, J. (Eds.). *New Technology and Human Error*, pages 181–191, John Wiley & Sons, New York.

[15]Leveson G.N., 2002, System Safety Engineering: Back To The Future, M.I.T.

[16]Leveson N., 2004, A New Accident Model for Engineering Safer Systems, Elsevier.

[17]Leveson N., Daouk M.,Dulac N., Marais K.,2003, A Systems Theoretic Approach to Safety Engineering, M.I.T

[18]Leveson, N.G., 1995. Safeware: System Safety and Computers, Addison Wesley, Reading, Massachusetts.

[19]Leveson, N.G., 2001. Evaluating Accident Models using Recent Aerospace Accidents, Technical Report, MIT Dept. of Aeronautics and Astronautics (available at http://sunnyday.mit.edu/accidents).

[20]Leveson, N.G., Allen, P., Storey, M.A., 2002. The Analysis of a Friendly Fire Accident using a Systems Model of Accidents, 20th International Conference on System Safety. Sarter, N.N., Woods, D.D., 1995. Strong, silent, and out-of-the-loop, CSEL Report 95-TR-01,Ohio State University, February.

[21]Nielsen. D.S. 1974. Use of cause-consequence charts in practical systems analysis. In: Reliability and Fault Tree Analysis. Theoretical and Applied Aspects of Systems Reliability and Safety Assessment. Papers of the Conference on Reliability and Fault Tree Analysis. Berkeley. 3-7 September 1974. Society for Industrial and Applied Mathematics. Philadelphia. pp. 849-880.

[22]Plat, M., and Amalberti, R., 2000. Experimental crew training to deal with automation surprises. In: N. Sarter and R. Amalberti (Eds.) Cognitive Engineering in the Aviation Domain, Laurence Erlbaum Associates, Mahway, New Jersey, pp. 287–307.

[23]Rasmussen J., Svedung I,, 2000, Proactive Risk Management in a Dynamic Society, Swedish Rescue Agency.

[24]Rasmussen, J., 1997. Risk Management in a Dynamic Society: A Modeling Problem, Safety Science, vol. 27, No. 2/3, Elsevier Science Ltd., pages 183–213.

[25]Rosness, R. 2001. Om jeg hamrer eller hamres, like fullt sa skal der jamres: Malkonflikter ogsikkerhet (If I hammer or get hammered, in any case there will be groaning: Goal Conflicts and Safety), SINTEF Technologies Report, STF38 A01408 (www.risikoforsk.no/Publikasjoner/Ragnar

[26]Sarter, N.N., Woods, D.D., 1995. Strong, silent, and out-of-the-loop, CSEL Report 95-TR-01, Ohio State University, February.

[27]Suokas, J. and Pyy, P., 1988. Evaluation of the Validity of Four Hazard Identification Methods with Event Descriptions. Research report VTT 516, Technical Research Center of Finland.

[28]Svedung I., Rasmussen J., 2002, Graphic representation of accident scenarios: mapping system structures and the causation of accidents, Pergamon.

[29]Svedung. 1.. Rasmussen. J.. 1998. Begrepp till st6d *for* proaktiv hantering av olycksrisker. Farslag till taxonomi (A proposal for a Taxonomy supporting a pro-active Risk-Management Strategy). The Swedish Rescue Services Agency. P21-295/99 (in Swedish).

APPENDICES

APPENDIX A

In this appendix, figures from Chapters 3 and 4 are reprinted for better review by the reader.

SYSTEM. "ActorMap for Helios Airways flight HCY522"
EVENT: Crashed

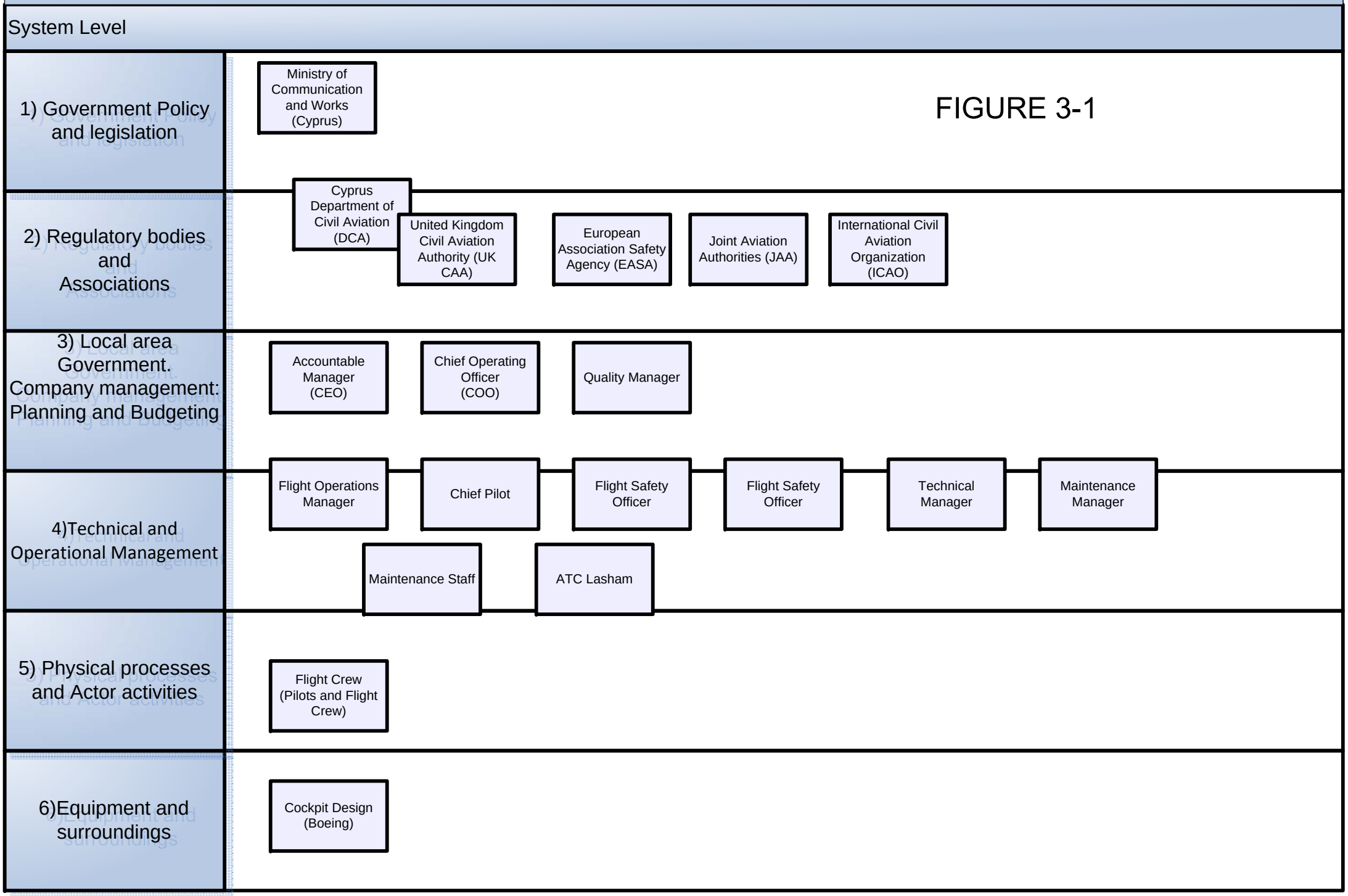


FIGURE 3-1

SYSTEM.“AcciMap for Helios Airways Flight HCY 522”
EVENT: Crashed

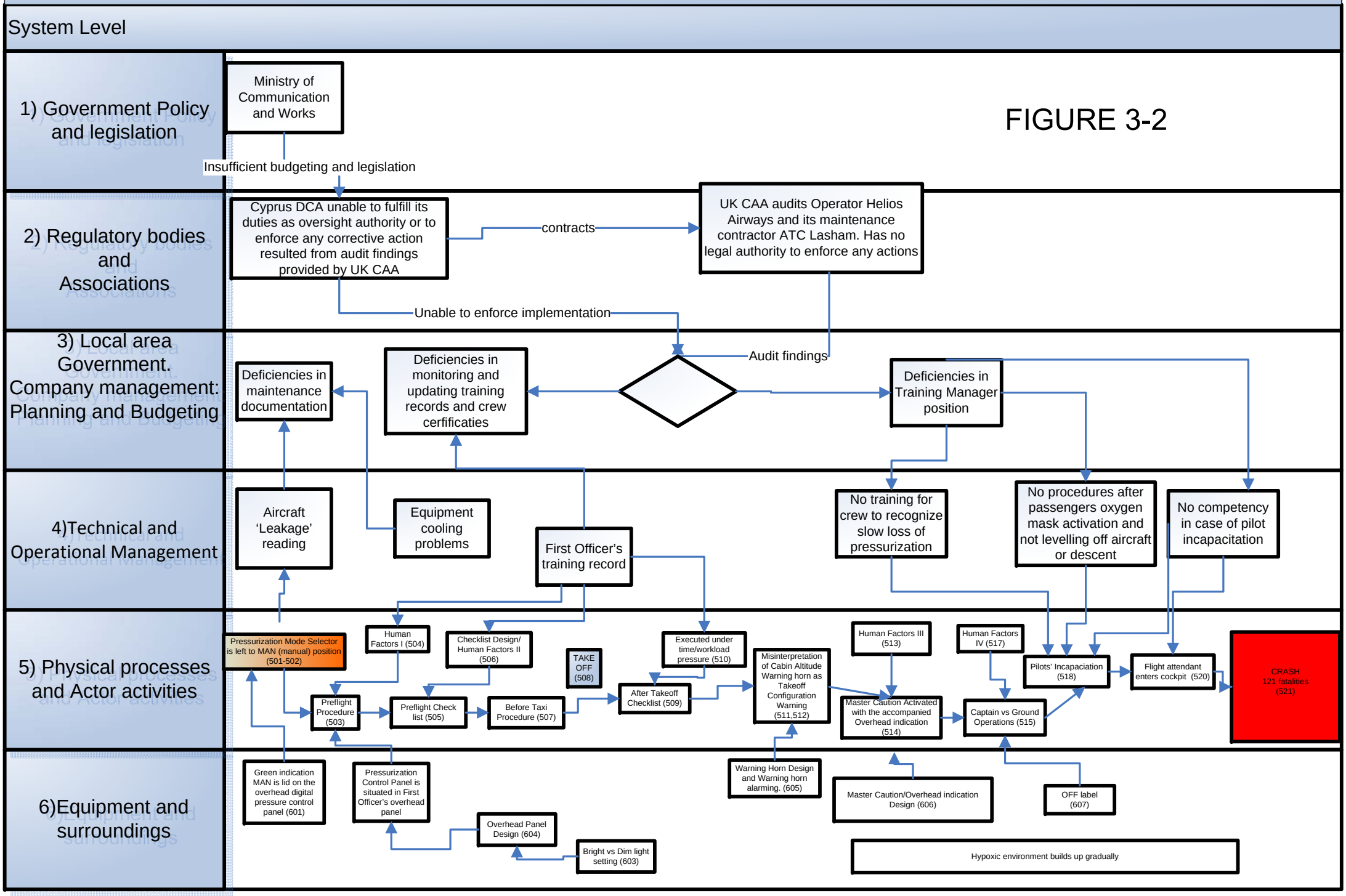
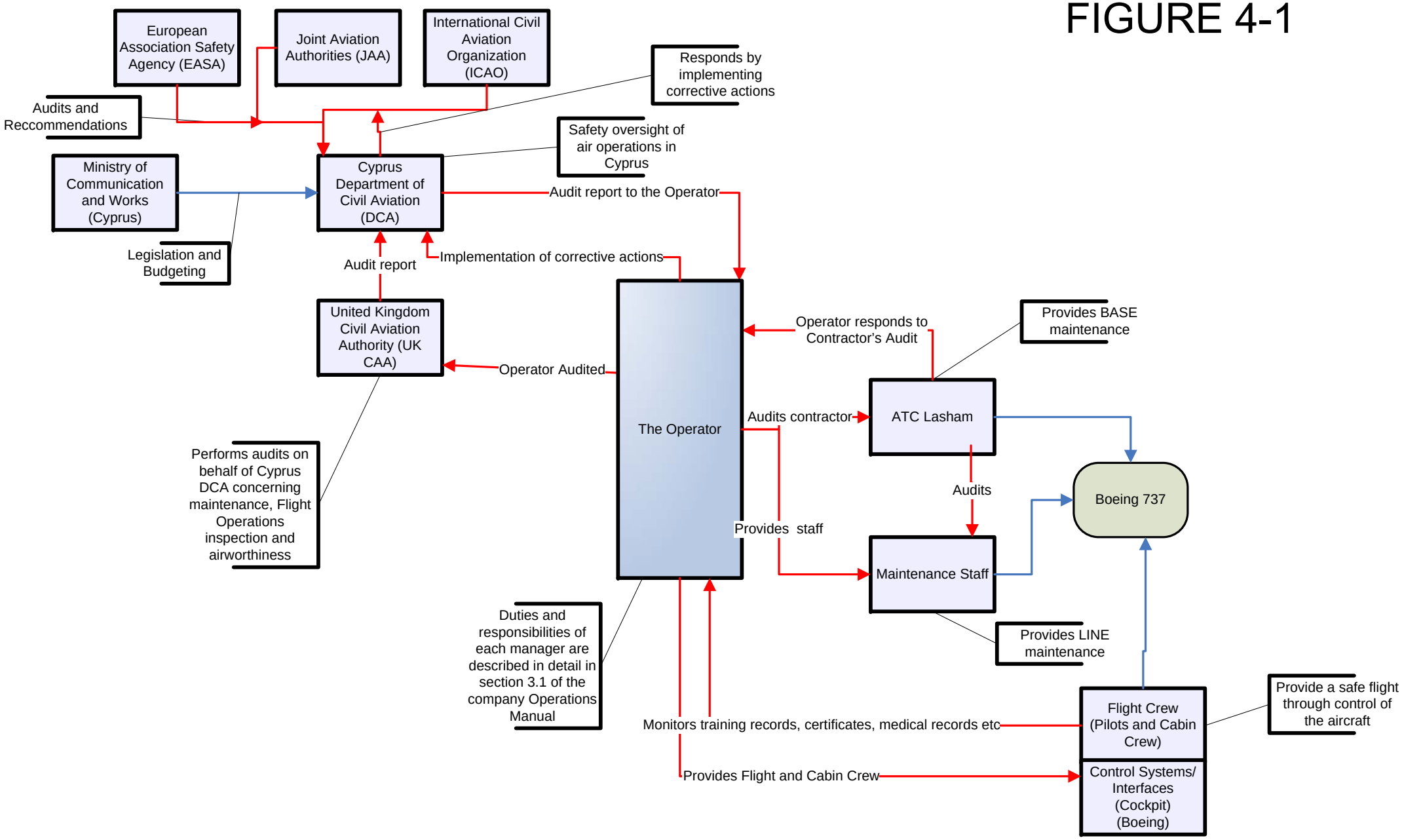


FIGURE 3-2

FIGURE 4-1


European Association Safety Agency (EASA)
Joint Aviation Authorities (JAA)
International Civil Aviation Organization (ICAO)
Responds by implementing corrective actions
Audits and Reccommendations
Safety oversight of air operations in Cyprus
Ministry of Communication and Works (Cyprus)
Cyprus Department of Civil Aviation (DCA)
Audit report to the Operator
Legislation and Budgeting
Audit report
Implementation of corrective actions
United Kingdom Civil Aviation Authority (UK CAA)
Operator responds to Contractor's Audit
Provides BASE maintenance
Operator Audited
The Operator
Audits contractor
ATC Lasham
Performs audits on behalf of Cyprus DCA concerning maintenance, Flight Operations inspection and airworthiness
Audits
Boeing 737
Provides staff
Maintenance Staff
Duties and responsibilities of each manager are described in detail in section 3.1 of the company Operations Manual
Provides LINE maintenance
Monitors training records, certificates, medical records etc
Flight Crew (Pilots and Cabin Crew)
Provide a safe flight through control of the aircraft
Provides Flight and Cabin Crew
Control Systems/ Interfaces (Cockpit) (Boeing)

Pilots: Captain and First Officer

Safety Requirements and Constraints:

- Licensed and qualified for the flight in accordance with requirements.
- Held valid medical certificates and medically fit to operate the flight.
- Resting and flight duty times in compliance with Cyprus DCA and Operator requirements.
- Two in the cockpit, one performs the other monitors.
- Accomplish flight according to Flight Safety Manual and associated procedures.

Context in Which Decisions Made:

- Time pressure to meet departure times.
- High workload after take-off.
- Stressful environment due to an alarming sound.

Inadequate Control Actions

- First Officer: Failure to set pressurization selector to AUTO as the respective checklists required.
- Captain: Failure to identify Pressurization mode selector was in MAN position during preflight procedures and after takeoff procedures.
- Failure to identify the cabin altitude warning and act as required by Non-Normal Procedures (e.g emergency descent, don oxygen masks).
- Failure to maintain a conductive to troubleshooting environment in the cockpit.
- Captain: Failed to transmit the situation to the Dispatcher/Ground Engineer.
- Not canceling Master Caution in time, caused the second event that could triggered it, to pass unnoticed.
- Captain: Concentrated on equipment cooling system instead on the fact that passengers' oxygen masks were activated.
- First Officer: Completely failed to assist Captain in the escalating situation.
- Failure to don oxygen masks which resulted in pilot's incapacitation due to no pressurization.
- Complete failure in utilizing CRM and monitor crucial processes like cabin altitude.

Model Mental Flaws

- The Takeoff Configuration Warning sounds while on ground where as Cabin Altitude Warning sounds while in the air.
- Pilots may never come across pressurization problems thus they associate the sound only with take off configuration warning.
- Not aware that passengers oxygen masks were activated.

System Design Flaws

- Both Takeoff Configuration Warning and Cabin Altitude Warning have the same sound

Feedback.

- No feedback from cabin crew that oxygen masks were activated.

Provides checklists

Manufacturer: Boeing

Safety Requirements and Constraints:

- Provides the aircraft/control systems. Aircraft control system's interface design aims to minimize pilots errors and omissions.
- Provides instructions through manuals for a safe handling of the aircraft systems.
- Receives from aircraft users' feedback and acts where appropriate in updating and clarifying instructions/manuals in pursuit of safety and proper aircraft use.

Context in Which Decisions are Made:

- Studies recommendations from incidents/accidents boards' investigations.
- Studies alerts bulletins from NASA ASRS office.

Inadequate Control Actions

- Vague instruction in AMM for Pressure Leak Test procedure. It does not specify to return the mode selector in AUTO position.
- Green indication MAN doesn't alert pilots of an abnormality.
- Preflight Procedure and checklists design was not effective against omissions from flight crew in checking and verifying controls position on the pressurization panel. They are executed in time pressure for departure and thus in a hurried manner.
- Although the position pressurization mode selector is critical for aircraft pressurization, its required position is not listed as a separate action in checklist referring to pressurization.
- Preflight Procedure may contain 40-80 actions executed by First Officer under time pressure. Execution from memory, automatically without conscious effort and attention.
- Preflight checklist for verification of Preflight Procedure may lead to false verification of items since those items were addressed just before in previous procedure.
- After Takeoff checklist carried under high workload.
- Failure to provide a distinctive sound recognition for cabin altitude warning that is mistaken as takeoff configuration warning.
- Master Caution/Overhead indication. If two events that activate master caution occur before Master Caution is canceled, the second event will not be registered to pilots.
- Overhead Panel Design. MAN illuminate indication in green, a color that typically imply nothing abnormal.
- Failure to provide effective measures although several warnings from incidents involving confusion between the two types of warnings.

Model Mental Flaws

- For the Pressure Leak Test blur instruction. The manufacturer provides several steps and actions in preflight and after takeoff checklists that would ensure that the pressurization mode selector is to be set in AUTO position.
- No illuminated indications should be presented on pressurization panel if checklists were carried out as required.
- A decline in percentage of incidents involving passenger oxygen system activation from 1999-2000 to 2003-2004 may have caused Boeing to hold back from enforcing more effective safeguards against pressurization incidents

Feedback

- Feedback channels are kept open from all associated partners in aviation industry

Provides AMM Manual

Dispatcher/Ground Engineer

Safety Requirements and Constraints:

- Provide technical assistance when situations arose while an operation(a flight) was in the air.

Context in Which Decisions Made:

- Lingual issues made underrating and communication difficult between ground and flight deck.
- Not aware of pressurization problem. Thus not aware that useful conscious time (TUC) was limited.

Inadequate Control Actions

- Dispatcher: Failure to understand Captain's concerns and placed Ground Engineer on microphone without notifying him that Captain already reported Takeoff Configuration and Equipment Cooling lights.
- Failure to notice the sounding horn on the background of the communications.
- Failure to understand that Equipment Cooling indications OFF were illuminated.
- Failure to confirm that pressurization mode selector was in AUTO position (since he was the engineer who perform the unscheduled maintenance early in the morning).
- Failure to understand the whole nature of the problem at hand and provide effective remedy.

Model Mental Flaws

- The Ground Engineer was not aware that Equipment Cooling Indications were labeled OFF.

Cabin Crew

Safety Requirements and Constraints:

- Trained and qualified in accordance with regulations.
- Duty and resting times in accordance with regulations.
- Provide cabin assistance and service in accordance with Operator's Safety Manual.
- Legal requirement to conduct a pre-flight safety briefing prior to boarding the aircraft according to the Operator's Safety Manual.
- Normal procedures outlined the interaction between cabin crew and flight deck.
- Non-normal procedures provided actions in case of an emergency such as rapid decompression and oxygen mask deployment.

Context in Which Decisions Made:

- Alarming environment due to passengers' oxygen mask deployment.
- Hypoxia setting up due to no pressurization.

Inadequate Control Actions

- No actions taken due to lack of operational procedures to address the emerging situation.

Model Mental Flaws

- Expected descent/level off of aircraft and announcement to react.

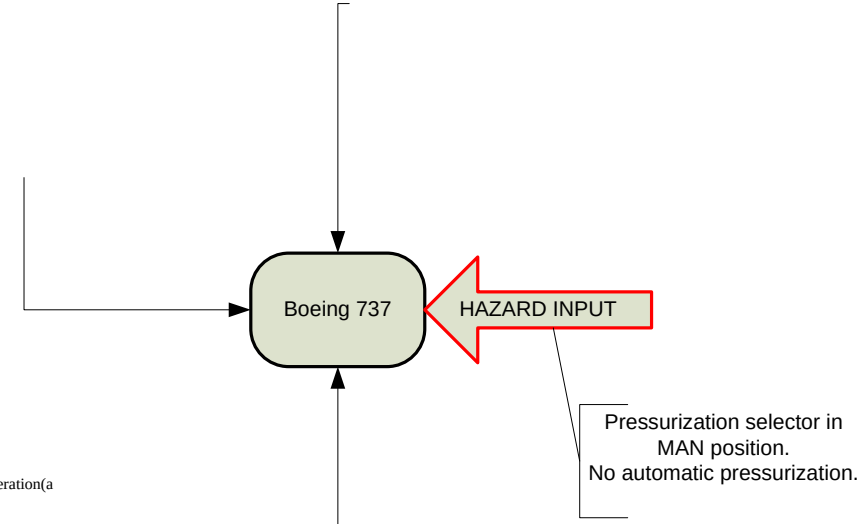


FIGURE 4-2

Manufacturer: Boeing

Safety Requirements and Constraints:

- Provides the aircraft/control systems. Aircraft control system's interface design aims to minimize pilots errors and omissions.
- Provides instructions through manuals for a safe handling of the aircraft systems.
- Receives from aircraft users' feedback and acts where appropriate in updating and clarifying instructions/manuals in pursuit of safety and proper aircraft use.

Context in Which Decisions are Made:

- Studies recommendations from incidents/accidents boards' investigations.
- Studies alerts bulletins from NASA ASRS office.

Inadequate Control Actions

- Vague instruction in AMM for Pressure Leak Test procedure. It does not specify to return the mode selector in AUTO position.
- Green indication MAN doesn't alert pilots of an abnormality.
- Preflight Procedure and checklists design was not effective against omissions from flight crew in checking and verifying controls position on the pressurization panel. They are executed in time pressure for departure and thus in a hurried manner.
- Although the position pressurization mode selector is critical for aircraft pressurization, its required position is not listed as a separate action in checklist referring to pressurization.
- Preflight Procedure may contain 40-80 actions executed by First Officer under time pressure. Execution from memory, automatically without conscious effort and attention.
- Preflight checklist for verification of Preflight Procedure may lead to false verification of items since those items were addressed just before in previous procedure.
- After Takeoff checklist carried under high workload.
- Failure to provide a distinctive sound recognition for cabin altitude warning that is mistaken as takeoff configuration warning.
- Master Caution/Overhead indication. If two events that activate master caution occur before Master Caution is canceled, the second event will not be registered to pilots.
- Overhead Panel Design. MAN illuminate indication in green, a color that typically imply nothing abnormal.
- Failure to provide effective measures although several warnings from incidents involving confusion between the two types of warnings.

Model Mental Flaws

- For the Pressure Leak Test blur instruction. The manufacturer provides several steps and actions in preflight and after takeoff checklists that would ensure that the pressurization mode selector is to be set in AUTO position.
- No illuminated indications should be presented on pressurization panel if checklists were carried out as required.

- A decline in percentage of incidents involving passenger oxygen system activation from 1999-2000 to 2003-2004 may have caused Boeing to hold back from enforcing more effective safeguards against pressurization incidents

Feedback

- Feedback channels are kept open from all associated partners in aviation industry

Pilots: Captain and First Officer

Safety Requirements and Constraints:

- Licensed and qualified for the flight in accordance with requirements.
- Held valid medical certificates and medically fit to operate the flight.
- Resting and flight duty times in compliance with Cyprus DCA and Operator requirements.
- Two in the cockpit, one performs the other monitors.
- Accomplish flight according to Flight Safety Manual and associated procedures.

Context in Which Decisions Made:

- Time pressure to meet departure times.
- High workload after take-off.
- Stressful environment due to an alarming sound.

Inadequate Control Actions

- First Officer: Failure to set pressurization selector to AUTO as the respective checklists required.
- Captain: Failure to identify Pressurization mode selector was in MAN position during preflight procedures and after takeoff procedures.
- Failure to identify the cabin altitude warning and act as required by Non-Normal Procedures.(e.g emergency descent, don oxygen masks)
- Failure to maintain a conductive to troubleshooting environment in the cockpit.
- Captain: Failed to transmit the situation to the Dispatcher/Ground Engineer.
- Not canceling Master Caution in time, caused the second event that could triggered it, to pass unnoticed.
- Captain: Concentrated on equipment cooling system instead on the fact that passengers' oxygen masks were activated.
- First Officer: Completely failed to assist Captain in the escalating situation.
- Failure to don oxygen masks which resulted in pilot's incapacitation due to no pressurization.
- Complete failure in utilizing CRM and monitor crucial processes like cabin altitude.

Model Mental Flaws

- The Takeoff Configuration Warning sounds while on ground where as Cabin Altitude Warning sounds while in the air.
- Pilots may never come across pressurization problems thus they associate the sound only with take off configuration warning.
- Not aware that passengers oxygen masks were activated.

System Design Flaws

- Both Takeoff Configuration Warning and Cabin Altitude Warning have the same sound

Feedback.

- No feedback from cabin crew that oxygen masks were activated.

Dispatcher/Ground Engineer
Safety Requirements and Constraints: • Provide technical assistance when situations arose while an operation(a flight) was in the air. Context in Which Decisions Made: • Lingual issues made underrating and communication difficult between ground and flight deck. • Not aware of pressurization problem. Thus not aware that usefuk conscious time (TUC) was limited. Inadequate Control Actions • Dispatcher: Failure to understand Captain's concerns and placed Ground Engineer on microphone without notifying him that Captain already reported Takeoff Configuration and Equipment Cooling lights. • Failure to notice the sounding horn on the background of the communications • Failure to understand that Equipment Cooling indications OFF were illuminated. • Failure to confirm that pressurization mode selector was in AUTO position (since he was the engineer who perform the unscheduled maintenance early in the morning). • Failure to understand the whole nature of the problem at hand and provide effective remedy. Model Mental Flaws • The Ground Engineer was not aware that Equipment Cooling Indications were labeled OFF.

Cabin Crew
Safety Requirements and Constraints: • Trained and qualified in accordance with regulations. • Duty and resting times in accordance with regulations. • Provide cabin assistance and service in accordance with Operator's Safety Manual. • Legal requirement to conduct a pre-flight safety briefing prior to boarding the aircraft according to the Operator's Safety Manual. • Normal procedures outlined the interaction between cabin crew and flight deck. • Non-normal procedures provided actions in case of an emergency such as rapid decompression and oxygen mask deployment. Context in Which Decisions Made: • Alarming environment due to passengers' oxygen mask deployment. • Hypoxia setting up due to no pressurization. Inadequate Control Actions • No actions taken due to lack of operational procedures to address the emerging situation. Model Mental Flaws • Expected descent/level off of aircraft and announcement to react.

Maintenance
Safety Requirements and Constraints:
- Maintenance in accordance with JAR OPS Subpart M.
- ATC Lasham was the maintenance contractor of the Operator. Contract specified the technical procedures and responsibilities of the relevant parties.
- ATC Lasham provided Base Maintenance at Lasham Airfield in UK. Certification of Base Maintenance was to be signed off by ATC Lasham approved engineers.
- All line maintenance and minor scheduled maintenance was carried out by ATC Lasham engineers of the Operator or ATC Lasham in accordance with the Part 145 approval. Certification of line maintenance minor scheduled maintenance ,inspections and defect rectification was to be signed off by the Operator or ATC Lasham engineers as authorized by ATC Lasham.
- Line maintenance was carried out at Larnaca and other approved line stations.
- Maintenance documentation was handled by ATC Lasham.

Context in Which Decisions Made:
- Upon unsuccessful efforts from the Maintenance Contractor to obtain maintenance documentation concerning activities in Larnaca from the Operator.
- Upon Level 1 findings by UK CAA audit and possible suspension of AOC of the Operator.
- High change over rate in maintenance staff at Larnaca was not conductive in establishing and maintaining teamwork.

Inadequate Control Actions
- Ground Engineer 1: Failed to carry out and document correctly unscheduled maintenance in morning of 14th of August.
- Line Maintenance: Failure to address the error message: 030 INFLOW/LEAKAGE appeared on NVM chip for the last 42 flights. Attempts proved insufficient and thus airplane was in service with repeatedly safety issues.
- Refresher familiarization courses for engineers were not held by the Operator as required.
- Inadequate resources and financial support to remedy manpower planning raised as Non Conformance report after ATC Lasham audit in April 2005.
- ATC Lasham quit efforts to obtain maintenance documentation after several attempts. This was a major issue since the Maintenance Contractor was unable to review Line Check activities carried at Larnaca.

Model Mental Flaws.
- Level 1 findings were cleared by a meeting between inspector, ATC Lasham and the Operator.
- ATC Lasham does not interrupt collaboration upon Operator's non conformance with obligation to submit maintenance documentation.

The Operator's (Management)
Safety Requirements and Constraints:
Management:
- Determination of the company's flight safety policy.
- Allocation of responsibilities and duties and issuing instructions to individuals sufficient for implementation of company policy and the maintenance of safety standards.
- Monitoring of flight safety standards.
- Recording and analysis of any deviations from company standards ensuring corrective action.
- Evaluating the safety record of the company in order to avoid the development of undesired trends and
- Liaison with the Authority.

Nominated Postholders (Manager Positions) must also have:
- Expertise in the applications of safety standards and safe operating practices.
- Comprehensive knowledge of international, European and Cypriot regulations and requirements the Operator's specifications and the need for and the content of, the relevant parts of the manuals in their areas of responsibility.
- The appropriate management experience acquired in their previous positions of at least five years, two of which preferably acquired in equivalent position in the aeronautical industry.
- Familiarity with the Operator's Quality System.

Context in Which Decisions Made:
- Low-fare operator.
- Market competition.
- Official Language: English.
- Multinational employee spectrum.

Inadequate Control Actions
- Failure to monitor maintenance contractor through audits.
- Failure to submit maintenance documentation to Maintenance Contractor.
- Failure to monitor Line maintenance.
- Failure or slow response in enforcing remedial actions for audit's findings (even in the case of Level 1 findings).
- Staffing management position with individuals who did not possess the required qualifications.
- Failure to enforce a robust in house Quality System.
- Failure to monitor, review and update training records, medical certificates and pilots' certificates concerning both flight and cabin crew. Thus no remedial action could be taken upon accident's First Officer's record.
- Key positions remained vacant for considerable time periods e.g the Training Standards Manager position. Individuals possessing two management positions such as the Operations Manager who also took over as Training Manager.
- Insufficient office time by pilots who held managerial positions.
- Failure on permissible duty times, encouragement to stretch the rules to the limits through impractical scheduling.
- Failure to provide cabin crew training for non-normal procedures e.g. in case of passenger masks oxygen mask deployment and non level off or descent.
- Failure to preserve safety culture in upper management levels and inherit it down to the operational levels.

Model Mental Flaws.
- Safety standards were not compromised although audit findings are specific e.g. July 2004 audit "The lack of operational management control is now unacceptable as there is evidence of flight safety being compromised.".
- Thought they conducted a "friendly/open door" management philosophy (whereas some staff had an opposite view).

Operator's Staff
Safety Requirements and Constraints:
- Accomplish duty tasks according to Operator's procedures and corporate manuals.

Context in Which Decisions Made:
- Multinational composition (72% Cypriots, 13% dual nationality, 13% foreign nationals).
- Official language of communication: English.
- 33% of staff were seasonal part-time employees.

Inadequate Control Actions
- Did not voice out any complaints or deficiencies concerning safety to the appropriate authorities.

Model Mental Flaws.
- Multinational composition let to different perceptions towards colleagues and procedures.
- Seasonal staff:
  1. Was not promoting professional development and personal ties that would lead to team ties and comfort to discuss incidents and issues.
  2. Feeling less important as a functional part of the operation with limited responsibility and a disregard to report any deficiencies.
  3. Feeling dispensable since it was lend to other companies due to seasonal nature of the industry.

All the above could not advocate in favor of a healthy working environment of professional standards.

Operator's Fleet

FIGURE 4-3

The Operator (Management)

Safety Requirements and Constraints:
Management:

- Determination of the company's flight safety policy.
- Allocation of responsibilities and duties and issuing instructions to individuals sufficient for implementation of company policy and the maintenance of safety standards.
- Monitoring of flight safety standards.
- Recording and analysis of any deviations from company standards ensuring corrective action.
- Evaluating the safety record of the company in order to avoid the development of undesired trends and
- Liaison with the Authority.

Nominated Postholders (Manager Positions) must also have:

- Expertise in the applications of safety standards and safe operating practices.
- Comprehensive knowledge of international, European and Cypriot regulations and requirements the Operator's specifications and the need for and the content of, the relevant parts of the manuals in their areas of responsibility.
- The appropriate management experience acquired in their previous positions of at least five years, two of which preferably acquired in equivalent position in the aeronautical industry.
- Familiarity with the Operator's Quality System.

Context in Which Decisions Made:

- Low-fare operator.
- Market competition.
- Official Language: English.
- Multinational employee spectrum.

Inadequate Control Actions

- Failure to monitor maintenance contractor through audits.
- Failure to submit maintenance documentation to Maintenance Contractor.
- Failure to monitor Line maintenance.
- Failure or slow response in enforcing remedial actions for audit's findings (even in the case of Level 1 findings).
- Staffing management position with individuals who did not possess the required qualifications.
- Failure to enforce a robust in house Quality System.
- Failure to monitor, review and update training records, medical certificates and pilots' certificates concerning both flight and cabin crew. Thus no remedial action could be taken upon accident's First Officer's record.
- Key positions remained vacant for considerable time periods e.g. the Training Standards Manager position. Individuals possessing two management positions such as the Operations Manager who also took over as Training Manager.
- Insufficient office time by pilots who held managerial positions.
- Failure on permissible duty times, encouragement to stretch the rules to the

limits through impractical scheduling.

- Failure to provide cabin crew training for non-normal procedures e.g. in case of passenger masks oxygen mask deployment and non level off or descent.
- Failure to preserve safety culture in upper management levels and inherit it down to the operational levels.

Model Mental Flaws.

- Safety standards were not compromised although audit findings are specific e.g July 2004 audit "The lack of operational management control is now unacceptable as there is evidence of flight safety being compromised".
- Thought they conducted a "friendly/open door" management philosophy (whereas some staff had opposite view).

Maintenance

Safety Requirements and Constraints:

- Maintenance in accordance with JAR OPS Subpart M.
- ATC Lasham was the maintenance contractor of the Operator. Contract specified the technical procedures and responsibilities of the relevant parties.
- ATC Lasham provided Base Maintenance at Lasham Airfield in UK. Certification of Base Maintenance was to be signed off by ATC Lasham approved engineers.
- All line maintenance and minor scheduled maintenance was carried out by ATC Lasham engineers of the Operator or ATC Lasham in accordance with the Part 145 approval. Certification of line maintenance minor scheduled maintenance ,inspections and defect rectification was to be signed off by the Operator or ATC Lasham engineers as authorized by ATC Lasham.
- Line maintenance was carried out at Larnaca and other approved line stations.
- Maintenance documentation was handled by ATC Lasham.

Context in Which Decisions Made:

- Upon unsuccessful efforts from the Maintenance Contractor to obtain maintenance documentation concerning activities in Larnaca from the Operator.
- Upon Level 1 findings by UK CAA audit and possible suspension of AOC of the Operator.
- High change over rate in maintenance staff at Larnaca was not conductive in establishing and maintaining teamwork.

Inadequate Control Actions

- Ground Engineer 1: Failed to carry out and document correctly unscheduled maintenance in morning of 14th of August.
- Line Maintenance: Failure to address the error message: 030 INFLOW/LEAKAGE appeared on NVM chip for the last 42 flights. Attempts proved insufficient and thus airplane was in service with repeatedly safety issues.
- Refresher familiarization courses for engineers were not held by the Operator as required.
- Inadequate resources and financial support to remedy manpower planning raised as Non Conformance report after ATC Lasham audit in April 2005.
- ATC Lasham quit efforts to obtain maintenance documentation after several attempts. This was a major issue since the Maintenance Contractor was unable to review Line Check activities carried at Larnaca.

Model Mental Flaws.

- Level 1 findings were cleared by a meeting between inspector, ATC Lasham and the Operator.
- ATC Lasham does not interrupt collaboration upon Operator’s non conformance with obligation to submit maintenance documentation.

Operator's Staff
Safety Requirements and Constraints: • Accomplish duty tasks according to Operator's procedures and corporate manuals. Context in Which Decisions Made: • Multinational composition (72% Cypriots,13% dual nationality, 13%foreign nationals). • Official language of communication: English. • 33% of staff were seasonal part-time employees. Inadequate Control Actions • Did not voice out any complaints or deficiencies concerning safety to the appropriate authorities. Model Mental Flaws. • Multinational composition let to different perceptions towards colleagues and procedures. • Seasonal staff: 1. Was not promoting professional development and personal ties that would lead to team ties and comfort to discuss incidents and issues. 2. Feeling less important as a functional part of the operation with limited responsibility and a disregard to report any deficiencies. 3. Feeling dispensable since it was lend to other companies due to seasonal nature of the industry. All the above could not advocate in favor of a healthy working environment of professional standards.

International Oversight Organizations (ICAO,JAA,EASA)
Safety Requirements and Constraints:
- Ensure that oversight authorities are enforcing the Chicago Convention.
- Ensure that aviation safety is not compromised on international level.
- Propose regulations in order to achieve all of the above.

Context in Which Decisions Made:
- International Level.

Inadequate Control Actions
- Although their audits clearly showed the DCA's deficiencies; no pressure was excreted in order for the latter to meet its international obligations in the shortest possible time.

Model Mental Flaws.
- Although they have international range, such organizations have no legal authority. The responsibility rests to the state in order to comply with proposed regulations.

Cyprus Department of Civil Aviation (DCA)
Safety Requirements and Constraints:
- Fulfill state's obligations under the Chicago Convention.
- Oversight of flight operations and maintenance.
- Licensing of operational personnel.
- Aircraft certification.
- Certification of air operators and maintenance organizations.

Context in Which Decisions Made:
- Understaffed.
- Voices that Helios was given preferential treatment (no SAFA checks).
- Non-colleague atmosphere.

Inadequate Control Actions
- Lack of resources and qualified personnel.
- Inadequacy in performing oversight duties as required by ICAO.
- Inadequate training for Cypriots inspectors to assume fully the inspecting duties.
- Heavy reliance on UK CAA.
- Lack of DCA competency to assess UK CAA inspections and audit reports findings.
- Lack of ensuring corrective actions are implemented by the audited Operator
- Inadequacy in DCA structure to monitor oversight in Cyprus.
- Lack of exploitation of courses offered by the UK CAA to Cypriot inspector in order to prepare them for assuming sole inspection duties.
- Inadequacy of effective implementation of corrective action plans from international organizations.

Model Mental Flaws.
- UK CAA from advisor was the de facto oversight body, replacing DCA.

Aviation Industry Safety
Public Safety

UK CAA
Safety Requirements and Constraints:
- .Audits the Operator on behalf of Cyprus DCA by contractual agreement.

Context in Which Decisions Made:
- Advising nature of UK CAA towards Cyprus DCA.

Inadequate Control Actions
- Consented in clearing findings, even of Level 1, in a meeting.

The UK CAA due to the advising legal role could not take any action in proposing and ensuring that corrective actions are effectively implemented.

Model Mental Flaws.
- The auditor could not ensure or take measures against the audited if corrective actions are not implemented.

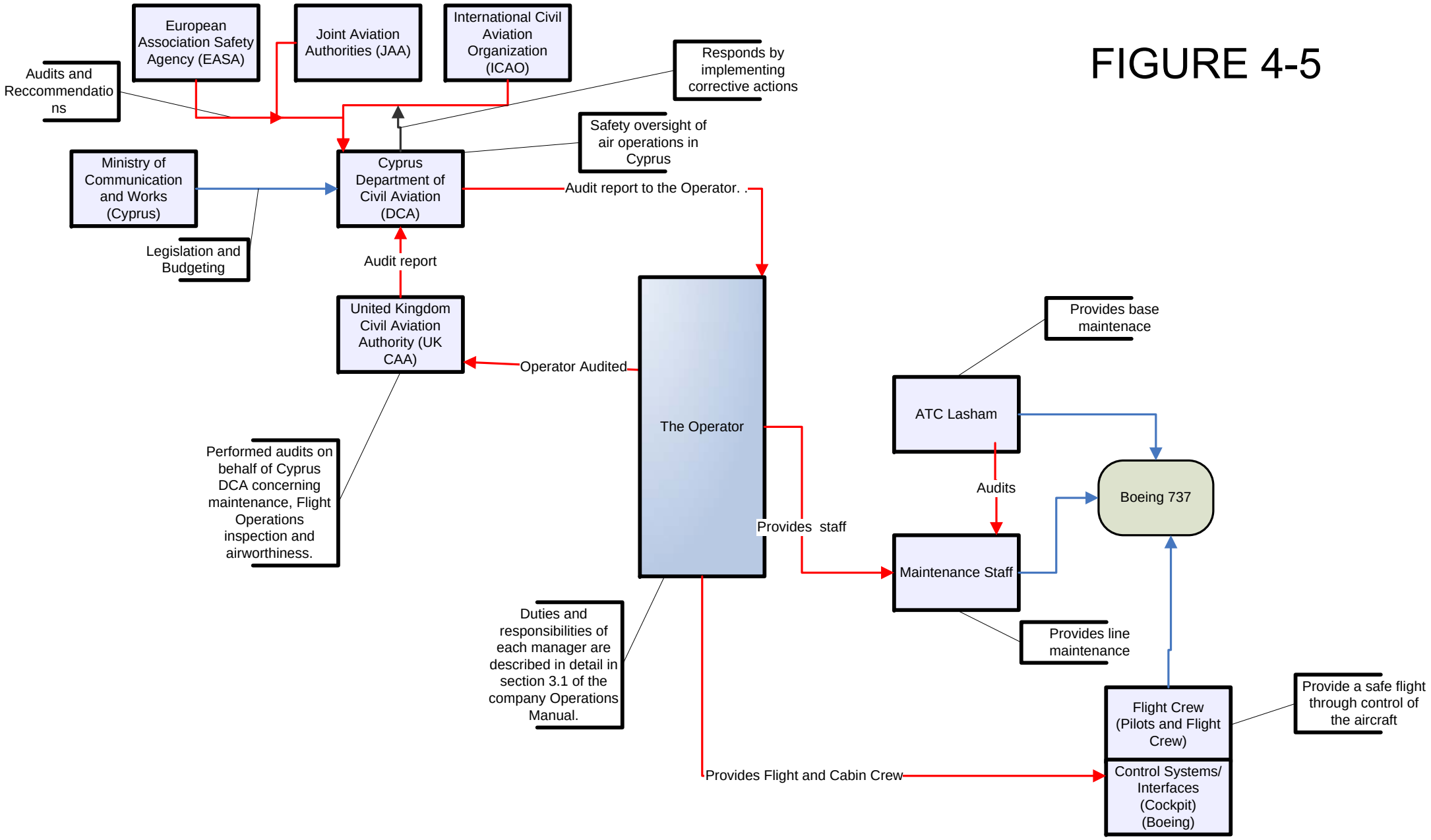
FIGURE 4-4

Cyprus Department of Civil Aviation (DCA)
Safety Requirements and Constraints: • Fulfill state's obligations under the Chicago Convention. • Oversight of flight operations and maintenance. • Licensing of operational personnel. • Aircraft certification. • Certification of air operators and maintenance organizations. Context in Which Decisions Made: • Understaffed. • Voices that Helios was given preferential treatment (no SAFA checks). • Non-colleague atmosphere. Inadequate Control Actions • Lack of resources and qualified personnel. • Inadequacy in performing oversight duties as required by ICAO. • Inadequate training for Cypriots inspectors to assume fully the inspecting duties. • Heavy reliance on UK CAA. • Lack of DCA competency to assess UK CAA inspections and audit reports findings. • Lack of ensuring corrective actions are implemented by the audited Operator. • Inadequacy in DCA structure to monitor oversight in Cyprus. • Lack of exploitation of courses offered by the UK CAA to Cypriot inspector in order to prepare them for assuming sole inspection duties. • Inadequacy of effective implementation of corrective action plans from international organizations. Model Mental Flaws. • UK CAA from advisor was the de facto oversight body, replacing DCA.

UK CAA
Safety Requirements and Constraints: • Audits the Operator on behalf of Cyprus DCA by contractual agreement. Context in Which Decisions Made: • Advising nature of UK CAA towards Cyprus DCA. Inadequate Control Actions • Consented in clearing findings, even of Level 1, in a meeting. *The UK CAA due to the advising legal role could not take any action in proposing and ensuring that corrective actions are effectively implemented.* Model Mental Flaws. • The auditor could not ensure or take measures against the audited if corrective actions are not implemented.

International Oversight Organizations (ICAO,JAA,EASA)
Safety Requirements and Constraints: • Ensure that oversight authorities are enforcing the Chicago Convention. • Ensure that aviation safety is not compromised on international level. • Propose regulations in order to achieve all of the above. Context in Which Decisions Made: • International Level. Inadequate Control Actions • Although their audits clearly showed the DCA's deficiencies; no pressure was excreted in order for the latter to meet its international obligations in the shortest possible time. Model Mental Flaws. • Although they have international range, such organizations have no legal authority. The responsibility rests to the state in order to comply with proposed regulations.

FIGURE 4-5


European Association Safety Agency (EASA)
Joint Aviation Authorities (JAA)
International Civil Aviation Organization (ICAO)
Audits and Reccommendations
Responds by implementing corrective actions
Safety oversight of air operations in Cyprus
Ministry of Communication and Works (Cyprus)
Cyprus Department of Civil Aviation (DCA)
Audit report to the Operator. .
Legislation and Budgeting
Audit report
United Kingdom Civil Aviation Authority (UK CAA)
Operator Audited
The Operator
Provides base maintenace
ATC Lasham
Performed audits on behalf of Cyprus DCA concerning maintenance, Flight Operations inspection and airworthiness.
Audits
Boeing 737
Provides staff
Maintenance Staff
Duties and responsibilities of each manager are described in detail in section 3.1 of the company Operations Manual.
Provides line maintenance
Flight Crew (Pilots and Flight Crew)
Provide a safe flight through control of the aircraft
Provides Flight and Cabin Crew
Control Systems/ Interfaces (Cockpit) (Boeing)

SYSTEM.“SYSTEM DYNAMICS for Helios Airways Flight HCY 522”
EVENT: Crashed

System Level

1) Government Policy and legislation

2) Regulatory bodies and Associations

3) Local area Government. Company management: Planning and Budgeting

4)Technical and Operational Management

5) Physical processes and Actor activities

6)Equipment and surroundings

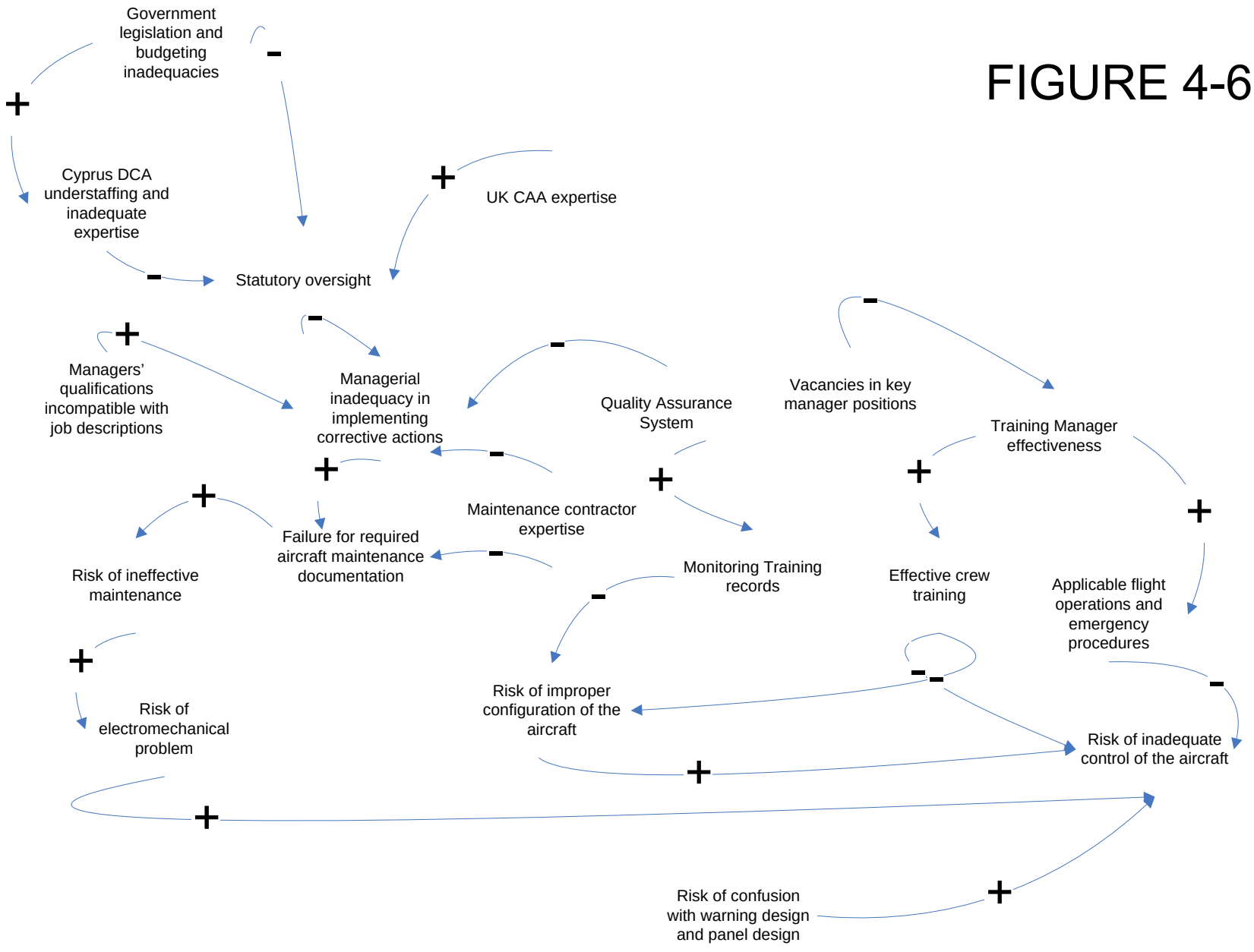


FIGURE 4-6

APPENDIX B

In this appendix, the ‘Look up tables’ are printed which are associated with Appendix C diagram and the AcciMap (Figure 3-2).

LEVEL 2
REGULATORY BODIES AND ASSOCIATIONS
ACCIMAP
Coding:200

α/α	EVENT	ACTION		Reference in report	Comments
201	Cyprus DCA	1. <u>Audits by ICAO</u> *1996* Personnel Licensing : The DCA does not have a structure, policy or procedures for personnel licensing and training. Flight Operations The DCA Director has no authority to establish a flight operations inspections organization to assist in carrying out the functions and responsibilities of the DCA .The DCA has limited information available regarding the system of air operator certification and surveillance. There is no established system for the continued surveillance of operators. Airworthiness: The DCA does not fully comply with Article 12 of the Convention which requires the State to assume responsibility for ascertaining that aircraft on its registry and operations within its jurisdiction comply with the Standards laid won in th Annexes to the Convention. *1999* Technical review, inspection, and evaluation tasks were conducted by the UK CAA and the DCA was responsible for taking action on the basis of information and advice provided by the UK CAA.		Page 88 Sec. 1.17.3	

α/α	EVENT	ACTION		Reference in report	Comments
		The DCA had no internal expertise to assess the inspection conducted on it behalf or to assess any other technical aspects of the work performed.. Difficulties of DCA to comply with ICAO Standards and Recommended Practices and insufficient and inadequately trained and qualified staff. Corrective action plan: The use of UK CAA to develop appropriate regulations for airworthiness and flight operations matters.(target completion 1999). A legal advisor service to develop primary legislation and civil aviation regulation (target completion 2000).To recruit personnel including inspectors who would be properly trained to gradually function independently by the end of 2001. The intention ti assess the feasibility of establishing a licensing system for commercial pilots and maintenance engineers. *2002* Limited progress. A draft of Civil Aviation Law was found not to contain several essential provisions considered to be important for an effective and efficient system of safety oversight in Cyprus. Deficiencies in organization, definition of duties and responsibilities, staffing, recruitment of qualified personnel, formal training policy and program for inspectors. The above were attributed			

α/α	EVENT	ACTION		Reference in report	Comments
		to the inevitable bureaucracy since DCA is a functional department of the Ministry of Communications and Works which limits it effectiveness and efficiency. A system for pilot and engineer licensing (issuance and validation) was still not in place. *August 2005 (after accident)* A letter from president of ICAO expressing the magnitude of ICAO's concern about the safety oversight capability in quantity terms. A lack of effective implementation in excess of 15% generally indicates significant problems in terms of State oversight capability. The2002 audit determined the lack of effective implementation of corrective action plans following the previous audits was 46.57%". 2. <u>Audits by JAA.</u> *2003* DCA urgently develop its ownership of the commitment made towards the Chicago Convention and the Cyprus Arrangements by increasing its human resources in all JARs' related fields (Airworthiness/Maintenance Operations and Licensing) and provide the necessary training to its personnel. Take more ownership of the Aviation Safety Regulatory activity by developing its own aviation safety culture and to fine a comprehensive			

α/α	EVENT	ACTION		Reference in report	Comments
		solution to the complex personnel matter *2004* The DCA must maintain its existing program of support by external agency expert assistance It remains clear that the presence of the current consultant is essential part of the good running of the system at least for the time being" *2005 April OPST* The Authority has not established a procedure for renewals of AOCs as AOCs have no expiry date. Only one out four of the inspecting staff is permanently employed as a member of SRU. Two are by short term contracts and the remaining one is seconded from UK CAA. This situation seems to be inadequate in order to fulfill the responsibilities and duties of an oversights function. The Authority could not document how findings from inspections carried out in 2004 had been responded to by operators. The Authority could not provide inspection plan for the previous years (2004). The Authority has not established a procedure for issuing Operational Directives. 3. <u>By European Commission</u> (after accident) *August 2005* The officials found the Cyprus DCA to still be			

α/α	EVENT	ACTION		Reference in report	Comments
		lacking the necessary strength to comply fully with is international obligations. Recommended that Cypriot Government to take the necessary political commitment to supply DCA with resources required to carry out fully its safety oversight function and to reorganize the chain of command in order to give safety the high priority it deserves inside the organization. 4. <u>By Private Firm November 2005</u> (after the accident): The structure of the DCA to support safety oversight is inadequate to support current and future operations. The Systems supporting the technical programs are not fully implemented in the areas of safety and security. At the time of this Diagnostic there was no evidence that confirmed the existence of any Risk Management process within the DCA. The DCA has not taken a more controlling position in directing the contracted (UK CAA) and allowed them to perform as they saw fit. Airworthiness Section : Understaffed and also unable to adequately cover required ICAO safety requirements.			

α/α	EVENT	ACTION		Reference in report	Comments
202	UK CAA Audits/Inspection-Helios	1. 2003 Audit An in-house Quality System should be adopted as soon as possible 2. March 2004 Audit Deficiencies in the areas of updating Operational Manuals, training files, recording of scheduled and permissible duty and rest times. The system in place for monitoring pilots' certificates, medicals and training was characterized as unable to access any historical data. Senior management personnel were not logging sufficient office time. Requirement of a robust in house quality system, by the 2003 audit had not been enforced. Such a system would identify above findings and an appropriate action would have been taken 3. April 2004 audits. 7th April. Inspectors stated that the 1 May 2004 target start date for the Boeing 737 is no longer realistic since Operators has not submitted Part B, C, D, Cabin Crew Manual and MEL . 4. July 2004 the same CAA UK inspector who reviewed all previous audits on the 30th of		Page 88 sec.1.17.3.2-3	1. Audits between 23 March and 1 May 2004 concerned the inclusion of the accident aircraft in the Operators AOC. 2. A few days away from 1st of May several deficiencies needed to be addressed (ELT missing). Various Sections of manuals (MEL, Operations Manual Part A,B, Cabin Safety Card, Cabin Crew Manual, Flight Safety Manual and QRH) were re-submitted up to 2 times during a three day audit. 3. The Accountable Manager was notified in November 2003,March 2004 and July 2004 in not meeting the expected standards of the

α/α	EVENT	ACTION		Reference in report	Comments
		April noted that: The lack of operational management controls is now unacceptable as there is evidence of flight safety being compromised. The Accountable Manager must be asked to formally review his management structure and staff as clearly urgent action is required now. 5. July 2004 audit. No action was taken to fill the post of the Training Manager Standards 6. July 2004 audit : Aircraft Inspection/ Facilities and Organization Inspection characterized as symptomatic of a lock of operational management control which had resulted in pilots being cleared to operate public transport flights without the necessary competence etc. Pilots with managerial duties didn't dedicate inadequate office duty time. Incomplete training records . Crew minimum resting times were violated. Crew records lacked certificate of competence in case of pilot incapacitation 7. September 2004 Audit. Pointed the continuing deficiencies in the area of Quality System, updating records (duty and training) the amount of office time spent from pilots holding managerial positions.. Audit stated that the vacant position of Training Manager			Operatior. Lack of operational Management control at the airline. Training Manager Standards had resigned. DCA is alerted. 4. DCA was alerted for this unacceptable situation. 7. DCA forwarded audit, observing that "The issues of Training Post Admin. Time for management pilots and quality system to be subject to follow up actions." Previous reports did not carry any comments or signatures from Cyprus DCA.

α/α	EVENT	ACTION		Reference in report	Comments
203	UK CAA Audits/Inspection-Maintenance , ATC Lasham (on behalf of Cyprus DCA)	1. 2nd June 2004 audit. Findings of 2003 audit had not been corrected. Eight findings were raised, two of the as level 1 : Failure of the operator (as a JAR OPS operator) to submit compete maintenance document to ATC Lasham as (maintenance contractor). Incomplete records of the maintenance tasks and inadequate definition of who was responsible for the completion of the Maintenance Card Summary Pages. 2. 9-10 November 2004. Letter to ATC Lasham stating that findings from previous audits (1,3,4,5,6) will be raised to level 1 if adequate corrective has not been implemented, by 17 December 2004 7th December 2004. All critical findings were confirmed closed at the meeting between CAA Inspector , Technical Manager of ATC Lasham and the Operator.		Page 90	2) At level 1 Helios Airways JAR OPS Maintenance Management approval and AOC will be suspended. It is Helios responsibility to ensure that matters are corrected satisfactory. ATC Lasham has contractual obligations to address findings 4,5,6,7 and to monitor the actions taken to correct findings 2 and 3. The findings: 1. Helios Airways has not carried out an audit on the JAR OPS maintenance functions performed on its behalf by ATC Lasham. 2. Errors noted in a completed A Check work pack documentation returned to ATC Lasham from Helios staff at Larnaca. Errors included incomplete dating

α/α	EVENT	ACTION		Reference in report	Comments
					documentation,not grouping together stamps cleared by a single stamp and depanel charts not stamped. 3. Helios is still not returning completed maintenance documentation in timely manner. 4. No procedure for closing completed work packs of maintenance document that are returned to Technical Records from JAR OPS operators supported by ATC Lasham. 5. It was not clear who is responsible for confirming that all maintenance tasks have been completed on the Maintenance Card Summary Pages, 6. Technical records do not appear to hold the original copies of

α/α	EVENT	ACTION		Reference in report	Comments
					Airworthiness Directive compliance documentation for Helios Airways as defined by the contract Helios/ATC 7. Technical records do not appear to hold original copies of Log Technical Paes or JAA Form 1's ad defined by Helios/ATC contract. 8. It is suggested that ATC Lasham introduces a sample procedure to assist in identifying some of the problems identified above. 9. Aircraft Survey of 5B-DBI was carried during visit. Minor findings only recorded on aircraft Survey form.
203	Cyprus DCA audit	Maintenance audit. June 2005 Level 2 findings. Helios responded on 2nd August 2005			

α/α	EVENT	ACTION		Reference in report	Comments
204	UK CAA Audits/Inspection-Helios 2005	2005 Audits. March 7-10 Inspection. Quality System and Quality and Operations Manuals were found to have serious deficiencies. A two to three months time was given to address those deficiencies. Also it was reported that "Not all company personnel had been provided with quality related briefing as required and that the required meeting by several manager was not taken place as required,. Other concerns were variation of time flight limitations.. Inspector concluded that a lack of resources resulted in not having the relevant and related staff in certain areas of operations.. In June 2005 audit found an improvement in management's attempts to address raised findings but there was a concern as to how long the improvements will continue. September 2005 audit found 4 issues, the 3 of them were identical to previous audits :Insufficient office time for management pilots, lack in robustness of the Quality System and Impractical Methods of scheduling timing of routes to meet Flight Time Limitations. The fourth finding stated that The normal checklist did not appear in any manual aboard the aircraft			

LEVEL 3
(LOCAL AREA GOVERNMENT, COMPANY MANAGEMENT, PLANNING AND BUDGETING
ACCIMAP
Coding:300

α/α	EVENT	ACTION		Reference in report	Comments
301	Operators manager positions staffing/vacancies	1. At time of accident: Security Manager position was vacant 2. Position of the Training Manager was covered by the Flight Operations Manager		Page 74 1.17.13	
302	The Accountable Manager (CEO)	1. In office since June 2002. Cypriot citizen. 2. He stated that "no factors giving rise to causes for accident had mentioned", "he had never been informed that the company that may be degrading safety". 3. Believed that key positions were appropriately staffed and managed 4. He established open door policy when asked about working climate. 5. After his arrival weekly safety meetings had stopped. Replaced by meetings when situation arose, every 15 days or even sooner		Page 75 sec 1.17.1.4	UK CAA advised CEO in November 2003,March 2004,July 2004 of shortfalls in the standards that were expected of the Operator and of a lack of operational management control at the airline. Meetings statement by Flight Operation Managemer

α/α	EVENT	ACTION		Reference in report	Comments
303	The Chief Operating Officer	1. Assumed position in August 2005 (2 weeks before the accident). British Citizen. 2. He stated that Operator "gave some of concern", "there appeared to be a culture of fear where people encouraged to stretch the rules to the limits" and that "aircraft utilization was extremely high with inadequate down time". He said that schedules were extremely tight and there was some evidence that flight times were manipulated to bring them into limits		Page 75 sec 1.17.1.5	Several audit findings concerning schedule, time limits etc.
304	Commercial Manager	1. Cyprus Citizen 2. Stated that Operator had "positive work climate of collaboration and mutual respect … the current owners promote the same style of management, professional on a friendly basis".		Page 76 sec 1.17.1.6	
305	Flight Operation Manager	1. British Citizen 2. He described accident's First Officer very experienced. Despite this, he moved around a lot in different companies in his career, different philosophies and that		Page 76 sec 1.17.1.8	

α/α	EVENT	ACTION		Reference in report	Comments
		held him back from developing important skills in areas of CRM and decision making, 3. He had ordered a line check on the accident's Captain "with an emphasis on CRM" after receiving complaints. Complaints were not confirmed and the like check found him "satisfactory"			
306	Chief Pilot	1. Since December 2000. Bulgarian Citizen 2. Acknowledged the existence of cross-cultural friction as in any multi-national environment. 3. Believed there was a a family atmosphere among pilots and an open company culture. 4. He never saw any actual reports of complaints about the accident's Captain although he heard some by some First Officers (not following SOPs')		Page 77 sec 1.17.1.9	
307	Flight Safety Officer	1. Since December 2004.		Page 78	

α/α	EVENT	ACTION		Reference in report	Comments
		Cyprus citizen. 2. Instead of Safety Management System the Operator had a Flight Safety Program. Also his office managed a Flight Data Monitoring program and flight crews were invited to submit safety reports using company supplied reports.		sec 1.17.1.10	
308	Quality Manager	1. In office since June 2004. Cypriot citizen 2. Stated that he had not perceived any weaknesses in the maintenance of flight operations areas.		Page 78 sec 1.17.1.11	
309	Technical Manager	1. In office since Octeber 2004. Cyprus Citizen 2. He stated that Ground Engineers available during August was sufficient for scheduled maintenance and that in case of an unexpected need the Operator would request additona support for Cyprus Airways.		Page 79 sec 1.17.1.12	
310	Maintenance Manager	1. Since May 200. Slovenian citizen.		Page 79 sec 1.17.1.13	

α/α	EVENT	ACTION		Reference in report	Comments
		2. He was responsible as a Maintenance Manager to implement the approved maintenance program. 3. He described the accident aircraft as the "best-300" he had encountered in his 18-year career handling this type of aircraft.			
311	Operators Management	1. The qualifications of some managers did not to those required by job descriptions. 2. A number of interviews employees complaint about the management . The Accountable manager was characterized as unapproachable with little regard or concern for safety or for the well-being of the company employees.		Page 137 sec2.7.1	Confirming statement of former Technical Manager. UK's inspectors comments that the potential flight sayfety was being compromised due to the lack of operational management control and the hesitance with which some improvements were made.
312	Management Deficiencies in Training Manager Standards position	1. A Training Manager Standards had been appointed in March 2005 but resigned in 25 July 2005. Flight Operations			

α/α	EVENT	ACTION		Reference in report	Comments
		Manager assumed responsibilities of the Manager Training Standards. 2. Associated with the failure of the Operator to recognize and take appropriate corrective actions to remedy the chronic checklist and SOP omissions of the First Officer documented in his training records.			
313	Operator Staffing	1. Potential implications of multi-national staff composition. Different perceptions towards certain characters behavior 2. Large percentage of seasonal (part time) employees. Continuous changes in staff, is not promoting team ties and especially the comfort to discuss incidents or problems among employees and management. Also employees lacked sense of continuity and felt extendible.		Page 137 sec 2.72	Influence on CRM
314	Safety Culture	1. Standards existed in manuals for an accident prevention/safety management program. It was not clear if Operator met those standards. Those standards seem			

α/α	EVENT	ACTION		Reference in report	Comments
		to promote a reaction approach rather than a proactive one towards safety. Standards did not clearly and definitively point out the role and responsibility of management in ensuring and maintaining safe operations of the company. 2. Chief operating officer's statement seem to be illuminating. Resources utilized to the limit were not conductive in maintaining a safe environment. In addition such environment provides ground for human factor errors in flight operations and aircraft maintenance. 3. Audit reports provide findings that repeatedly concerned inspectors. (see level 2) 4. The fact that although First Officer's training record showed some concerning issues, not action was taken by management for remedies (Chief Pilot or Training			

α/α	EVENT	ACTION		Reference in report	Comments
		Manager) show that the Operator lack a mechanism and means to monitor its pilots. The often vacancy of Training Manager Position also amplified this.			
315	Quality Assurance	1. DCA and audit reports pointed that an effective Quality System was lacking at Helios. 2. The delay in appointing a Quality Management, the failure to set forth a quality audit plan and the non availability of any documents to suggest the internal management evaluations was taking place as required were all proof for that. 3. According to the Quality Manual "Auditors should not have any day to day involvement in the area of operations and/or maintenance activity which is to be audited. Yet the 3 appointed quality auditors were the Technical Pilot, the Quality Manager himself and the Technical Manager. 4. The official approval of the		Page 140 sec 2.7.4	

α/α	EVENT	ACTION		Reference in report	Comments
		DCA was not evident on the manuals. In certain manuals it was impossible to track the most recent revisions. 5. A 2004 audit Operations Manual, Part A, which was the Flight Operations Manager responsibility needed revisions. Examining the Operators manuals sufficient evidence that they were being properly updated was not found. 6. The Flight Operation manager incorporated only 'important', according to his judgment, updates to manuals issued by the manufacturer. 7. Case of the After Takeoff checklist was not revised as "AIR COND & PRESS…ON" and "PACKS…..AUTO" from "AIR COND & PRESS….SET"			

LEVEL 4
TECHNICAL AND OPERATIONAL MANAGEMENT INVOLVED
ACCIMAP
Coding:400

α/α	EVENT	ACTION		Reference in report	Comments
401	Vague AMM instruction for Cabin Pressure Leak test	1. AMM Task 05-51-91-702-001, F 'Put the Airplane back to its initial position'		Page 116 par 3,4	
402	First Officer's training record comments	1. Operator Proficiency Certificate, March 9nth 2005 2. "Standards achieved, but with room for lots of improvement. Some difficulties met in complex tasks. Do not rush through check lists. Recommendation –improve your understanding on the use of AFS"(Automatic Flight System) 3. A review of his training record (5 year period) uncovered remarks and recommendations referring to check list discipline and Standard Operational Procedures (SOP) difficulties		Page 13 par 1,2	
403	Cabin Crew	1. The two cabin crew members sitting behind the cockpit could hear the warning horn			Slow decompression involved in the accident

α/α	EVENT	ACTION		Reference in report	Comments
		2. Cabin crew was sufficiently trained to recognize physical characteristics of lack of pressurization.. 3. Flight Safety Manual mentioned the two types of decompression slow and rapid/explosive but discussed symptoms only for the rapid/explosive type . 4. Cabin crew members (including Cabin Chiefs) appeared to be confused in the availability and exact procedure of means available to open the cockpit door.			
404	Maintenance in Larnaca	1. 3-4 engineers 2-3 mechanics 2. Personnel change more than 80% three times within 16 months 3. Longest: 21 months Shortest: 3 days		Page 132 par3,4,5	Categorization of personnel as 'permanent' and 'contract' in employment status

α/α	EVENT	ACTION		Reference in report	Comments
		4. High rate of personnel change didn't favor the establishment of continuity and teamwork among employs. This also was preventing the setting of a good foundation in proactive management. 5. ATC Lasham Line Station Audit. June 2005. Findings concerning several operations matters such as manpower planning, processing matters , documentations material and equipment management.			
405	Engineer 1	1. Responsible for flight HCY522 preparation in the morning of 14rth August was hired through employment agency. 2. He was also employed by Helios two years earlier for 8 months (25/10/02-20/6/03). In the second period starting 15 April 2005, there was no			

α/α	EVENT	ACTION		Reference in report	Comments
		evidence that he participated a refresher familiarization course as prescribed by the MME. In fact he stated that he was not aware of such courses.			
406	Former Operator's Technical Manager	1. Resigned in January due to mismanagement in areas such as : Staffing of Managers posts with individuals with did not have required qualifications or did not possess managerial competence , Lack of business planning, incoherent corporate operations and occasional coverage of personnel requirements in all specialties of the corporate operations.			
407	Helios failure to provide maintenance documentation to ATC Lasham	1. ATC Lasham Technical Manager repeatedly requested the completed maintenance documentation as contract requires. Attempts failed and ATC Lasham quits requesting documentations		Page 134 par3	Finding from 2004 2005 audits
408	Level 1 findings reported as level 2, cleared by a later meeting	2. The philosophy of level 1 findings is the last barrier in interrupting a sequence of events tha may lea to an		Page 134 par 4	

α/α	EVENT	ACTION		Reference in report	Comments
		accident.			
409	Continuous Leakage of the aircraft	1. NVM recorded fault messages “030 INFLOW/LEAKAGE’ for 74 flight legs		Page 134 par 5	Messages were due to low flow through the OFV either because of low inflow or higher leakage rates in the aircraft fuselage.
410	Rapid decompression Incident	1. On 16 December 2006 the accident aircraft experienced rapid decompression at 2. FL 350 cruising level.		Page 135 par1	
411	Continuing Problems with equipment cooling systems	1. Nine-write ups in the Aircraft Technical Log concerning equipment cooling. 2. Problems persisted despite maintenance actions.		Page 135 par1	Problems with equipments system cooling occurred and on the accident flight. Unsolved technical issues that continued to exist are indications of organizational inadequacies of Helios Airways concerning maintenance organization. The equipment cooling system preoccupied the pilots at those crucial moments during the aircrafts’ ascend.
411	Crew Scheduling	1. Records available to the investigation board showed		Page 135 2.6.2	

α/α	EVENT	ACTION		Reference in report	Comments
		crew duty time within limits. 2. Several audits showed that Captain's Deviation Reports (CDRs) showed flight and duty times exceeded the approved limits and were not recorded or reported to the DCA. 3. There were statements that scheduling of flights was based on unrealistic times for some routes in order to fit limitations.			
412	Flight Crew Training	1. Approved by DCA and carried out in accordance with Helios Flight Training Manual 2. Syllabus and simulator training included only rapid decompression situations. Slow loss of pressurization situations were not included. Thus the crew was not aware of how to detect the gradual loss of pressurization as in the case of accident 3. Requirement in Helios		Page 135 2.6.3	Norwegian AIB proposed as safety recommendation to the airline involved in loss of pressurization incident ,Norway 2001, that gradual pressurization situations be included in simulator training.

α/α	EVENT	ACTION		Reference in report	Comments
		Training Manual required cabin and flight crew to be trained to the phenomena associated with hypoxia. 4. Lack of hypoxia training to sensitize flight crews in detecting gradual decompression or non pressurization of the aircraft during climb is a common situation in the airline industry			
413	Actions after oxygen mask activations in case of not level off or descend.	1. Operator's deficiencies in procedures and actions taken in such case.		Page 135 par3	Also other airlines in Cyprus and Greece did not have such procedures.
415	Accessing cockpit upon emergency	1. Only crew upon promotion to Cabin Chiefs were aware of the appropriate procedure. 2. Helios Flight Safety Manual contained guidance to the procedure but only for the case the door lock mechanism was inactive.		Page 136 par 4	

LEVEL 5
(PHYSICAL PROCESSES AND ACTOR ACTIVITIES
ACCIMAP
Coding:500

α/α	EVENT	ACTION		Reference in report	Comments
501	Decompression Event on previous flight			Page 21	
502	Pre-departure Unscheduled Maintenance	1. Pressure Leak Test (not completely in accordance with AMM) 2. Completing logbook(not compatible filling) 3. Left Pressurization mode selector was left to MAN (manual) position 4. Not consulting the flight crew for the maintenance activities		Page 113 par 2 -page 115	DCPS shows continous leakages.
503	Preflight Duties (Preflight Procedure, Before Start Procedure, Before Taxi Procedure, Before Start Checklist)	1. Failure to locate the selector in MAN position. 2. Failure to note the presence of the green light indicating MAN selector position		Page 117 See 1.17.2.2	Duties involving over 80 actions.
504	Human Factors (I)	1. 'look without seeing' 2. memorization of long list, automatic execution without consciousness and attention 3. Assumption that every switch/indicator is in expected position.		Page 118,par 4 –page 18	Pressurization selector very rarely in not AUTO position. Green colour is not associated with something not normal. Orange is

α/α	EVENT	ACTION		Reference in report	Comments
					associated with caution. Red with warning.
505	Preflight Checklist	1. Oral Execution 2. item 12 of 15 'AIR COND &PRESS… PACKS, BLEED ON, SET 3. Failure to detect improper configuration of the pressurization panel		Page 119	First opportunity to correct earlier error.
506	Checklist Design/Human Factors (II)	1. Refers to two different system with the same source of energy,i.e air From the three only the third refers to pressurization panel. 2. SET reply only by confirming landing and cruise altitude in practise, since relevant pressurization panel actions were performed just before during Preflight Procedure. 3. Checklist carried out in time pressure circumstances. Often in hurried automatic manner. Rushing leads to inadequate allocation of attention to the current carrying out task and eventually to errors		Page 119 par 5- page 120	

α/α	EVENT	ACTION		Reference in report	Comments
		4. First Officer (K2) training records. Difficulties in following SOP's, mistakes omissions ,tendency to overreact and lose confidence in non normal situations			
507	Before Taxi Procedure	1. FCOM , pilots verify that all system annunciator lights illuminate and the extinguish –recall check 2. By design, no clues were provided by this action that pressurization selector was on MAN position.		Page 120 par3	
508	TAKE OFF	PRRESSURIZATION SELECTOR IN MANUAL POSITION GREEN INDICATION 'MANUAL' STILL LID		Page 119	Airborne with manual pressurization.
509	After Takeoff checklist	First item to check is the pressurization system and verify its settings Failure to rectify selectors position.		Page 120 par 5	Second missed opportunity to correct an earlier error
510	After Takeoff checklist executed under time/workload pressure	Performed under pressure. Pilots attentions is consumed by other **concurrent tasks**.(retracting labdibg gear and flaps,monitoring the climb communicating with		Page 120 par 5	First Officer Training records into account.

α/α	EVENT	ACTION		Reference in report	Comments
		ATC)			
	Ascent (Climb)				
511	Cabin Altitude Warning Horn	Misinterpreted as Takeoff configuration warning.		Page 121 par1,2	Both warnings have the same sound. **But** Cabin Altitude Warning sounds while in air whereas Takeoff configuration warning sounds on the ground (during taxiing.
512	Horn misinterpretation as Takeoff Configuration warning	Disengagement of autopilot and auto throttle, reduce throttle. Contacts company and reports Takeoff Configuration warning (not recorded).		Page 121 par4	Takeoff Configuration warning sounds when a takeoff attempt takes place without having the plane configured properly (set trim, flaps, speed brake). Also when the captain manners the throttles in a certain manner in order to verify that the horn is operating.

α/α	EVENT	ACTION		Reference in report	Comments
					Similar confusion events are reported worldwide
513	Human Factors III	Declarative memory and muscle memory associates this warning horn with the throttles and thus with takeoff. Pilots may never face cabin pressurization problem with the specific warning sound during their career. Stress caused by a loud alarming and distracting sound combined with the element of surprise lead to automatic reactions relative to experience and frequency of encounter. Use of a non-native language although effective in carrying out normal circumstances duties may not be adequate or effective in cases of abnormal circumstances.		Page 121 par4 Page 122 par1	Declarative memory is the type of memory that stores events and facts Muscle memory is the skeletal muscle activity that becomes automatic with practice. Captain is German First Officer is Cypriot.
514	MASTER CAUTION light activated with the accompanying OVERHEAD indication	1. Not Canceled for 53 second 2. Due to : • Flow detectors of the equipment cooling system		Page 122 par4	

α/α	EVENT	ACTION		Reference in report	Comments
		reacted to low air density and illuminated the indication OFF of the Equipment Cooling section on the overhead panel.(Reported to the Ground Engineer) • Oxygen mask deployment in passenger cabin illuminating the PASS OXY on the aft overhead panel.(This event could not trigger MASTER CAUTION since it was already on, from previous event. Thus crew wasn't aware of this second event. Had no indication of looking into this second event e.g an overhead warning to look on the aft overhead panel since PASS OXY ON was lid. 3. Captain contacts company's ground operations			
515	Captain vs Ground Operations	1. Captain reports Takeoff Configuration Warning and Equipment Cooling Lights. 2. Dispatcher suggest and puts		Page 123	

α/α	EVENT	ACTION		Reference in report	Comments
		on microphone the on duty ground engineer (who also performed the maintenance before takeoff) without informing him that Takeoff Configuration Warning was reported 3. Captain reports to the engineer that both cooling equipment lights were off 4. Engineer wasn't aware that the light indications are labeled off thus unable to understand immediately the situation. 5. Captain asks for the location of the cooling equipment circuit breakers 6. Ground engineer asks confirmation that pressurization mode selector was set to AUTO. 7. Language difficulties prolonged resolution of problem while aircraft was climbing. 8. Initial effects of hypoxia,			

α/α	EVENT	ACTION		Reference in report	Comments
516	Cabin Altitude rising	1. Pilot's failure to notice cabin altitude rising due to low pressurization. Together with aircraft climbing limited differential pressure resulted 2. Hypoxia is favorable under these conditions		Page 123 par 3,4	
517	HUMAN FACTORS IV	High workload in the cockpit, facing an unpleasant and distracting warning sound. Realization of failure to provide a remedy for the situation. Since actions taken, were of no result. Diversion of attention to initial Master Caution indication. Crew preoccupation with one task i.e trying to fix the Equipment Cooling problem since they believed that was the situation to be solved. Instead of troubleshooting the source of the warning horn and ignoring or failure to note vital indication such as PASS OXY ON. First Officer's records show sub-optimal performance in non normal situations. Failure to note gradual hypoxias''		Page 124	Ground Engineer reported that Captain asked for the location of Equipment Cooling circuit breakers.

α/α	EVENT	ACTION		Reference in report	Comments
		symptoms that affected pilots' decision making. Hypoxia and distractions increases stress levels. Stress is known to affect humans' memory, attention, decision making, risk management and communication skills favoring errors.			
518	Pilots' Incapacitation.	Due to hypoxia. Cabin environment exceeded a cabin altitude of 10 000ft and progressive loss of pressure during climb to 34 000ft. Insufficient oxygen due to inadequate pressurization led to crew's loss of consciousness.		Page 125	
519	Cruise /F-16 observations	Leveling off at FL340 Flying according to Flight Management System (FMS) programmed route		Page 126	
520	Descent	KEA holding patter at FL340 Flight Attendant assumes the seat of the captain trying to assume control of the aircraft. Given hypoxia that was prevailing in the cabin environment and stresses he		Page 126	

α/α	EVENT	ACTION		Reference in report	Comments
		was unable to gain control although a incensed pilot. Fuel starvation at 08:49:50 h for the left engine and 08:59:47 h for the right engine.			
521	Crash	Site: Grammatikos Hill 09:03:32h An attempt was made by the person at the control to minimize impact. Fire outburst.			

LEVEL 6
EQUIPMENT AND SURROUNDING
ACCIMAP
Coding:600

α/α	EVENT	Description		Reference in report	Comments
601	Green Indication is lid.	Green indication MAN is lid on the overhead digital pressure control panel (601)		Page 117 par.4	
602	Pressurization Control Panel situated in First Officer's overhead panel.	Air conditioning and pressurization: First Officer's responsibility while aircraft was on the ground Pilot Monitoring while the aircraft was in the air.		Page 81 Par 1.17.2.2.1	
603	Bright vs Dim light settings	In Dim mode the green indication MANUAL was not particularly obvious. In Bright mode was clearly visible		Page 118	
604	Overhead Panel Design	Not safeguarding against inadvertent omissions Green doesn't imply an abnormality, whereas amber (orange) implies caution and red implies warning.			
605	Warning Horn Design	Same sound for 2 events Takeoff Configuration Warning			

α/α	EVENT	Description		Reference in report	Comments
		Cabin Altitude Warning			
606	Master Caution/Overhead indication Design	Had no holding events capability If an event activates Master Caution/ Overhead indication and another event occurs afterwards that would normally activate Master Caution/Overhead indication, before it is cancelled, the second event would be invisible to the pilots through the Master Caution warning		Page 122 par4	Master Caution was not cancelled for 53 s
607	OFF light indication of Equipment Cooling	Lid indication of OFF labels. Lingual difficulties especially when communicating in foreign tongue. Captain stated that both the Equipment Cooling lights were off He meant Equipment Cooling fan OFF indications were illuminated		Page par1	Prolonged dialogue, loss of valuable time in presence of initial hypoxia effects on pilots.
608	F-16 interception	No structural damage on aircraft Oxygen masks were deployed in passengers cabin. Some passengers were wearing the masks and all of them were seated.			

APPENDIX C

In this appendix, the ‘Big Picture’ diagram is printed which maps the events and actions from the official accident report [1].

SYSTEM: “Helios Airways Flight HCY 522”
EVENT: Crashed

System Level

1) Government Policy and legislation

- Ministry of Communications and Works (Cyprus)
  Civil Aviation Law N.213 (I) 2002,

2) Regulatory bodies and Associations

- Cyprus DCA (201)
- UK CAA Audits/ Inspections-Helios (202,204)
  - Quality system
  - Monitoring pilot certificates, medicals and training.
  - Senior managers and pilots with managerial positions were not logging sufficient office time
  - Training Manager vacant post
  - Violation of crew resting times
  - Crew records lack certificate of competence in case of pilot incapacitiaion
  - Impractical scheduling
- UK CAA Audits/ Inspections-ATC Lasham (203)
  - Level 1 findings
    - The operator had not submitted completed maintenance documents to ATC Lasham
    - Incomplete records of the maintenance tasks
    - Inadequate definition of who was responsible for the completion of the Maintenance Card Summary Pages.
- Cyprus DCA audit to Helios (303)
  - Level 2 findings

3) Local area Government. Company management: Planning and Budgeting

- Some Operators’ managers did not match job criteria for their respective positions (311)
- Security Manager position vacant (301)
- Flight Operations’ Manager assumes double position as Training Manager (301)
- General view of managers of a healthy organization (302,304,306-310)
- Deficiencies in Training Manager Standards position (312)
- Satisfactory line check on Captain with emphasis on CRM (305)
- Weekly safety meetings stopped. Replaced with meetings when situation arose. (302)
- Culture to stretch the rules to the limits, aircraft utilization was extremely high with inadequate downtime (303)
- Operators’ staffing.(313)
- Operators’ Safety Culture (315)
- Operators’ Quality Assurance (316)
- Instead of Safety Management System , Flight Safety Program was followed (307)

4)Technical and Operational Management

- Continuous leakage of the aircraft (409)
- Engineer 1 (405)
- Vague Instruction for pressure leak test in AAM (401)
- Audits’ Level 1 findings reported as Level 2 (408)
- Maintenance in Larnaca (404)
- Helios failure to provide maintenance documentation to ATC Lasham
- Firsts’ Officers training record (402)
- Former Operator’s Technical Manager statement (406)
- Repeated/unsolved problems with equiptment cooling system (411)
- Crew Scheduling (412)
- Cabin Crew (403)
- Flight Crew Training (413)
- Actions after oxygen masks activation in case of not level off or descent (414)
- Accessing Cockpit upon emergency (415)

5) Physical processes and Actor activities

- Pressurization Mode Selector is left to MAN (manual) position (501-502)
- Human Factors I (504)
- Preflight Duties (503)
- Checklist Design/ Human Factors II (506)
- Preflight Checklist (505)
- Before Taxi Procedure (507)
- TAKE OFF (508)
- After Takeoff Checklist (509)
- Executed under time/workload pressure (510)
- Misinterpretation of Cabin Altitude Warning horn as Takeoff Configuration Warning (511,512)
- Human Factors III (513)
- Master Caution Activated with the accompanied Overhead indication (514)
- Human Factors IV (517)
- Captain vs Ground Operations (515)
- Cabin Altitude rising (516)
- Pilots’ Incapaciation (518)
- Descent (520)
- CRASH 121 fatalities (521)

6)Equipment and surroundings

- Green indication MAN is lid on the overhead digital pressure control panel (601)
- Pressurization Control Panel is situated in First Officer’s overhead panel (602)
- Bright vs Dim illumination setting (603)
- Overhead Panel Design (604)
- Warning Horn Design and Warning horn alarming. (605)
- Master Caution/Overhead indication Design (606)
- OFF label (607)
- Hypoxic environment builds up gradually