Implementing Systems Theory in Accident Investigation using the MIT STAMP based approach Causal Analysis using Systems Theory (CAST)
Established September 2018

Chief Inspector appointed by the Chief Executive with a mandate to investigate air accidents and incidents as per ICAO Annex 13 and CAP 448B

AAIA is implementing Systems Theory in Accident Investigation using the MIT STAMP based approach Causal Analysis using Systems Theory (CAST) as the primary analysis tool for accident/incident investigation.
Annex 13 to the Convention on International Civil Aviation.2 Annex 13 defines an investigation (Chapter 1) as:

A process conducted for the purpose of accident prevention which includes the gathering and analysis of information, the drawing of conclusions, including the determination of causes and, when appropriate, the making of safety recommendations.
Understanding Accident Analysis

### Abstract

The quality of a safety investigation’s analysis activities plays a critical role in determining whether the investigation is successful in enhancing safety. However, safety investigations require analysis of complex sets of data and situations where the available data can be vague, incomplete and misleading. Despite its importance, complexity, and reliance on investigators’ judgements, analysis has been a neglected area in terms of standards, guidance and training of investigators in most organisations that conduct safety investigations.

To address this situation, the Australian Transport Safety Bureau (ATSB) developed a comprehensive investigation analysis framework. The present report provides an overview of the ATSB investigation analysis framework and concepts such as the determination of contribution and standard of proof. The report concludes by examining the nature of concerns that have been raised regarding the ATSB analysis framework and the ATSB’s consideration of these concerns.

The ATSB believes that its investigation analysis framework is well suited to its role as an independent, no-blame safety investigation body. It is hoped and expected that ongoing development and provision of information about the framework can help the safety investigation field as a whole consider some important issues and help develop the best means of conducting safety investigations to enhance future safety.

### Uncertainty, probability and likelihood

Probability and likelihood Uncertainty is a key component of inductive arguments and reasoning in many fields, and it can be characterised in several ways. In the ATSB analysis guidelines, uncertainty is primarily discussed as the degree of probability that a particular statement is true, based on the available evidence.

### Arguments, premises and findings

A safety investigation produces a series of findings or conclusions. To develop these findings, the investigation team needs to produce arguments. Arguments consist of a set of statements, one of which is the finding and the rest are premises.

Premises provide the reasons, grounds or justification for believing the finding, whereas the finding is the result of the argument. The premises may consist of items of evidence, as well as assumptions. Findings can also be termed ‘claims’ or ‘hypotheses’, although such terms are more useful when discussing proposed findings rather than verified findings.
1. Factual
All information relevant to an understanding of the factual information, analysis and conclusions is included under each appropriate heading;

2. Analysis
Analyse, as appropriate, only the information documented in 1. — Factual information and which is relevant to the determination of conclusions and causes and/or contributing factors.

3. Conclusions
List the findings, causes and/or contributing factors established in the investigation. The list of causes and/or contributing factors should include both the immediate and the deeper systemic causes and/or contributing factors.

4. Safety Recommendations
As appropriate, briefly state any recommendations made for the purpose of accident prevention and identify safety actions already implemented.
Investigation Scope
At the aircraft departure the following conditions apply:

- Aircraft is airworthy.
- MEL [faults] and deferred items are cleared [Airworthiness]
- Crew are within flight duty limitations [Fatigue]
- Cargo is fully compliant with the international Dangerous Goods regulations [Risk]
- No security items are logged at Dubai [Access to aircraft]

<table>
<thead>
<tr>
<th>Time (UTC)</th>
<th>Phase</th>
<th>Duration (minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:53</td>
<td>Take off</td>
<td>49</td>
</tr>
<tr>
<td>15:42</td>
<td>UCFIT</td>
<td></td>
</tr>
</tbody>
</table>
The problem of ‘Root Cause”

1) According to the International Civil Aviation Organisation (ICAO) ADREP classification, this is categorised as a loss of control accident (LOC-I).

2) Following a linear direct causal analysis, this is a Loss of control due to damage to the flight control mechanisms.

3) If you look for a direct root cause it’s the initiating action: ‘spontaneous combustion of hazardous materials, resulting in an unconfined class D metal fire, rapidly escalating into an uncontrolled on-board fire’

4) If you look at cause and effect at a physical level it’s the failure of the separation barrier, the thin (2mm) polyglass cargo liner, under extreme thermal loading resulting in the material’s failure to maintain its integrity.

5) If you look at it organizationally, it’s a failure to recognise a documented and specific operational risk where the outcome is always catastrophic.

6) If looked at from a regulatory and oversight perspective it is a lack of oversight and a Safety Management System (SMS) which is not responding to operational risk analysis.

7) From a Pilot’s or crew perspective this is problem centered around decision making, it’s a deviation or non-compliance with Standard Operating Procedures (SOP’s) problem related to the QRH/Non-Normal checklist and operational non-conformance.

8) For the OEM, it’s a design flaw involving a Single point of Failure.
Duration of the Investigation: Sept 2010 – May 2013: 36 months

Safety Recommendations: Thirty Six [36]

Eight safety recommendations were excluded based on the inclusion criteria:

- ICAO procedures
- Operator's risk analysis
- SMS processes
- IATA dangerous goods standards
- Specific design requirements for cargo aircraft.

SR's focused on Technical/Design/Regulatory/Standards Approvals/Cargo/Operations/Ignition sources for lithium battery fires
CAST REVIEWED SAFETY RECOMMENDATIONS

Safety Recommendations: Forty Six [46]

Inspections
- NVGR
- Training Options
- Checklists
- Crew Martin
- Full Face Oxygen Mask
- E2F Training
- Evidence Based Training

Safety Recommendations
- SCAD
- SCAD Technical Instructions
- Operator Data
- SMS
- RSK
- RSK
- Critical Systems Protection
- Single Points of Failure
- Active Fire Detection
- Fire Standards
- Certification
- LNG Design
- Screening

QCRA
ATC
ATC
Asynchronous Evolution and Emergent Risks

Safety Investigation Workshop
TRACING NEW SAFETY THINKING PRACTICES IN SAFETY INVESTIGATION REPORTS

Dr Nektarios Karanikas
Aviation Academy, Amsterdam University of Applied Sciences (NL)

Dimitrios Chionis MSc, PhD candidate
Bolton University (UK)

3rd International Cross-industry Safety Conference (ICSC)
Amsterdam, 31 October – 2 November 2018
# Analysis Tools – Model Groups

## SAFETY/ACCIDENT MODEL GROUPS

<table>
<thead>
<tr>
<th>Type</th>
<th>Brief description</th>
<th>Example model(s)</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequential</td>
<td>Direct cause-effect relationships: clearly defined timeline of failures, errors</td>
<td>Domino</td>
<td>SEQ</td>
</tr>
<tr>
<td></td>
<td>and violations that lead to an event.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Epidemiological</td>
<td>Direct and indirect cause-effect relationships: clearly defined timeline of active</td>
<td>Swiss cheese</td>
<td>EPD</td>
</tr>
<tr>
<td></td>
<td>failures along with long-lasting effects of latent problems that contribute to</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>active failures.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systemic</td>
<td>Dynamic, emerging and complex system behaviours: examining interactions,</td>
<td>STAMP AcciMap</td>
<td>SYS</td>
</tr>
<tr>
<td></td>
<td>interdependencies and relationships between parts to understand a system as a</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>whole, including effects of the behaviour of individual elements.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Using System Theory to Understand Accident Causality

- Systems Theory considers accidents as arising from the interactions among systems components and usually does not specify single causal variables or factors.
- Traditional safety models and event chain models focus on unsafe acts or conditions.
- System safety models examine what went wrong with the systems operations or organisation to allow the event to occur.
- Systems approach treats safety and an emergency property, the product of complex interactions of components of the systems.
- Emergent properties – e.g. safety – are controlled or enforced by constraints (control laws) related to the behaviour of the system components.

Safety = Control Problem

Safety Constraints
Three Basic Constructs Underlie STAMP

A focus on preventing failures to the broader goal of designing and implementing controls that will enforce the necessary constraints.

The STAMP (System-Theoretic Accident Model and Processes) accident model is based on these principles. Three basic constructs underlie STAMP: safety constraints, hierarchical safety control structures, and process models.

4.1 Safety Constraints

Safety Constraints

Hierarchical Control Structures

Process Models
In STAMP, accidents are conceived as resulting not from component failures, but from inadequate control or enforcement of safety-related constraints on the development, design, and operation of the system. The most basic concept in STAMP is not an event, but a constraint.
CAST Process

1. Identify the System Level Hazards involved in the loss

2. Identify the Control Structure designed to control the Hazard

3. Determine the Proximate Events leading to the loss

4. Analyze the loss at the Physical System Level
   - Identify the physical controls and equipment involved
   - Identify any physical safety requirements and constraints meant to prevent the accident
   - Identify any failures or inadequate controls in the physical equipment
   - Identify contextual factors that explain the physical failures or inadequate controls

5. Analyze higher levels of control to determine how and why each successive higher level contributed to inadequate control at the current level
   - Identify the unsafe decisions and control actions
   - Identify process model flaws that explain the unsafe decisions and control actions
   - Identify contextual factors that explain why the behaviour seemed appropriate at the time
   - Identify the safety-related responsibilities for the next higher level of control

6. Look at factors that involve the interaction among system components and not just individual components.
   - Identify communication and coordination deficiencies that contributed to the events
   - Identify dynamics and changes over time that led to the behaviors and events
   - Identify safety culture flaws contributing to the events
STAMP/CAST Software

- Enables the investigator to concentrate on investigation analysis
  - As automated as possible.
  - Analysts only need to focus on thinking.
  - CS diagrams from the Component extraction table is automatically generated.
  - Guided chart editing with intuitive operation is available.

- Help analysis. It's not just an editing tool.
  - Automatic ID numbering (proactive support for repetitive analysis)
  - Real-time Model collaboration
  - Highlights of related information, parallel display

- Guide the analysis procedure, but does not limit operational scope
  - Step guidance window for beginner
  - Available from any step for experts
  - It can be used as a construction tool of CS Diagram.
  - Two-way support of Diagram Table, and Table Diagram
CAST Software

System Control Loop

System Control Loop