A STAMP-based Hazard Log for Use during Development and Operations

Andrea Scarinci

Alessandro Giusti

scarinci@mit.edu

alessandro.giusti@alitalia.com
THE PROBLEM

Review of policies for operations in areas potentially contaminated by VOLCANIC ASHES

MAIN HAZARDS:
• Loss of thrust;
• Obstruction of Pitot static ports;
• Partial/Total loss of hydraulic system;
• Short circuits in the electrical system;
• Degradation of avionic cooling;
• Cabin air contamination;
• Braking action degradation.

RISK CONTROL: AVOID & MONITOR
CURRENT SOLUTIONS

Risk Identification through:

• **Brainstorming** conducted by group of experts (Flight Ops, Maintenance, Ground Ops);

  **SUBJECTIVITY**

• **ARMS** (Aviation Risk Management Solutions) semi-structured method based on “barriers to accident” identification and likelihood estimation;

  **DIFFICULT TO ESTIMATE PROBABILITIES**
HAZARD LOG

1. Risk identification
   - Brainstorming, FMEA ...

2. Risk Management/Mitigation
   - Probabilistic Risk Assessment
NEW STAMP-based HAZARD LOG

1. Risk identification

2. Risk Management/Mitigation

- STPA
- Assumptions Identification and Leading Indicators
### Risk identification

<table>
<thead>
<tr>
<th>High level Hazard</th>
<th>Severity</th>
<th>Control Action</th>
<th>Unsafe Control Actions</th>
<th>Causal Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuel exhaust in flight</td>
<td>A or High</td>
<td>Define fuel plan</td>
<td>UCA1, UCA2</td>
<td>SC1, SC2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refuelling</td>
<td>UCA3, UCA4</td>
<td>SC3, SC4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
NEW STAMP-based HAZARD LOG

Risk Management/Mitigation

Assumptions Identification and Leading Indicators

Leading Indicators

Identify key parameters to monitor the safety of operations

“Accident precursors”

Chemical, Health, Naval, Nuclear Industries
**NEW STAMP-based HAZARD LOG**

**Assumptions**

Control/Mitigation action → Assumptions on how the system will operate

- Pilot Orders De-Icing Fluid Application on Contaminated Surfaces
- Pilot will Take Off within the prescribed Holdover Time

**VIOLATION OF ASSUMPTIONS IS OFTEN THE CAUSE OF ACCIDENTS**
NEW STAMP-based HAZARD LOG

Assumptions  ➔  Leading Indicators

Leveson, 2015

A Systems Approach to Risk Management Through Leading Safety Indicators
NEW STAMP-based HAZARD LOG

**Assumptions**

- Pilot will Take Off within the prescribed Holdover Time
- Cockpit window will not crack during approach due to bird strike, because the approach speed is always below a certain threshold

**Leading Indicators**

- Monitor elapsed time between termination of De-Icing procedure and T/O clearance
- Monitor approach speed below specified altitude.
# NEW STAMP-based HAZARD LOG

## Risk Management/Mitigation

<table>
<thead>
<tr>
<th>Causal Scenarios</th>
<th>Mitigation Action</th>
<th>Assumption</th>
<th>Monitoring Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Leading Indicator</td>
</tr>
<tr>
<td>SC1</td>
<td>M1</td>
<td>A1</td>
<td>L1</td>
</tr>
<tr>
<td>SC2</td>
<td>M2</td>
<td>A2</td>
<td>L2</td>
</tr>
<tr>
<td>SC3</td>
<td>M3</td>
<td>A3</td>
<td>L3</td>
</tr>
<tr>
<td>SC4</td>
<td>M4</td>
<td>A4</td>
<td>L4</td>
</tr>
</tbody>
</table>

**SMI Device**

[Massachusetts Institute of Technology](https://www.mit.edu)
NEW STAMP-based HAZARD LOG

Decision Making

<table>
<thead>
<tr>
<th>Mitigation action</th>
<th>Leading Indicator monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Feasibility</strong></td>
<td><strong>Cost</strong></td>
</tr>
<tr>
<td>Yes/No</td>
<td>$$$</td>
</tr>
<tr>
<td>Yes/No</td>
<td>$$</td>
</tr>
<tr>
<td>Yes/No</td>
<td>$$$</td>
</tr>
<tr>
<td>Yes/No</td>
<td>$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feasibility</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes/No</td>
<td>$$$</td>
</tr>
<tr>
<td>Yes/No</td>
<td>$</td>
</tr>
<tr>
<td>Yes/No</td>
<td>$$$</td>
</tr>
<tr>
<td>Yes/No</td>
<td>$</td>
</tr>
</tbody>
</table>

**WORK IN PROGRESS**
In which contexts do we think the use of this Hazard Log could be particularly beneficial?
NEW STAMP-based HAZARD LOG

DATA → LEADING INDICATORS
MODEL

GET YOUR DATA HERE!
HUMAN BEHAVIOR

• Difficult to enforce constraints;
• Greatest number of assumptions (procedures, training...);
• Difficult to assign probabilities.

NEW STAMP-based HAZARD LOG

LEADING INDICATORS ASSUMPTIONS
Future work:

- APPLICATION: apply to more and different systems;
- THEORY: extend Hazard log with DECISION MAKING section;
- THEORY: refine/review terminology based on experience acquired from applications.
# VOLCANIC ASHES

**A1:** Loss of A/C;  
**A2:** Injury of passenger and crew;  
**H1:** Flight in airspace contaminated by VA  
**H2:** A/C not compliant with airworthiness requirements

<table>
<thead>
<tr>
<th>High level Hazard</th>
<th>Severity</th>
<th>Control Action</th>
<th>Unsafe Control Actions</th>
<th>Causal Scenarios</th>
</tr>
</thead>
</table>
| H1                | High     | Route 60 NM off the erupting volcano | **Provided** when the wind is pushing the VA cloud toward the area where the A/C is supposed to fly. | CS1.1) The maps on which the rerouting is based are wrong;  
CS1.2) The wind changed from the moment in which the rerouting was issued;  
CS1.3) Assumptions on wind speed vs. aircraft speed are wrong. |
# VOLCANIC ASHES

**A1:** Loss of A/C;  
**A2:** Injury of passenger and crew;  
**H1:** Flight in airspace contaminated by VA  
**H2:** A/C not compliant with airworthiness requirements

<table>
<thead>
<tr>
<th>Mitigation Action</th>
<th>Assumption</th>
<th>Monitoring Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA1.3)</td>
<td>AS1.3)</td>
<td>LI1.3)</td>
</tr>
<tr>
<td>Make sure to</td>
<td>Established</td>
<td>Report</td>
</tr>
<tr>
<td>include time</td>
<td>time and</td>
<td>log</td>
</tr>
<tr>
<td>margin (XXm) and</td>
<td>distance</td>
<td>MO1.3)</td>
</tr>
<tr>
<td>distance margin</td>
<td>margin are</td>
<td>FR1.3)</td>
</tr>
<tr>
<td>(+XX NM) when</td>
<td>adequate.</td>
<td>Every</td>
</tr>
<tr>
<td>uncertain about</td>
<td></td>
<td>flight in VA</td>
</tr>
<tr>
<td>VA speed and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>direction.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

H1: Flight in airspace contaminated by VA  
H2: A/C not compliant with airworthiness requirements

MA1.3) Make sure to include time margin (XXm) and distance margin (+XX NM) when uncertain about VA speed and direction.  
AS1.3) Established time and distance margin are adequate.  
LI1.3) Nbr of times in which an A/C found itself close to a VA cloud because time/space calculations were not conservative enough.  
MO1.3) Report log  
FR1.3) Every flight in VA

**A1:** Loss of A/C;  
**A2:** Injury of passenger and crew;  
**H1:** Flight in airspace contaminated by VA  
**H2:** A/C not compliant with airworthiness requirements

<table>
<thead>
<tr>
<th>Mitigation Action</th>
<th>Assumption</th>
<th>Monitoring Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA1.3)</td>
<td>AS1.3)</td>
<td>LI1.3)</td>
</tr>
<tr>
<td>Make sure to</td>
<td>Established</td>
<td>Report</td>
</tr>
<tr>
<td>include time</td>
<td>time and</td>
<td>log</td>
</tr>
<tr>
<td>margin (XXm) and</td>
<td>distance</td>
<td>MO1.3)</td>
</tr>
<tr>
<td>distance margin</td>
<td>margin are</td>
<td>FR1.3)</td>
</tr>
<tr>
<td>(+XX NM) when</td>
<td>adequate.</td>
<td>Every</td>
</tr>
<tr>
<td>uncertain about</td>
<td></td>
<td>flight in VA</td>
</tr>
<tr>
<td>VA speed and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>direction.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

H1: Flight in airspace contaminated by VA  
H2: A/C not compliant with airworthiness requirements

MA1.3) Make sure to include time margin (XXm) and distance margin (+XX NM) when uncertain about VA speed and direction.  
AS1.3) Established time and distance margin are adequate.  
LI1.3) Nbr of times in which an A/C found itself close to a VA cloud because time/space calculations were not conservative enough.  
MO1.3) Report log  
FR1.3) Every flight in VA

**A1:** Loss of A/C;  
**A2:** Injury of passenger and crew;  
**H1:** Flight in airspace contaminated by VA  
**H2:** A/C not compliant with airworthiness requirements

<table>
<thead>
<tr>
<th>Mitigation Action</th>
<th>Assumption</th>
<th>Monitoring Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA1.3)</td>
<td>AS1.3)</td>
<td>LI1.3)</td>
</tr>
<tr>
<td>Make sure to</td>
<td>Established</td>
<td>Report</td>
</tr>
<tr>
<td>include time</td>
<td>time and</td>
<td>log</td>
</tr>
<tr>
<td>margin (XXm) and</td>
<td>distance</td>
<td>MO1.3)</td>
</tr>
<tr>
<td>distance margin</td>
<td>margin are</td>
<td>FR1.3)</td>
</tr>
<tr>
<td>(+XX NM) when</td>
<td>adequate.</td>
<td>Every</td>
</tr>
<tr>
<td>uncertain about</td>
<td></td>
<td>flight in VA</td>
</tr>
<tr>
<td>VA speed and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>direction.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

H1: Flight in airspace contaminated by VA  
H2: A/C not compliant with airworthiness requirements

MA1.3) Make sure to include time margin (XXm) and distance margin (+XX NM) when uncertain about VA speed and direction.  
AS1.3) Established time and distance margin are adequate.  
LI1.3) Nbr of times in which an A/C found itself close to a VA cloud because time/space calculations were not conservative enough.  
MO1.3) Report log  
FR1.3) Every flight in VA

**A1:** Loss of A/C;  
**A2:** Injury of passenger and crew;  
**H1:** Flight in airspace contaminated by VA  
**H2:** A/C not compliant with airworthiness requirements

<table>
<thead>
<tr>
<th>Mitigation Action</th>
<th>Assumption</th>
<th>Monitoring Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA1.3)</td>
<td>AS1.3)</td>
<td>LI1.3)</td>
</tr>
<tr>
<td>Make sure to</td>
<td>Established</td>
<td>Report</td>
</tr>
<tr>
<td>include time</td>
<td>time and</td>
<td>log</td>
</tr>
<tr>
<td>margin (XXm) and</td>
<td>distance</td>
<td>MO1.3)</td>
</tr>
<tr>
<td>distance margin</td>
<td>margin are</td>
<td>FR1.3)</td>
</tr>
<tr>
<td>(+XX NM) when</td>
<td>adequate.</td>
<td>Every</td>
</tr>
<tr>
<td>uncertain about</td>
<td></td>
<td>flight in VA</td>
</tr>
<tr>
<td>VA speed and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>direction.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

H1: Flight in airspace contaminated by VA  
H2: A/C not compliant with airworthiness requirements

MA1.3) Make sure to include time margin (XXm) and distance margin (+XX NM) when uncertain about VA speed and direction.  
AS1.3) Established time and distance margin are adequate.  
LI1.3) Nbr of times in which an A/C found itself close to a VA cloud because time/space calculations were not conservative enough.  
MO1.3) Report log  
FR1.3) Every flight in VA

**A1:** Loss of A/C;  
**A2:** Injury of passenger and crew;  
**H1:** Flight in airspace contaminated by VA  
**H2:** A/C not compliant with airworthiness requirements

<table>
<thead>
<tr>
<th>Mitigation Action</th>
<th>Assumption</th>
<th>Monitoring Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA1.3)</td>
<td>AS1.3)</td>
<td>LI1.3)</td>
</tr>
<tr>
<td>Make sure to</td>
<td>Established</td>
<td>Report</td>
</tr>
<tr>
<td>include time</td>
<td>time and</td>
<td>log</td>
</tr>
<tr>
<td>margin (XXm) and</td>
<td>distance</td>
<td>MO1.3)</td>
</tr>
<tr>
<td>distance margin</td>
<td>margin are</td>
<td>FR1.3)</td>
</tr>
<tr>
<td>(+XX NM) when</td>
<td>adequate.</td>
<td>Every</td>
</tr>
<tr>
<td>uncertain about</td>
<td></td>
<td>flight in VA</td>
</tr>
<tr>
<td>VA speed and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>direction.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

H1: Flight in airspace contaminated by VA  
H2: A/C not compliant with airworthiness requirements

MA1.3) Make sure to include time margin (XXm) and distance margin (+XX NM) when uncertain about VA speed and direction.  
AS1.3) Established time and distance margin are adequate.  
LI1.3) Nbr of times in which an A/C found itself close to a VA cloud because time/space calculations were not conservative enough.  
MO1.3) Report log  
FR1.3) Every flight in VA
<table>
<thead>
<tr>
<th>HAZARD</th>
<th>SEVERITY</th>
<th>CONTROL ACTIONS ASSOCIATED</th>
<th>RISK INDETIFICATION</th>
<th>RISKS SCENARIOS ASSOCIATED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuel exhaust in flight</td>
<td>A</td>
<td>Mechanic Conducts underwater fuel quantity inspections</td>
<td>From Mechanic to Fuel Tanks</td>
<td>Unsafe Control action: 1) when impossible to obtain correct results, 2) when fuel indicators in the cockpit show higher than real fuel qty values, 3) too late, too early, no order</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dispatcher Estimates fuel quantity for flight</td>
<td>From Dispatcher to Pilot</td>
<td>Unsafe Control action: 1) when not aware of weather, traffic contingencies which will require more fuel, 2) when not aware of real fuel consumption of aircraft;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pilot Reviews and communicates fuel quantity</td>
<td>From Pilot to Fuel Ramp agent</td>
<td>Unsafe Control action: 1) when updates have been made to the dispatcher plan due to changes in weather/traffic contingencies; 2) when not aware of weather, traffic contingencies which will require more fuel, 2) when not aware of real fuel consumption of aircraft;</td>
</tr>
</tbody>
</table>
### RISK MANAGEMENT

<table>
<thead>
<tr>
<th>Mitigation Action</th>
<th>Assumption</th>
<th>Monitoring on effectiveness of mitigation action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Leading indicator</td>
</tr>
<tr>
<td>MA1.1) Testing instruments before each check</td>
<td>AS1.1) Test will not be bypassed by operator</td>
<td>L1.1) Nbr of faulty instruments reported during test</td>
</tr>
<tr>
<td>MA2.1) Put visible coloured/ clear labels on instruments to distinguish each A/C</td>
<td>AS2.1) Label will be effective</td>
<td>L2.1) (maybe?) Nbr of broken instruments because used on wrong A/C</td>
</tr>
<tr>
<td>MA1.1) Put in a place a system for pilots to detect and report doubts on correct calibration of fuel gauges; MA2.1) Make sure critical discrepancy level is well stated in manuals and considers worst case scenarios (i.e. routes with tightest reserve margin)</td>
<td>AS1.1) Pilots know how to detect dubious fuel quantity indications and reporting is simple</td>
<td>L1.1) Nbr of suspect fuel indications reported</td>
</tr>
<tr>
<td>MA1.1) Plan some non-routine underwing inspections</td>
<td>AS2.1) Manual based training will be effective</td>
<td>L2.1) Nbr of times critical discrepancy level has been reported by pilots and no action taken</td>
</tr>
<tr>
<td>MA2.1) Set compulsory inspections after specific flight cycle conditions are reported by the pilots</td>
<td>AS1.1) Non-routine inspections will be carried out seriously without being biased by the fact it is a precautionary measure AS2.1) It will be easy for the pilots to identify the flight cycles which may have altered the fuel gauges calibration.</td>
<td>L1.1) Real number of inspections performed</td>
</tr>
<tr>
<td>MA1.1) Establish a last minute check the dispatcher has to make on weather/traffic conditions before submitting fuel plan to the pilot; MA1.2) Do not make fuel calculations too early (&gt;XX hours) before the flight; MA2.1) Highlight most common mistakes during training and build embedded checks in fuel planning software</td>
<td>AS1.1) The last minute check won’t be dismissed due to complacency or time pressure AS1.2) Fuel plans will be anticipated to prevent overload in peak hours; AS2.1) Training will be effective and sufficient and embedded checks as well</td>
<td>L1.1) Nbr of fuel plans modified before submitting to the pilots</td>
</tr>
</tbody>
</table>

**Mitigation Action:**
- MA1.1: Testing instruments before each check
- MA2.1: Put visible coloured/ clear labels on instruments to distinguish each A/C
- MA1.1: Put in a place a system for pilots to detect and report doubts on correct calibration of fuel gauges; MA2.1: Make sure critical discrepancy level is well stated in manuals and considers worst case scenarios (i.e. routes with tightest reserve margin)
- MA1.1: Plan some non-routine underwing inspections
- MA2.1: Set compulsory inspections after specific flight cycle conditions are reported by the pilots
- MA1.1: Establish a last minute check the dispatcher has to make on weather/traffic conditions before submitting fuel plan to the pilot; MA1.2: Do not make fuel calculations too early (>XX hours) before the flight; MA2.1: Highlight most common mistakes during training and build embedded checks in fuel planning software

**Assumption:**
- AS1.1: Test will not be bypassed by operator
- AS2.1: Label will be effective
- AS1.1: Pilots know how to detect dubious fuel quantity indications and reporting is simple
- AS2.1: Manual based training will be effective
- AS1.1: Non-routine inspections will be carried out seriously without being biased by the fact it is a precautionary measure AS2.1: It will be easy for the pilots to identify the flight cycles which may have altered the fuel gauges calibration.
- AS1.1: The last minute check won’t be dismissed due to complacency or time pressure AS1.2: Fuel plans will be anticipated to prevent overload in peak hours; AS2.1: Training will be effective and sufficient and embedded checks as well

**Monitoring on effectiveness of mitigation action:**
- L1.1) Nbr of faulty instruments reported during test
- L1.2) (maybe?) Nbr of broken instruments because used on wrong A/C
- L1.1) Nbr of suspect fuel indications reported
- L1.2) Nbr of times critical discrepancy level has been reported by pilots and no action taken
- L1.1) Real number of inspections performed
- L1.2) Nbr of precautionary inspections requested by the pilot after an “at risk” flight cycle
- L1.1) Nbr of fuel plans modified before submitting to the pilots
- L1.2) ? Issuing time of first draft fuel plan
- L2.1) Nbr of fuel plans modified by pilots after submission due to non contingent factors

**What to do if mitigation action reveals ineffective [hedging action]:**
- MA1.1: Understand what is the problem: test too long, equipment missing, difficult to perform.
- MA2.1: Change size/type of label
- NA
- NA
- MA1.1) Review pilot training and/or reporting system
- HA2.1) Change size/type of label
- HA1.1) Be more conservative on frequency of routine underwing inspections
- HA1.1) Review way in which critical flight cycles can be identified by pilots

**Owner:**
- L1.1) XXX
- L1.2) XXX
- L1.1) XXX
- L2.1) XXX
- L1.1) XXX
- L1.2) XXX
- L1.1) XXX
- L2.1) XXX
- L1.1) XXX
- L2.1) XXX
- HA1.1) XXX
- HA2.1) XXX
- HA1.2) XXX
- HA1.2) XXX
- HA2.1) XXX

**Frequency:**
- XXX