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

Andrea Scarinci

Alessandro Giusti

MIT AEROASTRO

ETIHAD AIRWAYS PARTNER | Alitalia SKYTEAM

scarinci@mit.edu

alessandro.giusti@alitalia.com

THE PROBLEM

*Review of policies for operations in areas potentially contamined 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**
   - *STPA*
2. **Risk Management/Mitigation**
   - *Assumptions Identification and Leading Indicators*

NEW STAMP-based HAZARD LOG

Risk identification

High level Hazard	Severity	Control Action	Unsafe Control Actions	Causal Scenarios
Fuel exhaust in flight	A or High	Define fuel plan	UCA1 UCA2	SC1 SC2
		Refuelling	UCA3 UCA4	SC3 SC4
		…	…	
		…	…	

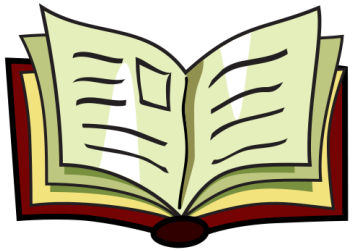
NEW STAMP-based HAZARD LOG

2

Risk Management/Mitigation

Assumptions Identification and Leading Indicators

Leading Indicators



Chemical, Health, Naval, Nuclear Industries

Identify key parameters to monitor the safety of operations

"Accident precursors"

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 Managment Through Leading Safety Indicators

NEW STAMP-based HAZARD LOG

Assumptions	→	***Leading Indicators***
Pilot will Take Off within the prescribed Holdover Time	→	Monitor elapsed time between termination of De-Icing procedure and T/O clearance
Cockpit window will not crack during approach due to bird strike, because the approach speed is always below a certain threshold	→	Monitor approach speed below specified altitude.

NEW STAMP-based HAZARD LOG

2

Risk Management/Mitigation

Causal Scenarios	Mitigation Action	Assumption	Monitoring Safety		
			Leading Indicator	Monitoring modality	Frequency
SC1	M1	A1	L1	QAR Data	Every flight
SC2	M2	A2	L2	Audits	Monthly
SC3	M3	A3	L3	Databases	Daily
SC4	M4	A4	L4	Etc.	etc.

NEW STAMP-based HAZARD LOG

3

Decision Making

DECISION MAKING			
Mitigation ac		Leading Indicator monitoring	
Feasibility	Cost	Feasibility	Cost
Yes/No	$$$		$$$
Yes/No	$$	Yes/	$$
Yes/No	$$$	Yes/No	$$$
Yes/No	$	Yes/No	$

WORK IN PROGRESS

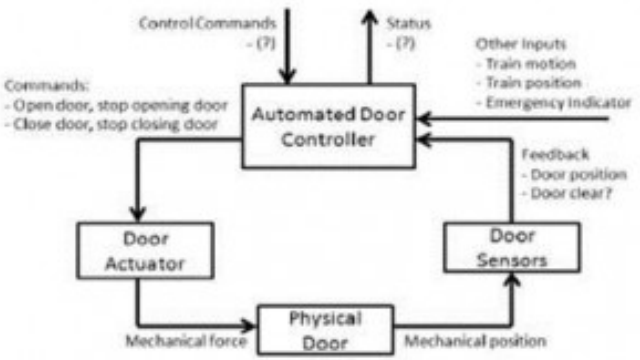
In which contexts do we think the use of this Hazard Log could be particularly beneficial?

NEW STAMP-based HAZARD LOG

DATA

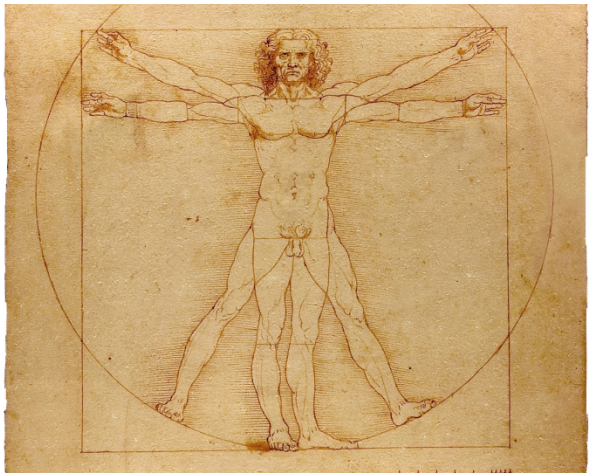
LEADING INDICATORS

MODEL



HUMAN BEHAVIOR

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

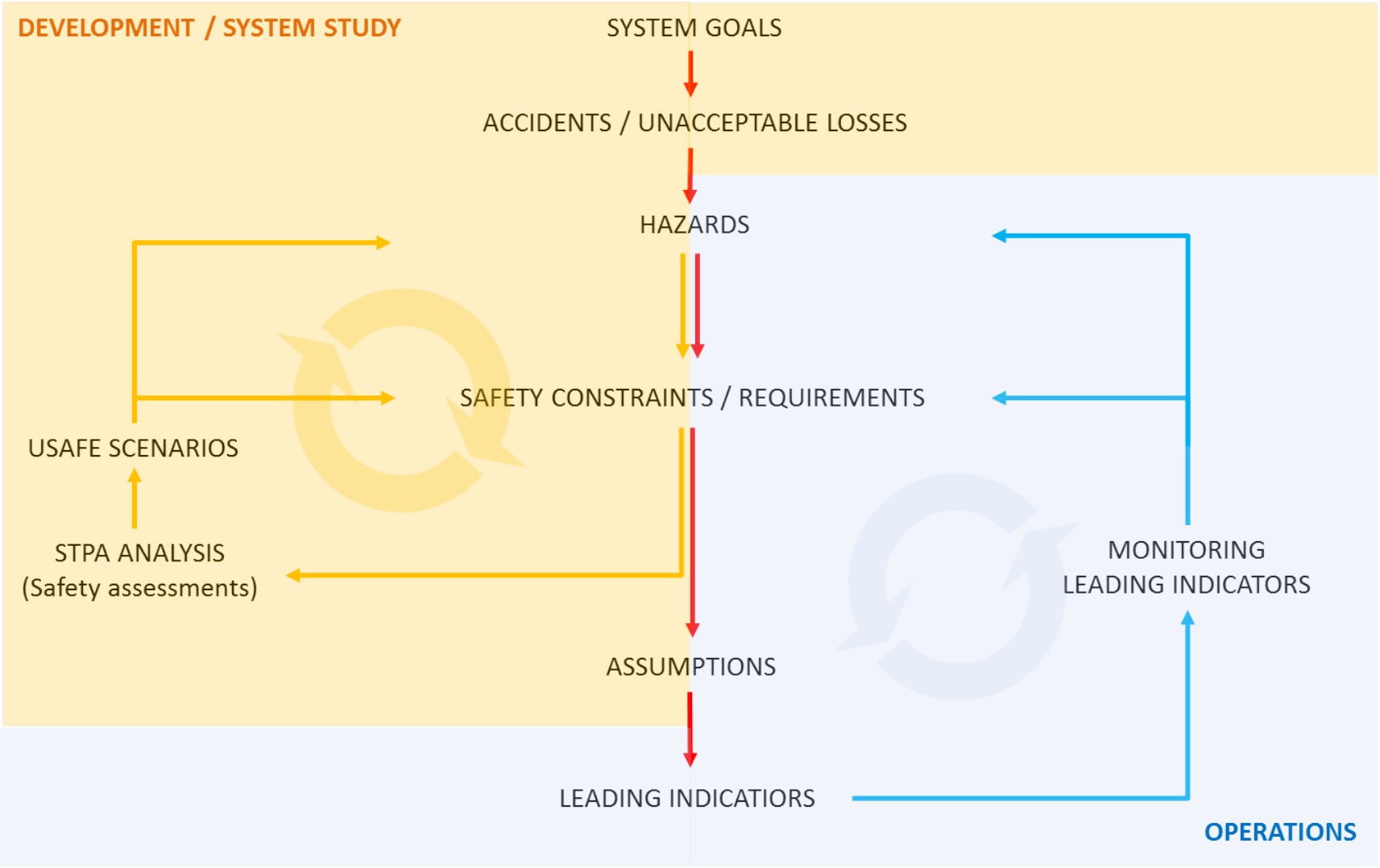


NEW STAMP-based HAZARD LOG

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.


DEVELOPMENT / SYSTEM STUDY
SYSTEM GOALS
ACCIDENTS / UNACCEPTABLE LOSSES
HAZARDS
SAFETY CONSTRAINTS / REQUIREMENTS
USAFE SCENARIOS
STPA ANALYSIS
(Safety assessments)
MONITORING
LEADING INDICATORS
ASSUMPTIONS
LEADING INDICATIORS
OPERATIONS

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

High level Hazard	Severity	Control Action	Unsafe Control Actions	Causal Scenarios
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

Mitigation Action	Assumption	Monitoring Safety		
		Leading indicator	Modality	Frequency
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

HAZARD	SEVERITY	RISK INDETIFICATION					
		CONTROL ACTIONS ASSOCIATED			RISKS SCENARIOS ASSOCIATED		
		From	Description	To		Unsafe Control action	Causal scenarios
Fuel exhaust in flight	A	Mechanic	Conducts underwing fuel quantity inspections	Fuel Tanks	CA provided	1) when impossible to obtain correct results	CS1) checks are performed with faulty instruments. CS2) checks are performed with wrong instruments for A/C type
					CA not provided	1) when fuel indicators in the cockpit show higher than real fuel qty values	CS1) checks are not performed because doubts on correct calibration of fuel gauges have not been reported by pilots or did not get to the maintenance team; CS2) checks are not performed because discrepancies reported by pilots are underestimated by maintenance team due to bad training
					CA provided too late, too early, wrong order	1) too late when incorrect calibration of the instruments is already significant	CS1) the scheduling of the maintenance activity is inadequate for that type of aircraft (maybe newly introduced) or the specific ship (ex. aged) CS2) the A/C has passed through a specific flight cycle which has altered the fuel gauges more than usual (turbulence, specific weather etc.)
					CA provided too long, too short	-	-
		Dispatcher	Estimates fuel quantity for flight	Pilot	CA provided	1) when not aware of weather, traffic contingencies which will require more fuel; 2) when not aware of real fuel consumption of aircraft ;	1.1) Weather updates are not communicated to the dispatcher fast enough or are incomplete; 2.1) Bad training (confusion on aircraft types, confusion on specific route requirements)
					CA not provided	-	-
					CA provided too late, too early, wrong order	?	-
					CA provided too long, too	-	-
		Pilot	Reviews and communicates fuel quantity	Fuel Ramp agent	CA provided	1) when not aware of weather, traffic contingencies which will require more fuel; 2) when not aware of real fuel consumption of aircraft.	1.1) Weather updates are not communicated to the pilot fast enough or are incomplete; 1.2) The pilot passively accepts dispatcher plan and does not double check on changes concerning the weather or traffic conditions; 2.1) Bad training, confusion on aircraft types,
					CA not provided	1) when updates have been made to the dispatcher plan due to changes in weather/traffic contingencies	1.1) The pilot believes that the changes have been directly communicated to the fuel ramp agent
					CA provided		

RISK MANAGMENT						
		Monitoring on effectiveness of mitigation action				
Mitigation Action	Assumption	Leading indicator	How	Owner	Frequency	What to do if mitigation action reveals ineffective [hedging action]
MA1.1) Testing instruments before each check MA2.1) Put visible coloured/clear labels on instruments to distinguish each A/C	AS1.1) Test will not be bypassed by operator AS2.1) Label will be effective	LI1.1) Nbr of faulty instruments reported during test LI2.1) (maybe?) Nbr of broken instruments because used on wrong A/C	LI1.1) Check/create log where faulty instruments are reported LI2.1) Check/create log where broken instruments are reported	LI1.1) XXX LI2.1) XXX	LI1.1) XXX LI2.1) XXX	HA1.1) Understand what is the problem: test too long, equipment missing, difficult to perform. HA2.1) Change size/type of label
MA1.1) Put in 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)	AS1.1) Pilots know how to detect dubious fuel quantity indications and reporting is simple AS2.1) Manual based training will be effetcive	LI1.1) Nbr of suspect fuel indications reported LI2.1) Nbr of times critical discrepacy level has been reported by pilots and no action taken	LI1.1) Check nbr and content of related pilot reports; LI2.1) Compare discrepancy reports and actions taken by maintenance.	LI1.1) XXX LI2.1) XXX	LI1.1) XXX LI2.1) XXX	HA1.1) Review pilot training and/or reporting system HA2.1) Change size/type of label
MA1.1) Plan some non-routine underwing inspections MA2.1) Set compulsory inspections after specific flight cycle conditions are reported by the piltos	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.	LI1.1) Real number of ispections performed LI2.1) Nbr of precuationary inspections requested by the pilot after an "at risk" flight cycle	LI1.1) Organize audits to see if inspections which are supposed to take place actually do take place; LI2.1) Record the number and monitor it's evolution (no occurences= difficult for the pilto to detect condition)	LI1.1) XXX LI2.1) XXX	LI1.1) XXX LI2.1) XXX	HA1.1) Be more conservative on frequency of routine underwing inspections HA2.1) Review way in which critical flight cycles can be identified by 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	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	LI1.1) Nbr of fuel plans modified before submitting to the pilots LI1.2) ? Issuing time of first draft fuel plan LI2.1) Nbr of fuel plans modified by pilots after submission due to non contingent factors	LI1.1) Analyze fuel plans periodically LI1.2) ? Analyze fuel plans periodically LI2.1) Analyze fuel plans periodically	LI1.1) XXX LI1.2) XXX LI2.1) XXX	LI1.1) XXX LI1.2) XXX LI2.1) XXX	HA1.1)XXXXX HA1.2)XXXXX HA2.1)XXXXX