Quantifying Risk in Commercial Aviation with Fault Trees and Event Sequence Diagrams

Robin L. Dillon-Merrill[a*], Vicki Bier[b], Sherry S. Borener[c], Mindy J. Robinson[c], Kandi K. Mitchell[d], Poornima Balakrishna[e], Amanda Hepler[f], Aleta Best[c]

[a] *presenting author*, Georgetown University, Washington, DC, United States
[b] University of Wisconsin-Madison, Madison, WI, United States
[c] Federal Aviation Administration, Washington DC, United States
[d] Crown Consulting, Inc., Arlington, VA
[e] Saab Sensis Corporation, Washington, DC
[f] Innovative Decisions Inc., Vienna, VA

Abstract: The mission of the Federal Aviation Administration (FAA) is to provide the safest and most efficient aerospace system in the world. As the FAA plans and develops the Next Generation (NextGen) Air Transportation System, quantitative risk assessments can help evaluate the impacts of new technologies and changed procedures. The FAA needs to ensure that NextGen changes that could potentially increase capacity or efficiency also maintain or improve safety. A systematic quantitative view of risk of the air transportation system provides the opportunity to fully understand how possible improvements can impact the overall safety of the system. This FAA modeling effort, led by the System Safety Management Transformation program (Sherry Borener, Program Manager), is called the Integrated Safety Assessment Model (ISAM). Within ISAM, event sequence diagrams (ESDs) describe the sequence of events that a flight must encounter for an accident scenario to occur, and a fault tree is developed for each of the pivotal events in the ESDs. The risks identified by the fault trees are linked to identifiable hazards with the goal of managing the hazards and improving system safety. This paper describes the process being used to develop the event sequence diagram-fault tree model, including lessons learned from applying probabilistic risk analysis modeling in the commercial aviation context.

Keywords: PRA, Commercial Aviation, Event Sequence Diagrams, Fault Trees.

1. INTRODUCTION

The System Safety Management Transformation program (SSMT) is an integral part of meeting FAA Aviation Safety (AVS) responsibilities for the implementation of NextGen. As the FAA plans and develops new operational improvements (OIs), quantitative risk assessments can help evaluate the impacts of these OIs, and ensure that changes maintain or improve safety while delivering capacity or efficiency benefits. For example, in an effort to reduce runway overruns caused by excessive tailwinds, one option is to switch the landing direction on runways more often to be more sensitive to shifting wind directions. While potentially decreasing one risk (i.e., runway overruns caused by excessive tailwinds), this increased switching could result in more confusion and more errors by air traffic controllers and flight crews which could thus result in more runway incursions. A systematic quantitative view of risk of the air transportation system provides the opportunity to fully understand how possible changes can impact the overall safety of the system.

[*] rld9@georgetown.edu

The overall modeling effort to create this systematic quantitative view of risk of the air transportation system is called the Integrated Safety Assessment Model (ISAM). The goal of ISAM is to produce a baseline risk for the National Aerospace System (NAS) using data collected across the NAS and through subject matter expert (SME) input. ISAM allows users to evaluate air traffic, airport and air vehicle systems and operators' individual and integrated impacts [1].

In January 2013, the SSMT program established a Fault Tree Working Group (FTWG) to develop event sequence diagrams and fault trees in support of ISAM. The FTWG began by reviewing event sequence diagrams and fault trees previously developed by the National Aerospace Laboratory of the Netherlands (NLR) as part of a project named the Causal Model for Air Transport Safety (CATS) [2] and the European Organization for the Safety of Air Navigation's (EUROCONTROL) Integrated Risk Picture (IRP) [3]. The FTWG modified and expanded the earlier European effort in particular to capture US versus European system differences. Additionally, the European effort was developed based on actual accident data, so the FTWG expanded the models to capture accident events that could occur but may not yet have occurred.

2. EVENT SEQUENCE DIAGRAMS

Table 1 lists the 35 ESDs developed for ISAM by the FTWG. Note that there are several numbers missing in the list. NLR originally developed 37 accident scenarios of which 33 were ultimately incorporated in the Causal Model for Air Transport Safety (CATS) [2]. The FTWG adopted 30 as applicable to the US system, and then added five scenarios (ESD 39-43) not addressed by NLR. In order to maintain correspondence of the ESDs to CATS scenarios, the original numbering was maintained on relevant ESDs and new ones were added to the end of the list.

Each ESD begins with the initiating event described in Table 1. Following the initiating event, the ESD includes the pivotal events and the possible outcomes, where the pivotal events are those events in the scenario that may occur or not occur depending on action (e.g., does rejected take-off occur, does the flight crew maintain control of aircraft, etc.). The possible scenario outcomes include successful outcomes (e.g., aircraft continues flight), failure outcomes (e.g., runway overrun, runway veer-off, aircraft collides with ground, etc.), and partially successful outcomes (e.g., aircraft stops on the runway).

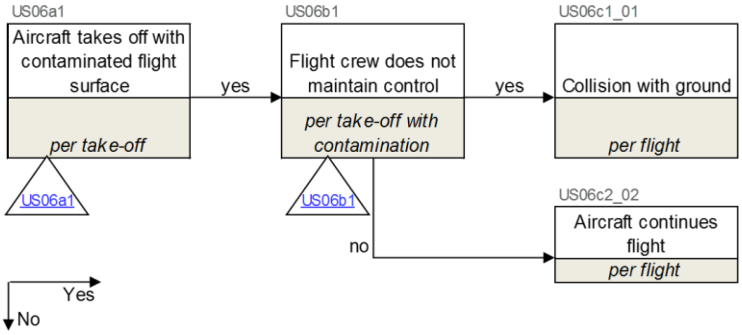
Figure 1 shows as an example ESD US06 – *aircraft takes off with contaminated flight surface*. A more descriptive definition for each node in each ESD is captured in a "data dictionary" that documents the ESDs/fault tree models. For example, in the data dictionary for ESD06, an aircraft takes off with a contaminated flight surface if: aircraft wing, horizontal stabilizer, tail and/or flight control surfaces (i.e. ailerons, elevator, trim, rudder) are contaminated with frost, ice, slush or snow, as the aircraft commences take-off. An event in which the contaminated wing results in engine problems due to ice/snow ingestion is considered in the scope of this ESD. Occurrences in which ice, snow or slush from the runway or landing gear enters the engine(s) and causes problems are excluded from this initiating event but are included in ESD US09.

Each node in the ESD has only two possible outcomes: occurs (or yes) and does not occur (or no). For the initiating event, there is not a "no" branch because the ESD is only applicable if the initiating event occurs. The probability of the scenario going in either direction at a particular node is determined by the corresponding fault tree developed for that node.

Table 1: Accident Event Sequence Diagrams

ESD	Initiating Event	Flight Phase	Number of Fault Tree Nodes
US 01	Aircraft system failure during take-off	take-off	425
US 02	ATC event during take-off	take-off	162
US 03	Directional control by flight crew inappropriate during take-off	take-off	134
US 04	Aircraft directional control related system failure during take-off	take-off	165
US 05	Incorrect configuration during take-off	take-off	132
US 06	Aircraft takes off with contaminated flight surface	take-off	57
US 08	Aircraft encounters wind shear after rotation	take-off	108
US 09	Single engine failure during take off	take-off	124
US 10	Pitch control problem during take-off	take-off	176
US 11	Fire on-board aircraft	in flight	223
US 12	Flight crew member spatially disoriented	in flight	52
US 13	Flight control system failure	in flight	152
US 14	Flight crew member incapacitation	in flight	20
US 15	Ice accretion on aircraft in flight	in flight	30
US 16	Airspeed, altitude or attitude display failure	in flight	128
US 17	Aircraft encounters adverse weather	in flight	67
US 18	Single engine failure in flight	in flight	57
US 19	Unstable approach	approach & landing	200
US 21	Aircraft weight and balance outside limits during approach	approach & landing	234
US 23	Aircraft encounters wind shear during approach or landing	approach & landing	199
US 25	Aircraft handling by flight crew inappropriate during flare	approach & landing	176
US 26	Aircraft handling by flight crew inappropriate during landing roll	approach & landing	59
US 27	Aircraft directional control related systems failure during landing roll	approach & landing	157
US 31	Aircraft are positioned on collision course in flight	in flight	114
US 32	Runway incursion involving a conflict	take-off/landing	82
US 33	Cracks in aircraft pressure boundary	in flight	149
US 35	Conflict with terrain or obstacle imminent	in flight	61
US 36	Conflict on taxiway or apron	take-off/landing	145
US 37	Wake vortex encounter	in flight	53
US 38	Loss of control due to poor airmanship	in flight	29
US 39	Runway incursion - incorrect presence of single aircraft for take-off	take-off	177
US 40	ATC event during landing	approach & landing	202
US 41	Taking off from a taxiway	take-off	177
US 42	Landing on a taxiway	approach & landing	63
US 43	Landing on the wrong runway	approach & landing	63

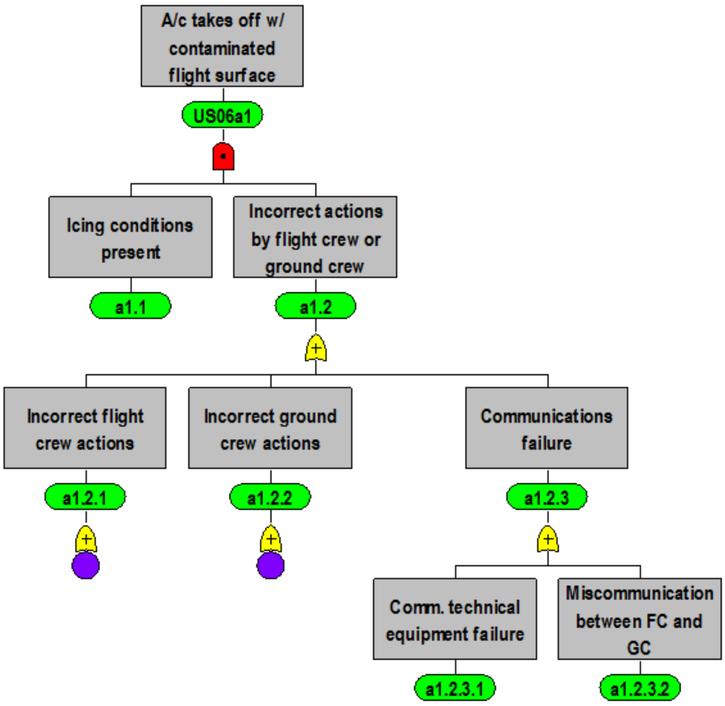
Figure 1: ESD US06 – Aircraft takes off with contaminated flight surface


US06a1
Aircraft takes off with contaminated flight surface
per take-off
US06a1
yes
US06b1
Flight crew does not maintain control
per take-off with contamination
US06b1
yes
US06c1_01
Collision with ground
per flight
no
US06c2_02
Aircraft continues flight
per flight
Yes
No

3. FAULT TREE DIAGRAMS

The triangles in Figure 1 denote the presence of a fault tree for that event node. Figure 2 shows part of the fault tree for the initiating event – *aircraft takes off with contaminated flight surface*. Figure 2 shows both types of gates used in the fault trees: OR gates and AND gates. The AND gate is the rounded red shape with the dot and means that both lower level events need to be true for the higher level event to be true. The OR gate is the more pointed yellow shape with the plus and means that the higher level event will be true if any of the lower level events are true. In order to increase the readability of the figure, not all nodes are shown in Figure 2. Figure 2 and all fault tree figures in this paper are drawn with Syncopation Software's Decision Programming Language Fault Tree package (DPL-f). In order for an aircraft to take off with a contaminated flight surface, ice needs to be present and either the flight crew or the ground crew need to perform an incorrect action (i.e., someone needs to fail to notice the icing on the flight surface since if all correct procedures are performed, ice present on a flight surface should be detected and treated before take-off). As shown in Figure 2, three reasons are identified for the failure to identify and correct the contaminated flight surface prior to take-off: *incorrect flight crew actions*, *incorrect ground crew actions*, or *communications failure* including technical difficulties such as equipment failure, or miscommunications between flight crew and ground crew.

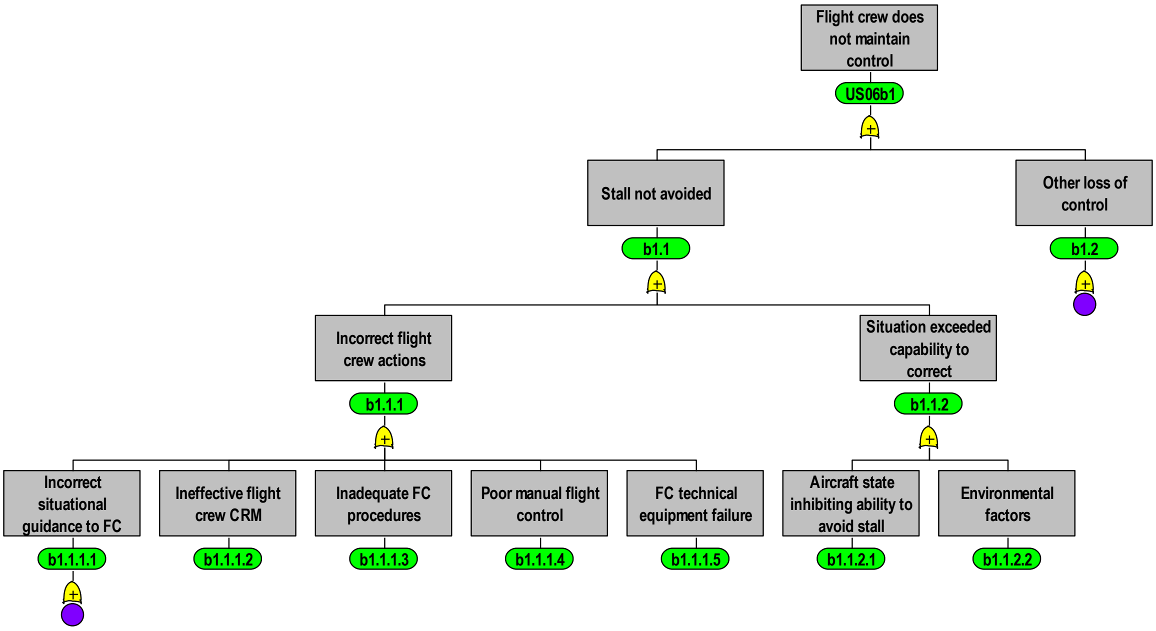
Figure 2: US06a1 – Fault tree for initiating event: aircraft takes off with contaminated flight surface (Not all nodes shown)


A/c takes off w/ contaminated flight surface
US06a1
Icing conditions present
a1.1
Incorrect actions by flight crew or ground crew
a1.2
Incorrect flight crew actions
a1.2.1
Incorrect ground crew actions
a1.2.2
Communications failure
a1.2.3
Comm. technical equipment failure
a1.2.3.1
Miscommunication between FC and GC
a1.2.3.2

The units for each node in the ESD appear in Figure 1. At this stage, the fault tree structures do not incorporate dependency among nodes or among ESDs beyond the conditional relationships defined by the units, so having clearly identified units are important for the quantification task. The initiating event in US06a1 is per take-off. Then, the second node, the pivotal event US06b1 – *flight crew does not maintain control*, is conditional on the initiating event occurring, i.e., the aircraft taking off with a contaminated flight surface. This conditional relationship is captured in the units for the pivotal event – per take-off with contamination. Within the fault tree, the nodes are interpreted as conditional with respect to the top event. In the data dictionary that accompanies the model (not shown here), units are described for each node. In the US06a1 tree shown in Figure 2, icing conditions present are in units of per take-off. All units in the incorrect actions by flight crew or ground crew sub-tree are per take-off in icing conditions. In the future, careful modeling is needed to capture critical dependencies. For example, some of the events that might cause the need to abort a take-off could also affect the aircraft's ability to stop after an aborted take-off (such as a landing gear system failure), and this failure would increase the likelihood of a runway overrun at a later pivotal event in the ESD.

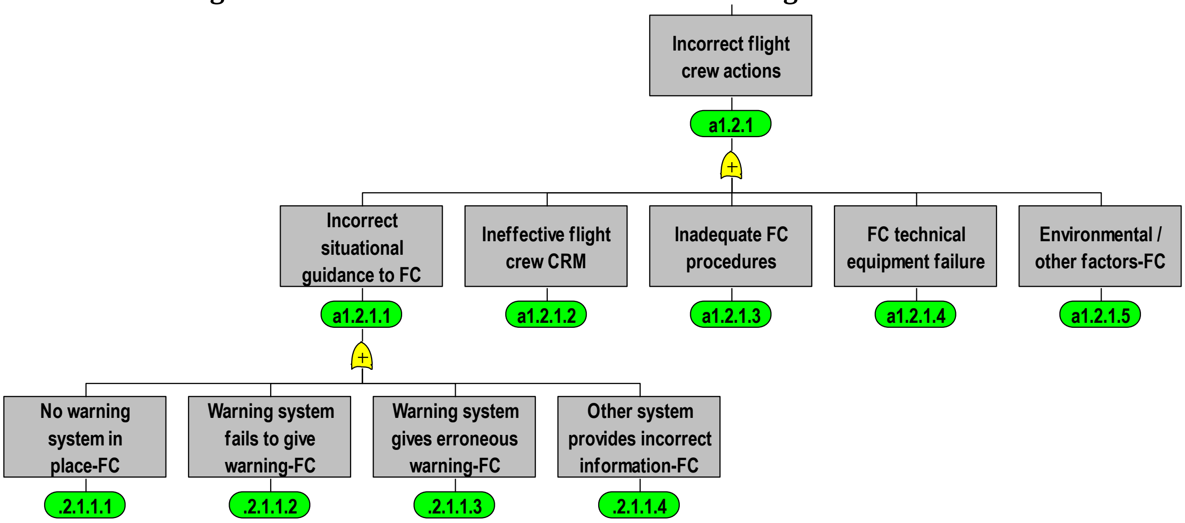
Figure 3 shows part of the fault tree for the pivotal event in US06b1 - *flight crew does not maintain control*. On take-off with a contaminated flight surface, a significant concern is the aircraft not getting enough lift and stalling. Other ways besides a stall where the flight crew does not maintain control are modeled in the b1.2 sub-tree (not shown here). Focusing on the b1.1 sub-tree as an example, the two ways that a stall is not avoided are: *incorrect flight crew actions* or the *situation exceeded the capability of the flight crew to correct* (i.e., correct actions by flight crew are performed, but the stall is unavoidable).

Figure 3: US06b1 – Fault tree for pivotal event: flight crew does not maintain controls (Not all nodes shown)


Flight crew does not maintain control
US06b1
Stall not avoided
b1.1
Other loss of control
b1.2
Incorrect flight crew actions
b1.1.1
Situation exceeded capability to correct
b1.1.2
Incorrect situational guidance to FC
b1.1.1.1
Ineffective flight crew CRM
b1.1.1.2
Inadequate FC procedures
b1.1.1.3
Poor manual flight control
b1.1.1.4
FC technical equipment failure
b1.1.1.5
Aircraft state inhibiting ability to avoid stall
b1.1.2.1
Environmental factors
b1.1.2.2

Reviewing Figures 2 and 3, one notices that human errors are a critical component in aviation accidents. In all 35 ESD's, at least one pivotal node always involves human intervention: *flight crew does not maintain control*, *flight crew does not regain control*, *flight crew does not resolve the conflict*, or *flight crew does not execute avoidance maneuver successfully*. While humans generally play an important role in most critical systems, their role is substantial in aviation accidents. Figure 4 provides the sub-tree for node a1.2.1 - *incorrect flight crew actions*. Similar sub-trees for incorrect flight crew actions appear 167 times across the 35 ESDs. The five identified contributing factors that could cause incorrect flight crew actions are: 1) *incorrect situational guidance* (i.e., receives inadequate information, leading to incorrect action), 2) *ineffective flight crew Crew Resource Management (CRM)* (i.e., follows inadequate procedures, leading to an incorrect action), 3) *inadequate flight crew procedures* (i.e., inadequate procedural guidelines, leading to an incorrect action), 4) *flight crew technical equipment failure* (i.e., experiences technical equipment failure, leading to an incorrect action), and 5) *environmental/other factors* (i.e., experiences environmental or other factors not otherwise accounted for in the fault tree lead to incorrect or insufficient flight crew instructions).

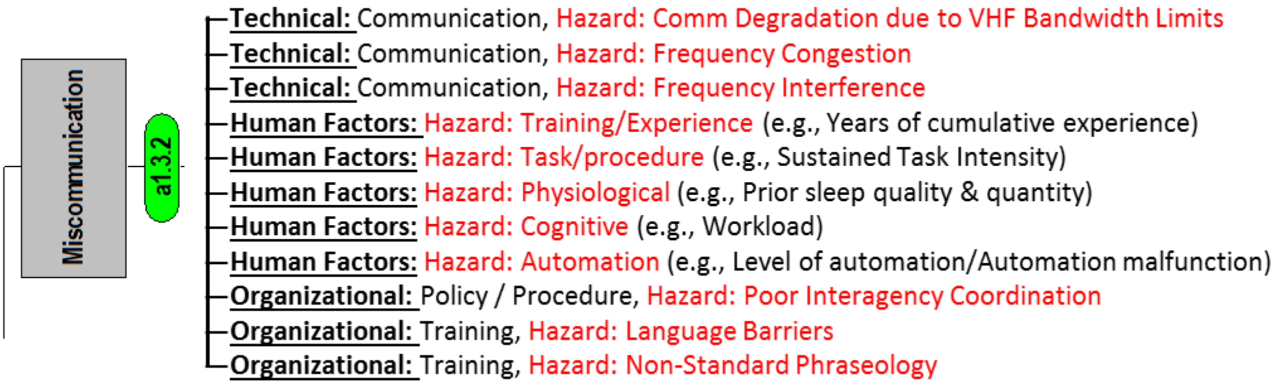
Figure 4: US06a1.2.1 – Sub-tree for incorrect flight crew actions


Incorrect flight crew actions
a1.2.1
Incorrect situational guidance to FC
a1.2.1.1
Ineffective flight crew CRM
a1.2.1.2
Inadequate FC procedures
a1.2.1.3
FC technical equipment failure
a1.2.1.4
Environmental / other factors-FC
a1.2.1.5
No warning system in place-FC
.2.1.1.1
Warning system fails to give warning-FC
.2.1.1.2
Warning system gives erroneous warning-FC
.2.1.1.3
Other system provides incorrect information-FC
.2.1.1.4

4. HAZARDS ASSESSMENT AND ISAM INTEGRATION

Implementing changes to reduce risks identified in the fault trees requires an additional step – linking the failure modes to identifiable hazards. As part of the ISAM effort, one single hazard database for hazards relevant to aviation safety was created from multiple previously existing efforts. This process resulted in a database of about 500 hazards. The hazards in this resultant list are organized into one of four categories: technical, environmental, organizational, and human factors. For the purposes of ISAM integration and validation, these groups were mapped to events in the ESDs and fault trees, such as Runway Incursion. During ISAM workshops, subject matter experts evaluated the validity of the hazard groupings and assignments, and determined which groups would be impacted by NextGen. In addition, they also had the opportunity to add new hazards or comment on definitions for existing hazards. This hazard assessment and assignment process is continuing as existing or new hazard databases are updated or identified. Thoroughly understanding the roles of hazards in the system provides the best opportunity to intervene and further improve the safety of the system. Figure 5 provides an example mapping of relevant hazards to the base event – *miscommunication between flight crew and air traffic control*.

Figure 5: Example mapping of hazards to base event in the fault tree model


Miscommunication
a1.3.2
Technical: Communication, Hazard: Comm Degradation due to VHF Bandwidth Limits
Technical: Communication, Hazard: Frequency Congestion
Technical: Communication, Hazard: Frequency Interference
Human Factors: Hazard: Training/Experience (e.g., Years of cumulative experience)
Human Factors: Hazard: Task/procedure (e.g., Sustained Task Intensity)
Human Factors: Hazard: Physiological (e.g., Prior sleep quality & quantity)
Human Factors: Hazard: Cognitive (e.g., Workload)
Human Factors: Hazard: Automation (e.g., Level of automation/Automation malfunction)
Organizational: Policy / Procedure, Hazard: Poor Interagency Coordination
Organizational: Training, Hazard: Language Barriers
Organizational: Training, Hazard: Non-Standard Phraseology

5. MODEL VALIDATION AND QUANTIFICATION

At the completion of the initial version of the ESD/fault trees model, the Microsoft Excel formatted workbook containing a separate worksheet for each accident scenario (including ESD and all fault trees, along with node definitions) was distributed to relevant SMEs from a variety of backgrounds including airport operations, air traffic control, and flight operations for review and validation. To start, ten review meetings occurred with different participants reviewing different scenarios based on their expertise. Some experts participated in person, but most of the reviews occurred via teleconference with a web-presentation link. The reviews specifically focused on mapping past historical accidents to the ESDs and fault trees to identify factors that contributed to historical accidents that were not clearly represented in the fault trees. Additionally, comments regarding the structure and wordings of both the ESDs and all fault trees were collected from the reviewers.

The FTWG then reviewed the comments and made suggestions on revisions to both ESDs and fault trees. ESDs and fault trees were revised in real-time so that reviewers could comment on how their suggestions were implemented in revisions of the model. In most cases, the reviewers identified more detail that should be included in the models, not less (i.e., very few suggestions were to delete what was there, and most suggestions were to include additional items that were missing).

The next step in this project is to quantify the ESDs and fault trees by assigning probabilities to the nodes based on historical data. One source of data being used is the FAA’s Aviation Safety Information Analysis and Sharing (ASIAS) system. ASIAS has 42 member airlines sharing data integrating both data from the Aviation Safety Reporting System (ASRS) (i.e., voluntary reports) and Flight Operational Quality Assurance (FOQA) data (i.e., recorded data) with other data sources such as the National Transportation Safety Board (NTSB) investigations [4]. The quantification task is on-going, and it is expected that many additional lessons will be learned from the quantification step.

6. LESSONS LEARNED

In total, the 35 ESDs and corresponding fault trees have 4,552 nodes. The final column in Table 1 shows the number of nodes in the fault trees per ESD. From reviewing this list, it is apparent that some accident scenarios are more complex than others.

Some of the lessons learned identified by the FTWG that would be helpful to others undertaking such a task are [5]:

- The task is best performed with a team of contributors. Breaking off the team to work on different ESDs/fault trees may prove ineffective and produce inconsistent models especially if types of events are similar across accident scenarios (e.g., *incorrect flight crew actions*).
- Review of the European CATS and IRP models included higher-level “luck” or “providence” nodes. These nodes likely represent situations when ATC and flight crews do everything right (as detailed by the sub-trees), but the aircraft still find themselves on a collision course or vice versa when ATC and flight crews do everything wrong but still do not collide. Initially, luck was not included in the 35 ESDs, but in a later iteration, in several ESDs a node named *Avoidance Essential* was added to reflect that subsequent to some failure events occurring, action by the flight crew or vehicle driver would still have been necessary to avoid a collision (i.e., good luck alone does not resolve the conflict for example).
- Actions by ATC to resolve conflicts are still dependent on flight crew actions in many cases. For example, ATC’s instructions alone cannot bring about a successful outcome. The flight crew has to successfully respond to the ATC instructions, and that needs to be clearly modelled in the fault trees.

Several significant challenges remain in completing this quantitative risk model. These challenges include:

- Quantification of the probabilities of the 4,552 nodes from available data, recognizing that some data may not exist in any searchable database. This could be a driver for the development of new data sets.

- Developing a common taxonomy. Existing safety reporting databases currently utilize ad-hoc language to describe events with little standardization. This problem makes the quantification task even more challenging.
- Understanding the role of luck (as described above).
- Appropriately capturing dependencies among nodes and among ESDs (e.g., in ESD US01 – *aircraft system failure during takeoff*: if system failure is associated with landing gear system, this will affect a later pivot event: *sufficient braking not accomplished*)
- Learning from near-misses. Quantifying the nodes relying on available data from events that have happened is hard enough, but since fault trees are binary (happened or did not happen), how can the risk model capture events that almost happened but did not happen, differently from those that never almost happened.
- Keeping it simple. As the team applied recommended changes to the fault tree structures, the structures became increasingly complex. Additionally, some ESDs were altered to reflect this complexity. While increasing complexity, these changes were necessary to ensure the model represents all possible events in a particular scenario; so simplicity versus completeness will always be a significant trade-off, and commonly more complex ESDs can result in simpler fault trees, another trade-off.

7. CONCLUSION

The FTWG developed a set of 35 accident ESDs and corresponding fault trees. Development and validation of the trees included input from more than 20 SMEs from a wide range of aviation and industry backgrounds. A series of workgroup sessions resulted in the initial development of the trees and a data dictionary. The data dictionary serves as a change tracking tool, hazard mapping tool, and integration mechanism for the web-based ISAM implementation. A single-source hazard database was developed and hazards are currently mapped to initiating-event fault trees for a priority set of ESDs and integrated in ISAM. Those hazard connections were validated by additional SMEs during multiple workshops. Validation of the fault trees occurred indirectly during the ISAM workshops and directly through a series of accident scenario mapping sessions. The validation process has revealed gaps in the development process. Many of those gaps are already fixed, but some questions remain for future work.

Acknowledgements

ISAM is funded by the System Safety Management Transformation program (Sherry Borener, Program Manager). This paper reflects the opinions of the authors only and does not reflect the opinion of the Federal Aviation Administration or any other organization affiliated with the authors.

References

[1] S. Borener, S. Trajkov, P. Balakrishna, “Design and Development of an Integrated Safety Assessment Model for NextGen”, American Society for Engineering Management, Proceedings of the 33rd International Annual Conference, Virginia Beach, (2012).
[2] B. Ale, L.J. Bellamy, R. Cooke, M. Duyvis, D. Kurowicka, P.H. Lin, O. Morales, A. Roelen, J. Spouge, *Causal Model for Air Transport Safety, Final Report*, (2009).
[3] Eurocontrol, D2.4.3-02, *SESAR Top-down Systematic Risk Assessment Version 1.01,* http://www.episode3.aero/public-documents, (accessed June 24, 2013).
[4] ASIAS (2013), FAA AVIATION SAFETY INFORMATION ANALYSIS AND SHARING (ASIAS) SYSTEM, http://www.asias.faa.gov/pls/apex/f?p=100:1:, (accessed February 26, 2014).
[5] M. Robinson, S. Borener, K. Mitchell, P. Balakrishna, R. Dillon-Merrill, A. Hepler, A. Best, “Development of an Event Sequence Diagram-Fault Tree Model for Integrated Safety Assessment in U.S. Commercial Aviation,” Federal Aviation Administration, White Paper, Washington DC, (2013).