ATC Safety incidents analysis and reaction
Risk Assessment in Air Traffic Management

Álvaro Rodríguez Sanz
Sergio Cámara Serrano
Rosa Arnaldo Valdés
Fernando Gómez Comendador

Department of Aerospace Systems, Air Transport and Airports
School of Aeronautical Engineering
Technical University of Madrid

UPM SUMMER SCHOOL
LISA - Laboratory of ideas for Safety in Aviation. Addressing Aviation and ATM Safety Challenges

La Granja 11th-14th July, 2016
OUTLINE

- Introduction
- Theory
- Multistate Aircraft Proximity Risk Model (MAPRM)
- Bayesian Network model construction
- Results and discussion
- Conclusions
INTRODUCTION

• Risk
• Aircraft Proximity Incidents & Mid-Air Collisions
• New approach to the problem
• Research objective
Risk: Combination of severity and probability

- Severity: Severity of the consequences of the hazard
- Repeatability: Probability of the hazard to happen again
Risk Events

- Aircraft Proximity Incident
- Mid-Air Collision
- Aircraft Proximity Incident (API)
  - Distance between airplanes has been reduced up to a point where their safety may have been compromised.
  - Relative positions and speeds have to be considered.
- Mid-Air Collision (MAC)
  - Two or more airplanes collide while airborne
  - Most severe expression of the events
Aircraft Proximity Incidents (APIs)
- Also known as “conflicts” and “loss of separation” among aircraft.
- Prescribed separation minima (*) in controlled airspace are infringed.
- Probabilistic risk models allow guessing the probability of APIs.

The probability of an Aircraft Proximity Incident is the probability that the distance between a pair of aircraft becomes smaller than a prescribed safety minimum separation value.

(*) Separation minima are specified for each type of airspace by the Air Traffic Control authorities, according to ICAO (International Civil Aviation Organisation) standards.
How are API and MAC studied? How could that study be improved?

**Traditional approach**
- Binary events
- FTA and ETA

**New approach**
- Multi-state events
- Bayesian Network
Main objective of the research

Study how the Risk involved in Aircraft Proximity Events can be estimated and analysed by the construction of a multi-state system model based on a Bayesian Network.
THEORY

• Probabilistic risk assessment (PRA)
• Multi state systems (MSSs)
• Bayesian Networks (BNs)
System’s reliability analysis involve a probabilistic risk assessment (PRA), which allows estimating the likelihood and consequences of incidents.

Besides, classification of potential scenarios can be developed by using PRAs.
How are PRA developed?

Traditional analysis methods assume that events involved are binary events:

- Perfect functionality
- Complete failure

In real situations, the system and its components can appear in different working or failure modes.

Binary events seems to be a non complete method of study
Multi-state systems (MSSs)

Components and system are allowed to have an arbitrary number of performance levels.

A system should be considered as MSSs when:

- Any system consisting of different units that have a cumulative effect on the entire system performance.
- The performance rate of the different elements that compose a system can also vary as a result of their deterioration.
• MSSs can be divided into two main types:

**Systems with multiple work (or failure) states**

- These systems can be in several work or failure states, in addition to the traditional two states.

**Systems with multi-performance levels**

- These systems are able to function at different performance levels.
In complex systems, any complete failure does not occur suddenly but usually is a result of accumulation of a sequence of many gradual or partial failures of different types.

Aircraft Proximity Events will be studied as an accumulation of several failures of the different involved elements. Besides, these elements can present an arbitrary number of failure levels.

This approach is in line with the Safety II concept by EUROCONTROL (flexible, variable and proactive/predictive).
Fundaments of MSSs models

Any system element \( i \) can have \( k_i \) different states corresponding to the performance rates \( g_i \).

The performance rate of an element \( i \) at an instant \( t \) is a random variable that takes its values from the sets of possible states \( (g_i) \).

The probabilities associated with the different states of the system element \( i \) at any instant \( t \) are represented by \( p_i(t) \).
Fundamentals of Bayesian networks (BNs)
Consist of two different elements:

- **Directed Acyclic Graph (DAG)**: graphical representation of the different involved elements (qualitative part of the model)
- **Conditional Probability Tables (CPTs)**: probability distributions (quantitative part of the model)
- DAG's elements:

  - **Parent Node**: Represents a primitive variable
  - **Arc**: Represents a relationship between nodes
  - **Descendant Node**: Represents a dependent variable
A BN is a pair \((G,P)\), where \(G\) is a DAG defined on a set of nodes (the random variables), and \(P\) is a set of CPTs, one for each variable.

- \(G\) contains qualitative information about relationships between variables.
- \(P\) contains quantitative information about states appearance’s likelihood.

**Bayes Theorem:**

\[
P(A|B) = \frac{P(B|A) \times P(A)}{P(B)}
\]

Joint probability density of all nodes:

\[
p(x) = p(x_1, \ldots, xn) = \prod_{i=1}^{n} p(x_i | \pi(xi))
\]

\[
P(x_1, x_2, x_3, x_4, x_5) = P(x_1)P(x_2|x_1)P(x_3|x_1)P(x_4|x_2, x_3)P(x_5|x_4)
\]
 Remember the Lego blocks...

\[
P\text{(red/yellow)} = \frac{P\text{(yellow/red)}P\text{(red)}}{P\text{(yellow)}}
\]

 Remember the sprinkler, the rain and the wet grass...
- Bayesian Networks and Multi-state Systems on risk assessment modelling
- BNs are suitable for characterising MSSs reliability and risk assessment due to their capability of describing the multi-state characteristics of the logic relationship of events.
Main contributions of MSSs and BNs:

- MSSs allow describing the different states of components and systems accurately.
- BNs allow reflecting the relationship between component performance and system performance, and between system reliability and system performance.
MULTISTATE AIRCRAFT PROXIMITY RISK MODEL (MAPRM)

- Risk contributory factors
- Parametrisation
- Model structure
Risk is defined as the combination of severity of a harm and the probability (likelihood) of occurrence of such harm.

\[ \text{RISK} = \text{PROBABILITY} \times \text{CONSEQUENCES SEVERITY} \]
Safe aircraft separation in controlled airspace is assured by Air Traffic Management (ATM).

ATM includes a set of services supplied by air traffic controllers (based on ground and, additionally, collision avoidance systems equipped on aircrafts).

Sources:

– Harmonisation of Safety Occurrence Severity and Risk Assessment (EUROCONTROL, 2005)
In ATM, risks are defined by two elements: severity and repeatability.
Severity:
- Proximity: closest distance + rate of closure.
- Controllability: performance of the ATC system barriers.

Repeatability:
- Systemic factors: ATC system and procedural failures or deficiencies.
- Non systemic factors: human errors and organisational issues.
A 5x5 risk matrix is commonly used in ATM risk assessment:

<table>
<thead>
<tr>
<th>REPEATABILITY</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Frequent</td>
<td>A1</td>
<td>B1</td>
<td>C1</td>
<td>E1</td>
<td>E1</td>
</tr>
<tr>
<td>Frequent</td>
<td>A2</td>
<td>B2</td>
<td>C2</td>
<td>E2</td>
<td>E2</td>
</tr>
<tr>
<td>Occasional</td>
<td>A3</td>
<td>B3</td>
<td>C3</td>
<td>E3</td>
<td>E3</td>
</tr>
<tr>
<td>Rare</td>
<td>A4</td>
<td>B4</td>
<td>C4</td>
<td>E4</td>
<td>E4</td>
</tr>
<tr>
<td>Extremely rare</td>
<td>A</td>
<td>B5</td>
<td>C5</td>
<td>E5</td>
<td>E5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SEVERITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
</tr>
<tr>
<td>B</td>
</tr>
<tr>
<td>C</td>
</tr>
<tr>
<td>D</td>
</tr>
<tr>
<td>E</td>
</tr>
<tr>
<td>Serious</td>
</tr>
<tr>
<td>Major</td>
</tr>
<tr>
<td>Significant</td>
</tr>
<tr>
<td>No safety effect</td>
</tr>
<tr>
<td>No determined</td>
</tr>
</tbody>
</table>
Parametrisation of variables

- **Serious - A**: Incident involving circumstances indicating that an accident nearly occurred. Critical near collision between aircraft.

- **Major - B**: Safety may have been compromised leading to a near collision between aircraft. Safety margins not respected. A crew avoidance manoeuvre and/or an ATC instruction allowed to reduce the risk without eliminating it.

- **Significant - C**: A serious or major incident could have occurred if the risk had not been managed by ATC or crew actions.

- **No safety effects - D**: An incident that has no safety significance.

- **Not determined - E**: Insufficient information available to determine the risk involved. Inconclusive or conflicting evidence precluded risk determination.
### Repeatability

- **Very frequent - 1:**
  - Has occurred a **very high number of times** throughout the total lifetime of the system.
  - Has occurred a **very high number of times at the same location**.

- **Frequent - 2:**
  - Has occurred **significant number of times** throughout the total lifetime of the system.
  - Has occurred a **significant number of times at the same location**.

- **Occasional - 3:**
  - Has occurred **several times** throughout the total lifetime of the system.
  - Has occurred **more than once at the same location**.

- **Rare - 4:**
  - Has occurred **very few times** throughout the total lifetime of the system.

- **Extremely rare - 5:**
  - Has **never occurred yet** throughout the total lifetime of the system.

### Parametrisation of variables
Risk contributory factors:
Risk dependencies:
- **Severity** component

  - **Proximity**
    - Rate of closure.
    - Achieved separation.

  - **Controllability**
    - ATM business/task model.
    - Defence and barriers model.
Proximity component

- **Proximity**
  - **Rate of closure**: Relative geometry between aircraft's paths.
  - **Achieved separation**: Physical horizontal and vertical separation achieved between aircraft.
- Rate of closure component

- None (R.C. = 0 kt.)
- Low (R.C. < 60 kt.)
- Medium (60 kt. < R.C. < 250 kt.)
- High (250 kt. < R.C. < 600 kt.)
- Very High (R.C. > 600 kt.)
Achieved separation component

- Achieved separation
- Minimum separation achieved
- 75% Min. <Separation< Min.
- 50% Min. <Separation< Min. 75%
- 25% Min. <Separation< Min. 50%
- Separation< Min. 25%

Separation among aircraft equals the prescribed minimum safety separation standard for a given airspace.
Controllability

- Pretends to reflect the influence of the performance of the ATM system and its barriers.
- Two intermediate developments:
  - **ATM business/task model**: behaviour of the system.
  - **Defence and barriers model**: safety related functions of an ATM system.
- ATM business/task model
- This risk model should cover all the ATM services that could be involved in aircraft risk of collision.
ATM business/task model
- ATM defences and barriers model
- Based on Reason theory:

- Fallible decisions
- Line deficiencies
- Psychological precursors of unsafe acts
- Unsafe acts
- Inadequate defenses
- Latent failures
- Active Failure
- Limited window of opportunity

Accident
- ATM defences and barriers model
- Example:
ATM defences and barriers model
- Controllability components
- Detection barrier

ATM conflict detection barrier

- Conflict detected
- Conflict detected late
- Conflict not detected
- ATC detection not applicable
- Unknown
- Controllability components
- Planning barrier

ATM conflict planning barrier

- Plan correct
- Plan inadequate
- No plan
- ATC planning not applicable
- Controllability components
- Execution barrier

ATM conflict execution barrier

- Execution correct
- Execution inadequate
- No execution
- ATC execution not applicable
- Controllability components
- STCA

[Diagram: Short Term Conflict Alert (STCA) with branches: STCA triggered, No STCA alarm, Not applicable]
- Controllability components
- Recovery by ATC

- Incident recovery by ATC
  - Adequate recovery
  - Inadequate recovery
  - No recovery
  - Not applicable
- Controllability components
- TCAS

![Traffic Collision Avoidance System](image)

- TCAS triggered
- No TCAS warning
- **Controllability components**
- **Pilot**

  - Pilot execution
    - Pilot followed RA/ATC instructions
    - Pilot insufficiently followed RA/ATC instructions
    - Pilot incorrectly followed RA/ATC instructions
    - No pilot action
Risk

Severity

Repeatability
- **Repeatability**
  - **Historical data:** similar accidents occurred in the past.
  - **Systemic issues:** equipment, procedural or management failures.
  - **Non systemic issues:** human factors errors.
  - **Window of opportunity:** likelihood of a particular operational scenario.
  - **Timing:** urgency to attend the event.
  - **Causes or events:** number of events that have to be attended by ATM workers.
- **Repeatability components**
- **Historical data**

![Diagram](attachment:image.png)
- Repeatability components
- Systemic issues
- **Repeatability components**
- **Non-Systemic issues**
- Repeatability components
- Window of opportunity
- **Repeatability components**
- **Timing**

![Diagram showing the relationship between Repeatability components and Timing, with branches for Irrelevant, Role playing, and Indispensable.](diagram.png)
- Repeatability components
- Causes or events

```
Causes or events
  - Many
  - Average
  - Few
```
Mind map for factors underlying in Aircraft Proximity Events
BAYESIAN NETWORK MODEL CONSTRUCTION

- Theoretical structure
- Data collection
- Practical structure
The structure is generated according to observations, expert judgement techniques and stakeholder validation.

Each state of different variables that have been identified for the system will have an assigned value.
Theoretical BN for severity component

Hazard resolution

Incident recovery
Theoretical BN for **repeatability** component
These networks will work independently and simultaneously.

Once introduced the related statements of the events, two different and complementary classifications will be obtained.

Once the network is designed, the implementation of the appropriate data will complete the CPT of each node.
Data collection

73 investigation reports of aircraft incident have been analysed.

All reports were published in 2015 by Spanish Aviation Safety Authority (AESA).
<table>
<thead>
<tr>
<th>Sub-network</th>
<th>Node</th>
<th>Estate</th>
<th>Nº of cases</th>
<th>Probability (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proximity</td>
<td>Minimum Separation</td>
<td>Achieved</td>
<td>8</td>
<td>11,11</td>
</tr>
<tr>
<td></td>
<td>More than 75%</td>
<td></td>
<td>11</td>
<td>15,28</td>
</tr>
<tr>
<td></td>
<td>From 50 to 75%</td>
<td></td>
<td>35</td>
<td>48,61</td>
</tr>
<tr>
<td></td>
<td>From 25 to 49%</td>
<td></td>
<td>16</td>
<td>22,22</td>
</tr>
<tr>
<td></td>
<td>Less than 25%</td>
<td></td>
<td>2</td>
<td>2,78</td>
</tr>
<tr>
<td>Rate of Closure</td>
<td>None</td>
<td></td>
<td>22</td>
<td>30,56</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td></td>
<td>15</td>
<td>20,83</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td></td>
<td>10</td>
<td>13,89</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td></td>
<td>17</td>
<td>23,61</td>
</tr>
<tr>
<td></td>
<td>Very High</td>
<td></td>
<td>8</td>
<td>11,11</td>
</tr>
<tr>
<td>Conflict Detection</td>
<td>Correct</td>
<td></td>
<td>49</td>
<td>67,12</td>
</tr>
<tr>
<td></td>
<td>Inadequate</td>
<td></td>
<td>2</td>
<td>2,74</td>
</tr>
<tr>
<td></td>
<td>Not Detected</td>
<td></td>
<td>22</td>
<td>30,14</td>
</tr>
<tr>
<td>Plan</td>
<td>Correct</td>
<td></td>
<td>20</td>
<td>27,40</td>
</tr>
<tr>
<td></td>
<td>Inadequate</td>
<td></td>
<td>30</td>
<td>41,10</td>
</tr>
<tr>
<td></td>
<td>No Plan</td>
<td></td>
<td>23</td>
<td>31,50</td>
</tr>
<tr>
<td>Execution</td>
<td>Correct</td>
<td></td>
<td>0</td>
<td>0,00</td>
</tr>
<tr>
<td></td>
<td>Inadequate</td>
<td></td>
<td>32</td>
<td>43,84</td>
</tr>
<tr>
<td></td>
<td>No Execution</td>
<td></td>
<td>41</td>
<td>56,16</td>
</tr>
<tr>
<td>STCA</td>
<td>STCA triggered</td>
<td></td>
<td>72</td>
<td>98,63</td>
</tr>
<tr>
<td></td>
<td>No STCA warning</td>
<td></td>
<td>1</td>
<td>1,37</td>
</tr>
<tr>
<td>Recovery</td>
<td>Correct</td>
<td></td>
<td>35</td>
<td>47,95</td>
</tr>
<tr>
<td></td>
<td>Inadequate</td>
<td></td>
<td>32</td>
<td>43,84</td>
</tr>
<tr>
<td></td>
<td>Not Recovery</td>
<td></td>
<td>6</td>
<td>8,21</td>
</tr>
<tr>
<td>TCAS</td>
<td>TCAS triggered</td>
<td></td>
<td>73</td>
<td>100,00</td>
</tr>
<tr>
<td></td>
<td>No TCAS RA</td>
<td></td>
<td>0</td>
<td>0,00</td>
</tr>
<tr>
<td>Pilot followed RA</td>
<td>Correct</td>
<td></td>
<td>72</td>
<td>98,63</td>
</tr>
<tr>
<td></td>
<td>Insufficiently</td>
<td></td>
<td>1</td>
<td>1,37</td>
</tr>
<tr>
<td></td>
<td>Incorrect</td>
<td></td>
<td>0</td>
<td>0,00</td>
</tr>
<tr>
<td>Sub-network</td>
<td>Node</td>
<td>Estado</td>
<td>Nº of cases</td>
<td>Probability (%)</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------</td>
<td>-----------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Procedures</td>
<td>Design</td>
<td>0</td>
<td>0,00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Implementation</td>
<td>2</td>
<td>2,74</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lack of</td>
<td>0</td>
<td>0,00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Not Applicable</td>
<td>71</td>
<td>97,26</td>
<td></td>
</tr>
<tr>
<td>Equipment</td>
<td>Design</td>
<td>1</td>
<td>1,37</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Implementation</td>
<td>1</td>
<td>1,37</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lack of</td>
<td>1</td>
<td>1,37</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Not Applicable</td>
<td>70</td>
<td>95,89</td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td>Design</td>
<td>2</td>
<td>2,74</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Implementation</td>
<td>1</td>
<td>1,37</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lack of</td>
<td>0</td>
<td>0,00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Not Applicable</td>
<td>70</td>
<td>95,89</td>
<td></td>
</tr>
<tr>
<td>Historical Data</td>
<td>None</td>
<td>0</td>
<td>0,00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Significant</td>
<td>9</td>
<td>12,33</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Few</td>
<td>35</td>
<td>47,95</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Very High</td>
<td>29</td>
<td>39,73</td>
<td></td>
</tr>
<tr>
<td>Situation</td>
<td>Daily routine</td>
<td>66</td>
<td>90,41</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Workload peak</td>
<td>7</td>
<td>9,59</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Emergency</td>
<td>0</td>
<td>0,00</td>
<td></td>
</tr>
<tr>
<td>Methods</td>
<td>Normal</td>
<td>71</td>
<td>97,26</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exceptional</td>
<td>2</td>
<td>2,74</td>
<td></td>
</tr>
<tr>
<td>Non-Systemic &amp; Human Involvement Issues</td>
<td>Reported Issues</td>
<td>23</td>
<td>31,51</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Not applicable</td>
<td>50</td>
<td>68,49</td>
<td></td>
</tr>
</tbody>
</table>
Once the structure of the network has been developed and the required data have been collected, the final and functional Bayesian Network, in which violated safety events are studied, can be built.

- Practical BN for severity and repeatability
Practical BN for severity component
Practical BN for **repeatability** component
RESULTS AND DISCUSSION

• Types of reasoning
• Examples
Two different operation modes.

- **Forward inference**: severity and repeatability classification in an effective, visual and quick way.

- **Backward inference**: diagnostic inference form effect to causes. Useful when some data is unknown.
Forward inference example (severity)

Report number 029/15 15 issued by the Spanish Aviation Safety Authority in relation to an incident in the TMA (Terminal Manoeuvring Area) of Seville that occurred the 30/04/2015.
- Forward inference example (severity)
- **Forward inference example (repeatability)**

- Report number 029/15 15 issued by the Spanish Aviation Safety Authority in relation to an incident in the TMA (Terminal Manoeuvring Area) of Seville that occurred the 30/04/2015.
Forward inference example (repeatability)
Backward inference example (severity)

Report number 003/15 issued by the Spanish Aviation Safety Authority in relation to an incident at the CTR (Controlled Traffic Region) of Jerez Airport occurred the 13/01/2015.
Backward inference example (severity)
CONCLUSIONS

• Utility of the model
• Applications
• Limitations
Air Traffic Incidents should be studied as a Multistate Systems (in line with the Safety II concept by EUROCONTROL).

A Bayesian Network approach allows dealing with uncertainty.

This new method is a more powerful tool than traditional methods (ETA and FTA) were.

Backward analysis provides a new contribution for the analysis of aircraft incidents.

More data (in number and from other geographical locations) are needed to improve the model.
“It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so”

Mark Twain
Thank you for your attention!

Álvaro Rodríguez-Sanz
Department of Aerospace Systems, Air Transport and Airports
School of Aeronautical Engineering
Technical University of Madrid
alvaro.rodriguez.sanz@upm.es