Belgocontrol

FAB EC Safety Assessment

Valérie Aussems
February 2008

Plan of this presentation

- Introduction
- Safety Study
- Safety Methodology
- Safety Assessment
- Safety Assessment Validation
- Conclusion

Belgocontrol

Introduction – FAB EC

- Functional Airspace Block (FAB) Europe Central
- Started in 2006
- 6 countries:

  Belgium,the Netherlands, Luxembourg,

  Germany, France, Switzerland

Belgocontrol

Introduction – FAB EC

- Commitment to increase ATM performances:

  - Safety
  - Capacity
  - Cost effectiveness

Belgocontrol

Luchtverkeersleiding Nederland
Air Traffic Control the Netherlands

AEROPORT LUXEMBOURG

DFS Deutsche Flugsicherung

EUROCONTROL

dgac
DSNA

skyguide

Belgocontrol

Introduction - FAB EC Feasibility Study

- **1st phase: Feasibility Study**

  => Basis to decide

- 2nd phase: FAB EC Master Plan
- 3rd phase: FAB EC Implementation

Introduction – FAB EC Organization

in Workgroups:

- OPS, TECH, Financial, HR,..
- **Safety Workgroup**
  - WP 7.1 Safety workgroup management
  - **WP 7.2 Safety assessment methodology dvp**
  - **WP 7.3 Assist in safety case building**
  - **WP 7.4 Safety case validation**
  - WP 7.5 SMS implementation plan

Plan of this presentation

- Introduction
- **Safety Study**
- Safety methodology
- Safety Assessment
- Safety Assessment Validation
- Conclusion

Safety study - Objective

- What? Provide sufficient information
- Why? Take decisions
- About? Safety Feasibility of FAB EC

=> High-level Policy Group

=> National level

Belgocontrol

Safety study – Safety criteria

- **Will the FAB EC be safer ?**

IF considering the predicted increase of movements in the FAB EC airspace

✓ **No increase** accidents / year

✓ **No increase** incidents / year

⇨ Safety level per movement ↗

Safety Study – Safety Criteria

Considering:

- ATM concept: safety benefits & hazards
- Increase of traffic

Statement:

Increased safety level per movement

IF all identified risks are acceptable*

*acceptable: based on expert judgement

Safety study - Framework

- Assumption: movements in the FAB EC airspace

  +40 to +50%

- Regulation: SES Common Requirements
- Available Input:

1) FAB EC Main Operational Changes (MOCs)
2) FAB EC ATM concept

- Results: 1st semester of 2008

Plan of this presentation

- Introduction
- Safety Study
- Safety methodology
- Safety Assessment
- Safety Assessment Validation
- Conclusion

Safety Methodology - Difficulties

- Various local approaches to create safety cases
- No definition of acceptable risk level
  for the FAB EC change
- Only generic operational concept

Belgocontrol

Safety Methodology - Main considerations

- No adequate and well-known methodology
- Defined by safety experts

  (Belgocontrol, DFS, DSNA, LVNL, MUAC, Skyguide)
- Qualitative approach
- As close as possible to SAM (Failure approach)

=> **Adapt SAM to a feasibility study**

Belgocontrol

Safety Methodology – Alternative approaches (1/2)

- **Safety Screening Tool**
  - Means to create safety awareness
  - Anticipate safety issues
  - Limited experience
  - Expected outputs: Safety considerations, System decomposition and scope of safety plan

☹ doesn’t answer to FAB EC Feasibility Study needs

Safety Methodology – Alternative approaches (2/2)

- **Success case**
  - Late in the feasibility study
  - To complement the failure approach
  - Limited experience
  - Additional effort higher that it was planned
  - Expected outputs: safety considerations, safety argument structure, safety plan

☺ Recognized added-value

⇒ Tool to use for building the safety plan in the final FAB EC project

Safety Methodology - Definition

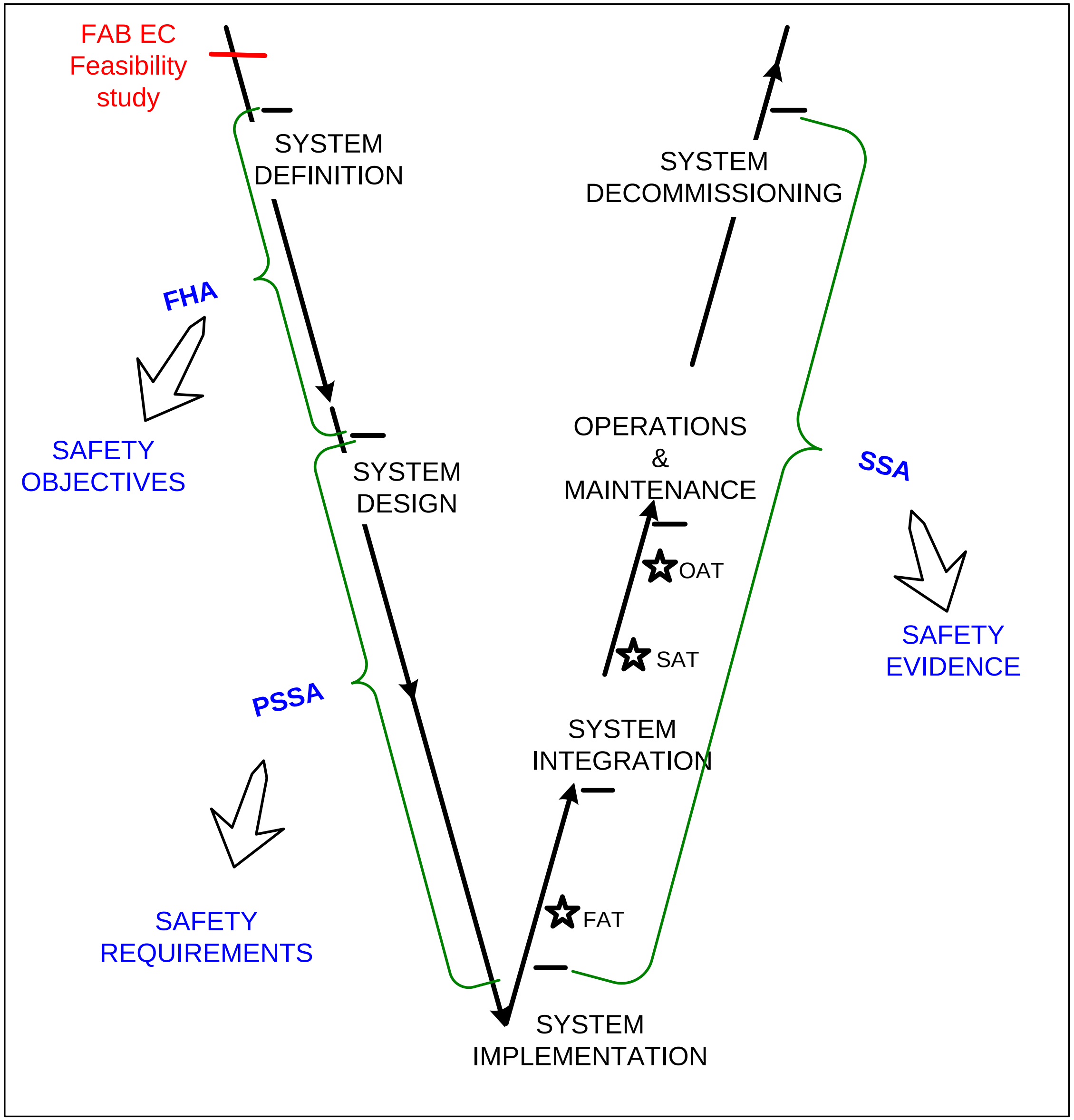
- Based on Eurocontrol SAM V2 (FHA/PSSA)
- Not enough information to conduct full FHA/PSSA
- High-level FHA & high-level PSSA

=> High-level hazards

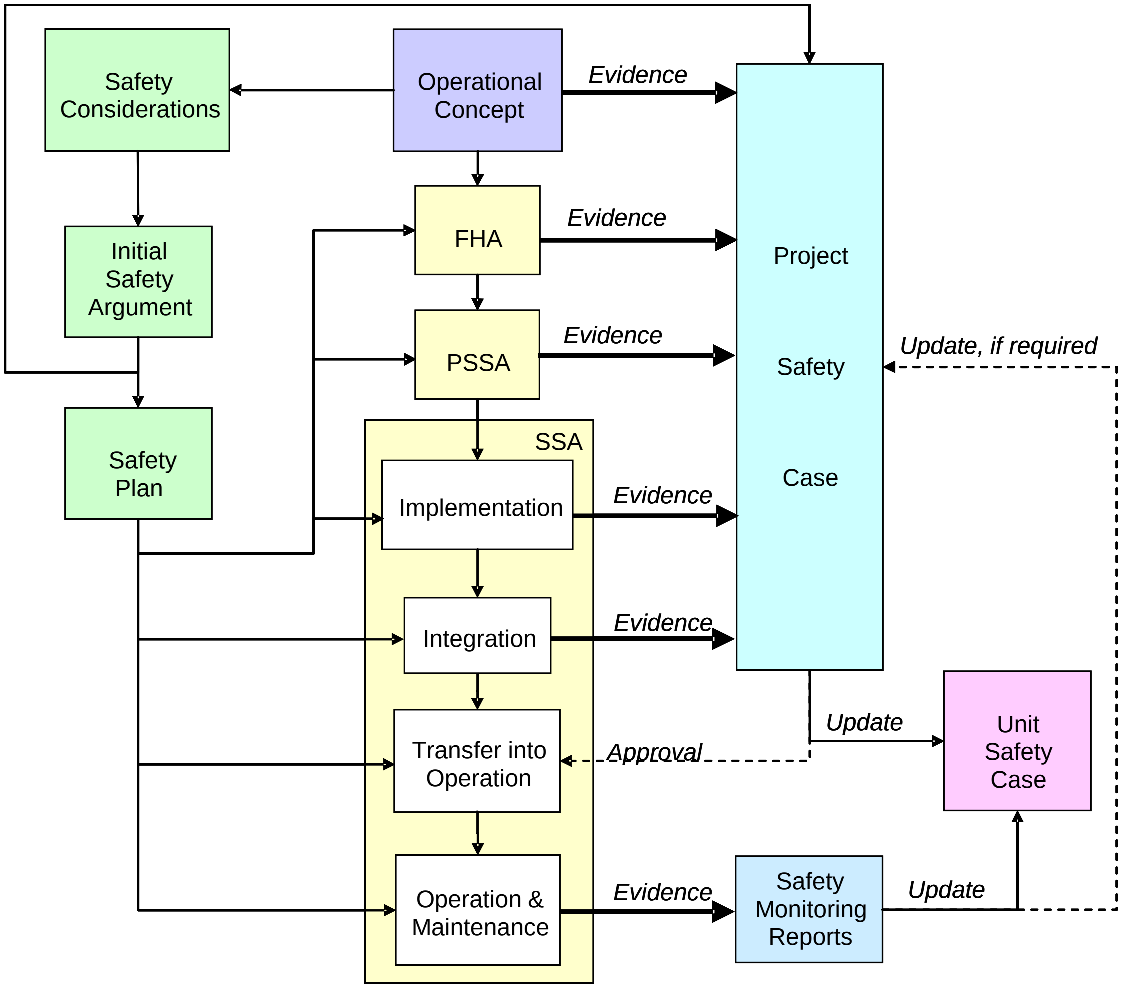
=> High-level Safety Requirements

Belgocontrol

Safety Methodology - SAM



Safety Methodology – Safety Case Process



Safety Methodology – Expected results

- Will FAB EC be safer than current operations or not ?
  - Expert judgements
  - Chosen methodology can’t answer
  - Provide a first overview
  - Indications that the FAB EC can/can’t be safer that current situation
- Review of operational concept

Safety Methodology - Summary

I) **Preliminary Safety Feasibility Study** *(MOCs)*

- High-level FHA
- High-level PSSA

II) **Final Safety Feasibility Study** *(ATM concept)*

- High-level FHA
- High-level PSSA

III) **Cross-check**: consistency between results of preliminary & final safety feasibility studies

Plan of this presentation

- Introduction
- Safety Study
- Safety Methodology
- Safety Assessment
- Safety Assessment Validation
- Conclusion

Safety Assessment – High-Level FHA

- High-Level FHA

1) Hazard identification

2) Hazard structuring

*Hazard: anything that might affect safety, safety item

Safety Assessment – High-Level FHA

1) **Hazard identification**

- Workshop following SAM guidelines
- Relevant participants (number & profiles):

  - Operational expert
  - Technical expert
  - Flight operational expert
  - Safety expert
  - Moderator

=> Output: list of safety items of different types

Safety Assessment – High-Level FHA

2) **Hazard structuring**

- Sort & structure identified hazards (vs causes & consequences)
- Traceability

=> Outputs: 46 summarized high-level hazards at the boundary of the ATM service provision

Safety Assessment – High-Level PSSA

1) Risk assessment

2) Mitigation identification

3) Mitigation feasibility

4) Risk re-assessment

⇒ Hazard analysis workshop

Safety Assessment – High-Level PSSA

Hazard analysis workshop: 1 group including

- Operational expert
- Technical expert
- Moderator
- Safety expert

(completion by a flight operational expert)

Safety Assessment – High-Level PSSA

- **Risk Classification Scheme** (RCS) used for the risk* assessment associated with each hazard

GREEN	well acceptable to the expert
YELLOW	at the boundary of what is acceptable to the expert
RED	not acceptable to the expert

Risk*: severity x frequency
of the potential effect of the hazards

Belgocontrol

Safety Assessment – High-Level PSSA

For each hazard:

- **Risk assessment**

  => Outputs: Classifications of the risks (RED, YELLOW, GREEN)

- **Mitigations identification** for RED (required)
  for YELLOW (recom.)

  => Outputs: Safety requirements (required & recommended)

Safety Assessment – High-Level PSSA

- **Mitigation feasibility**

  => Outputs: statements on the feasibility of the proposed mitigations

- **Risk re-assessment**

  => Outputs: new classifications of the risks (RED, YELLOW, GREEN)

Safety Assessment - Results

ATM component: Information management

- Common information sharing and management (4D trajectory management)
- SWIM
- Improved weather forecasting and information sharing
- FAB Operations Plan

Summarized hazard	Risk and motivation	Potential remedy	Feasibility and new risk
H2.Data link issues (aircraft-ATC) a. aircraft system failure/outage b. ground system failure/outage c. information too early or too late d. data link capacity overload e. interference because of quantity of Mode S interrogations f. undetected corrupted data g. usage of data link for time-critical messages, (potential for failures, and for slower or wrong pilot reaction)	a) One aircraft is annoying, but can be managed like for R/T failure today. b) Much information has to be transmitted via R/T, with a potential for overload, in particular the first 15 minutes (after this, traffic has been restricted). Urgent messages may take more time because of R/T overload. c) For late messages it is no problem, as there is R/T. Sending a message too early could however lead to conflicts (e.g. flight level change). d/e) Unlikely to occur. If it occurs, some messages will arrive too late or not at all. Fall back to R/T. For downlink of information there is no change in risk. f) This is unlikely to occur undetected due to protocols (*extended CRC*). g) *Datalink is not intended to be used for time-critical messages under normal conditions*.	b) • Redundant systems like for voice. • Training of controllers to cope with unusual situations. c) • HMI design preventing messages being sent too early. • Controller training to prevent messages being sent too early. • Introduction of ASAS	Most remedies are feasible (for ASAS this is aircraft dependent). Remedies effective in reducing the risk.

Safety Assessment - Results

ATM component: Information management

- Common information sharing and management (4D trajectory management)
- SWIM
- Improved weather forecasting and information sharing
- FAB Operations Plan

Summarized hazard	Risk and motivation	Potential remedy	Feasibility and new risk
H5. Interoperability issues Procedures, equipment (e.g., communication), working methods incompatible with a. adjacent non FAB EC centre b. ICAO, IATA, ... c. local airports, airlines, ...	There is no real difference compared to today's operation, as now there are different centres, airports as well. With largely common procedures, working methods, etc. it will become easier to agree on letters of agreement. This reduces the potential for incompatibility compared to today. Different aircraft equipment from different brands can form an issue, as there is no standardisation.	Issuing a standard for aircraft equipment.	Not feasible, as the time needed for implementation is too long.

Safety Assessment – Results

- Assumptions were made during the safety assessment: to be considered as Safety requirements

#	Description of assumption.	Compo-nent	Related to
2.	Datalink has extended cyclic redundancy check (CRC).	IM	H2
3.	Datalink is not used for time-critical messages, unless an aircraft cannot reached via R/T.	IM	H2
4.	The HMIs of controllers and pilots prevent overload of information.	IM	H4
5.	The HMIs of controllers and pilots make sure that one is aware of having the most recent version of data or not.	IM	H4
6.	Actors will have more information about the weather.	IM	H7, H8

Safety Assessment - Results

- 5 safety issues
  requiring more R&D to be improved

1. Communication & surveillance problems with UAVs
2. Autonomous a/c operations
3. Communications problems regarding dynamic sectorisation
4. Interception of civil a/c with a communication failure by military jets
5. Emergency descents

Safety Assessment - Conclusion

- High-level Inputs: MOCs & ATM concept
- High-level Safety Assessment
  => High-level safety requirements
- No assurance FAB EC will be safer or not
- FAB EC can be safer if
  - ✓ All safety requirements are fulfilled
  - ✓ The 5 safety issues are solved

Plan of this presentation

- Introduction
- Safety Study
- Safety Methodology
- Safety Assessment
- Safety Assessment Validation
- Conclusion

S.A. Validation - Definition

- Terminology from SAM

- Evaluation : The objective is to demonstrate that the *safety assessment process meets its overall objectives and requirements*

- Evaluation in 3 stages :
  - Validation
  - Verification
  - Process Assurance

S.A. Validation - Definitions

- Validation: « getting the right output »

- Verification : « getting the output right »

- Process assurance : « getting the process right and the right process »

! overlap between these activities

Belgocontrol

S.A. Validation - Methodology

1) Review and analyze the S.A. activities documentation by means of checklists
2) Validation checklist : correctness and completeness
3) Verification checklist : documentation, traceability and credibility
4) Process assurance checklist : activity in respect of planned methodology
5) Evaluation report of the S.A.

S.A. Validation - Organization

- Validation Team

  Experts didn’t participate to the workshops

- Planning

  Activities in progress

  First draft of report: mid of March

Plan of this presentation

- Introduction
- Safety Study
- Safety Methodology
- Safety Assessment
- Safety Assessment Validation
- Conclusion

Conclusion

- No knowledge of adapted methodology
- No answer: *will the FAB EC be safer?*
- High-level Safety Assessment , inspired by SAM

⇒ High-level (generic) safety requirements

⇒ Safety Feasibility indication: could be safer

⇒ Safety update of the operational concept

Conclusion

- Results

Expert-based confidence that FAB EC can be safer

IF

- ✓ All safety requirements are fulfilled
- ✓ The 5 safety issues are solved

Conclusion

- Need

  ANSP methodology harmonization

- Next steps
  - Collect of safety methodologies
  - SWOT analysis
  - Best practices
  - Initial safety argument

Belgocontrol

Belgocontrol

Q&A