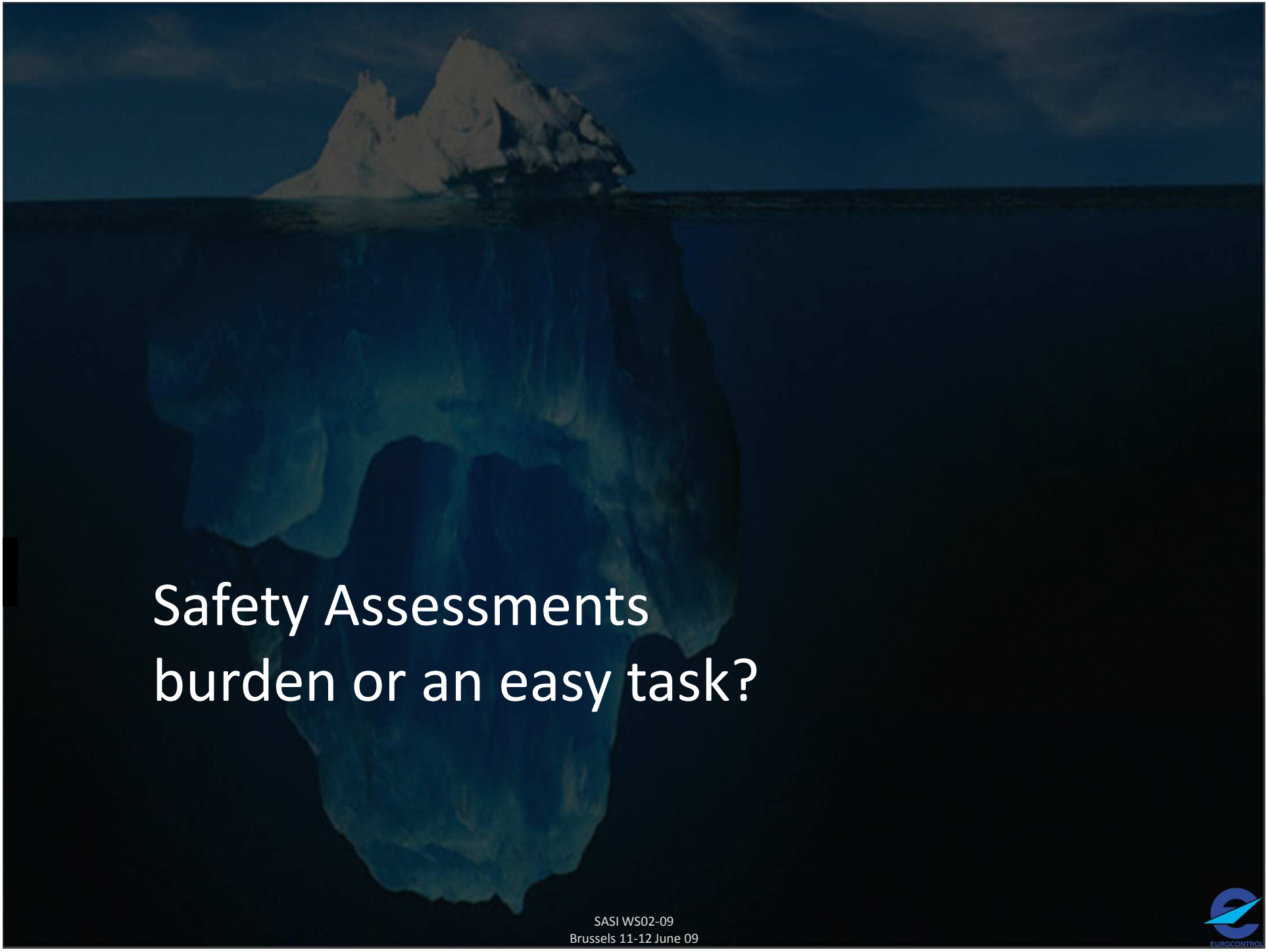
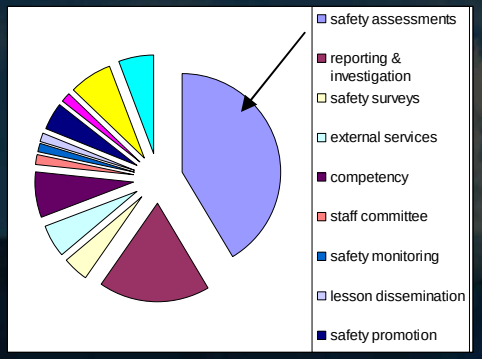
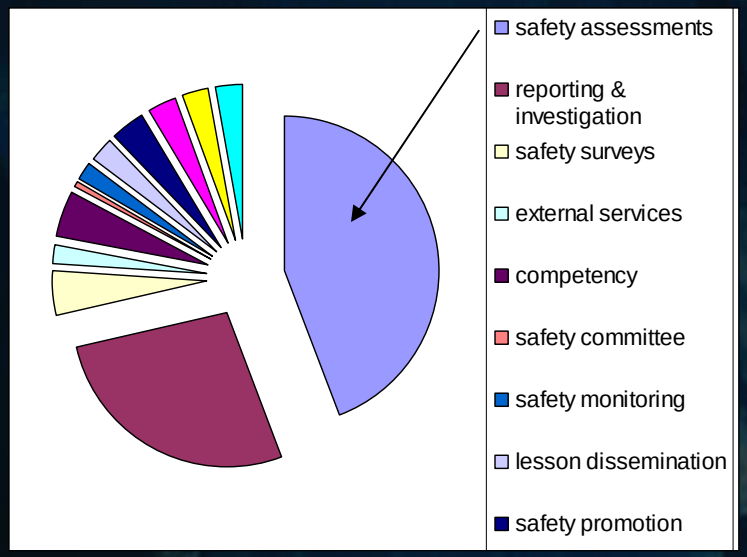
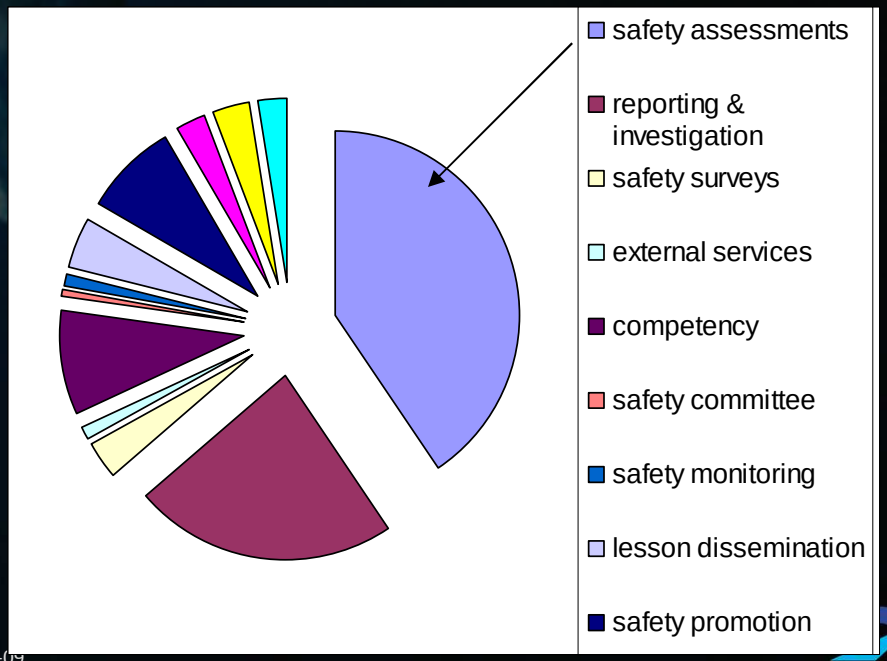


Safety Assessments burden or an easy task?

Most significant cost of an SMS







Methodologies

We are ALL still trying to find the best way forward

Corollary: RESULTS QUALITY?

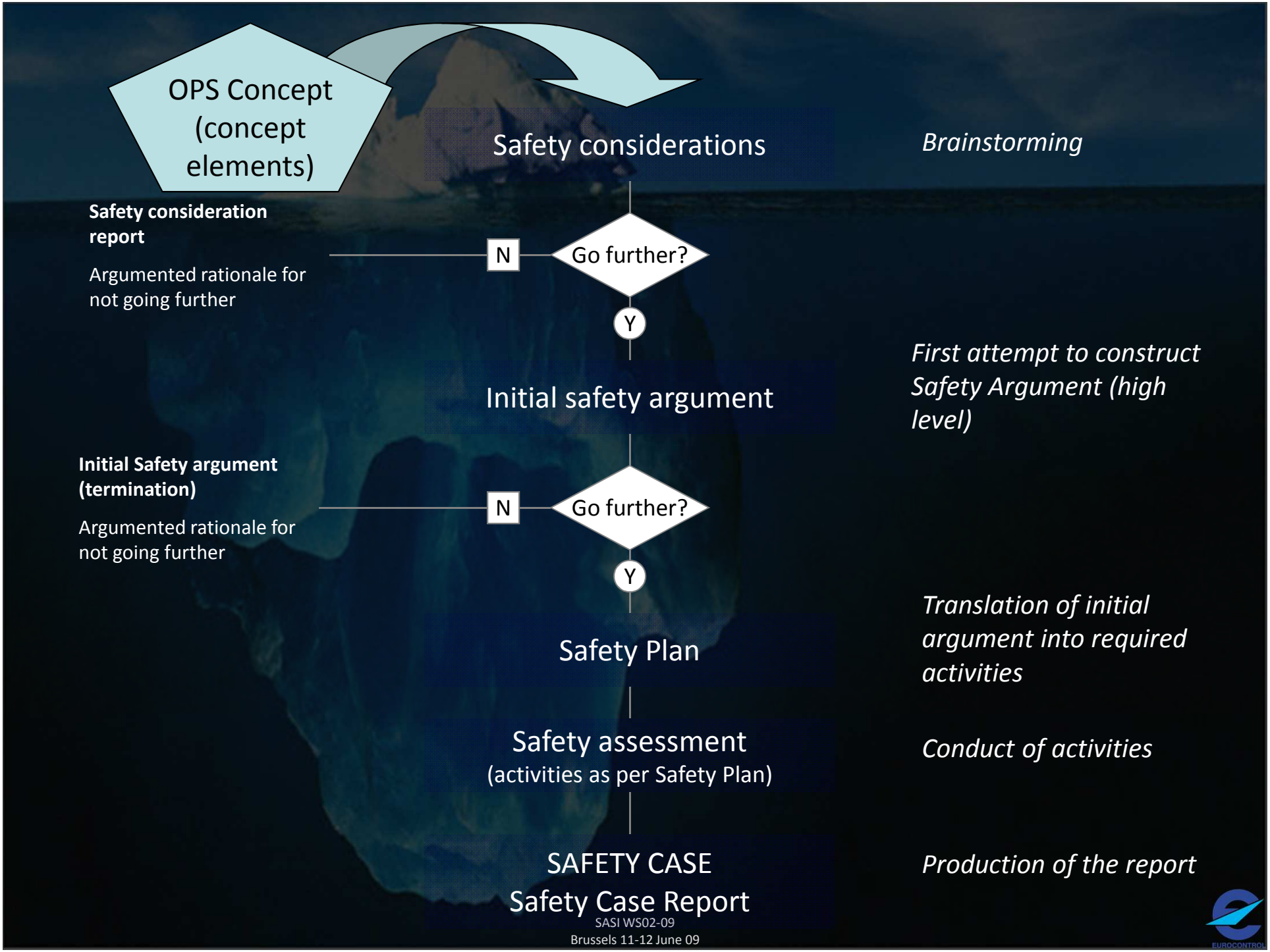
Huge documents but…..

- No operational concept
- Scope unclear
- Missing assumptions
- Safety requirements unrealistic
- Unclear usage of safety criteria
- Bad arguments
- Little or no evidence
- Errors in calculations
- No concept of operations
- Impact at boundaries not addressed
- Hazards classification questionable
- **SAFETY BENEFITS OF NORMAL OPERATIONS?**

Proposal for a response proportionate to the change

Its that a change or is that not a change?

- Non change (replacement by same spare part, same make, same model, same performance)
- Process based change (e.g. airways modification-ICAO)
- Procedure based change (RWY change, maintenance procedures…)
- Others? Hard to say…..


OPS Concept (concept elements)
Safety considerations
Brainstorming
Safety consideration report
Argumented rationale for not going further
N
Go further?
Y
First attempt to construct Safety Argument (high level)
Initial safety argument
Initial Safety argument (termination)
Argumented rationale for not going further
N
Go further?
Y
Translation of initial argument into required activities
Safety Plan
Safety assessment
(activities as per Safety Plan)
Conduct of activities
SAFETY CASE
Safety Case Report
Production of the report

Proposal for a response proportionate to the change

Practical example

Help the political authorities decide whether a highway circumnavigating a town should be built.

Needs a business case:

- Environment
- CBA
- Efficiency
- Security
- **Safety**

Proposal for a response proportionate to the change

Current “classical” way to address the issue is to go for a FHA

Highway function:
“To ensure a safe and orderly flow of traffic”

Hazards
H1: Highway totally unserviceable
H2: Highway partially unserviceable
H3: Highway corrupted

Proposal for a response proportionate to the change

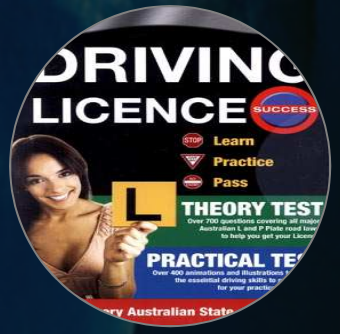
H1

- accident
- serious incident
- major incident
- significant incident
- no safety effect

Proposal for a response proportionate to the change

What does the FHA results tell decision makers?

The risk of an accident in case of H1, H2 or H3 are minimised thanks to the following mitigations:



Others…

Proposal for a response proportionate to the change

If you were a decision maker wouldn't you miss something?

In fact three things are missing:

-risk of an accident when highway serviceable and not corrupted

-safety impact on road network it is connected to

AND

-safety benefits in comparison to existing road network

Proposal for a response proportionate to the change

Risk of an accident when highway not blocked and not corrupted
Review operational concept & concept of operation

-list the conditions that must be fulfilled for the concept to work as specified (highway design adequate to speed, adequate to environment, type of traffic, cars circulating same direction, speed limits, usage of lanes, usage of emergency lanes, overtaking procedures etc…)

for each condition assess the consequence of this condition not being fulfilled (car wrong direction…)

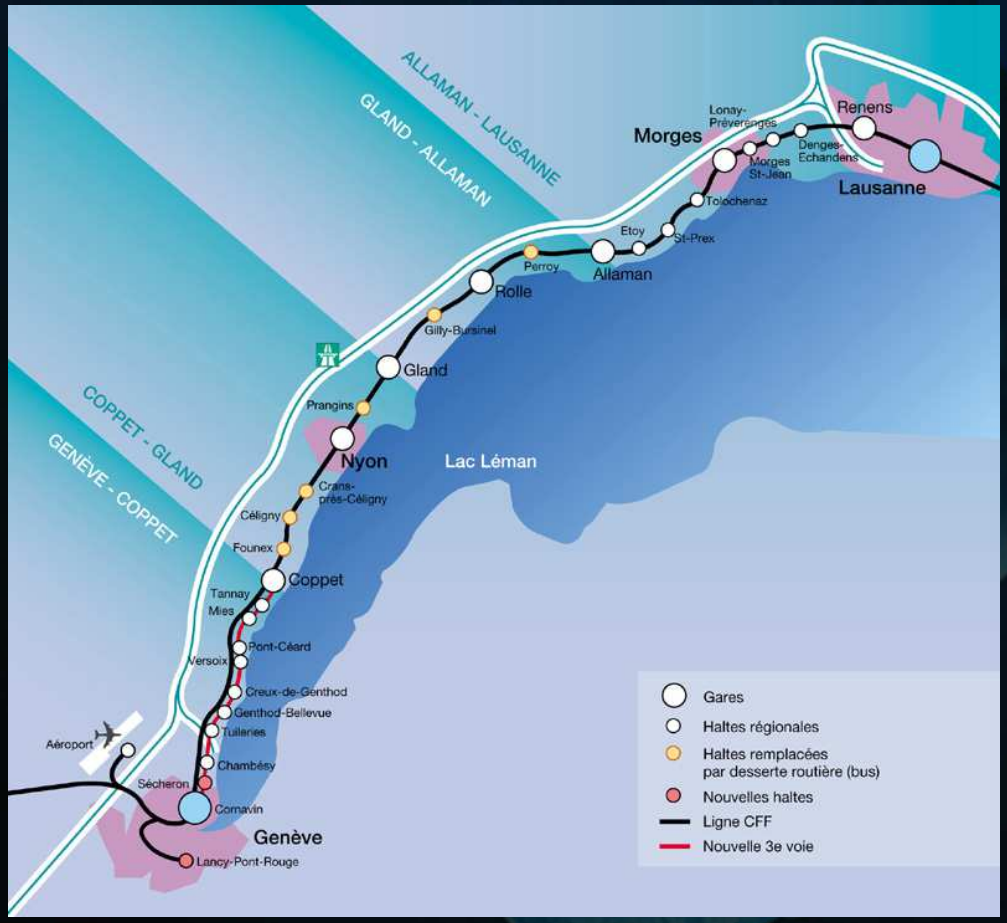
-introduce mitigations as required (signs and marking to prevent wrong entry, radio network warning, signs warning message, slow down & drive on right lane, drivers training etc…)

Proposal for a response proportionate to the change

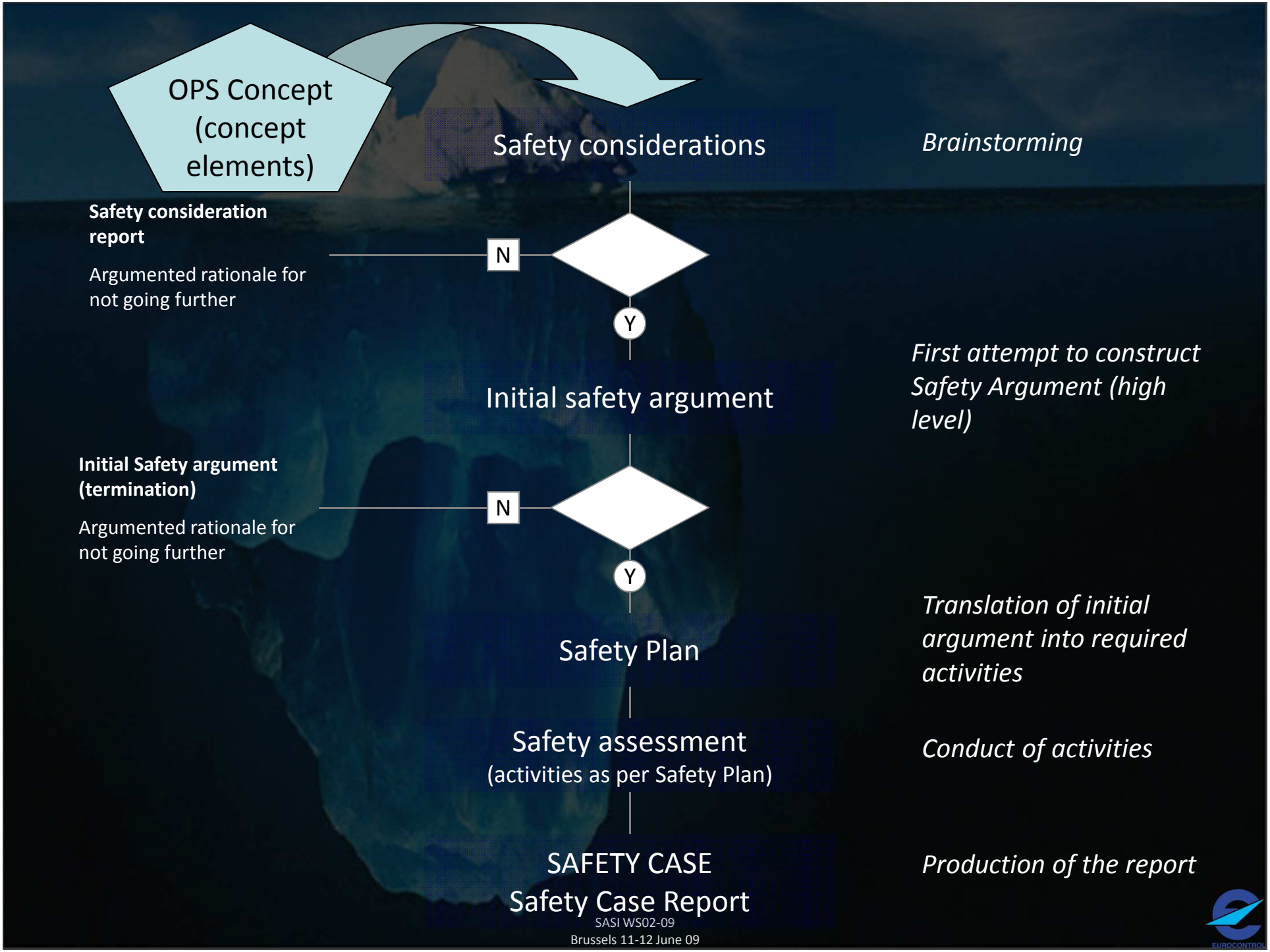
Safety impact on road network it is connected to

Identify interfaces and evaluate impact (connecting to the road network, e.g. are traffic capacities comparable?)

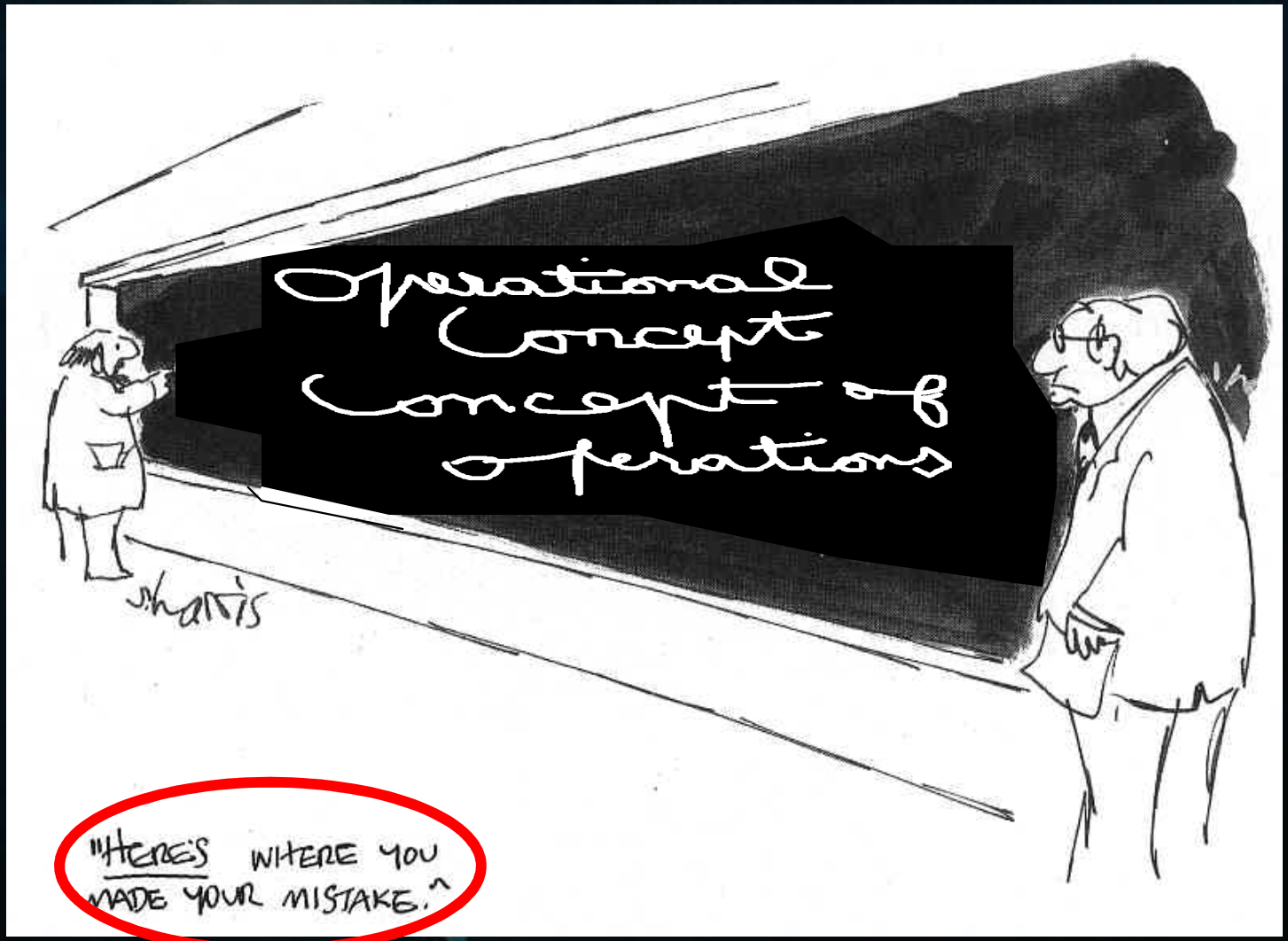
Safety benefits in comparison to existing road network



More than 25 villages, small towns avoided says enough to realise that the chances to avoid that will follow are significant……


OPS Concept (concept elements)
Safety considerations
Brainstorming
Safety consideration report
Argumented rationale for not going further
N
Y
Initial safety argument
First attempt to construct Safety Argument (high level)
Initial Safety argument (termination)
Argumented rationale for not going further
N
Y
Safety Plan
Translation of initial argument into required activities
Safety assessment
(activities as per Safety Plan)
Conduct of activities
SAFETY CASE
Safety Case Report
Production of the report

First principle
Take safety on board from the start….



Safety considerations process

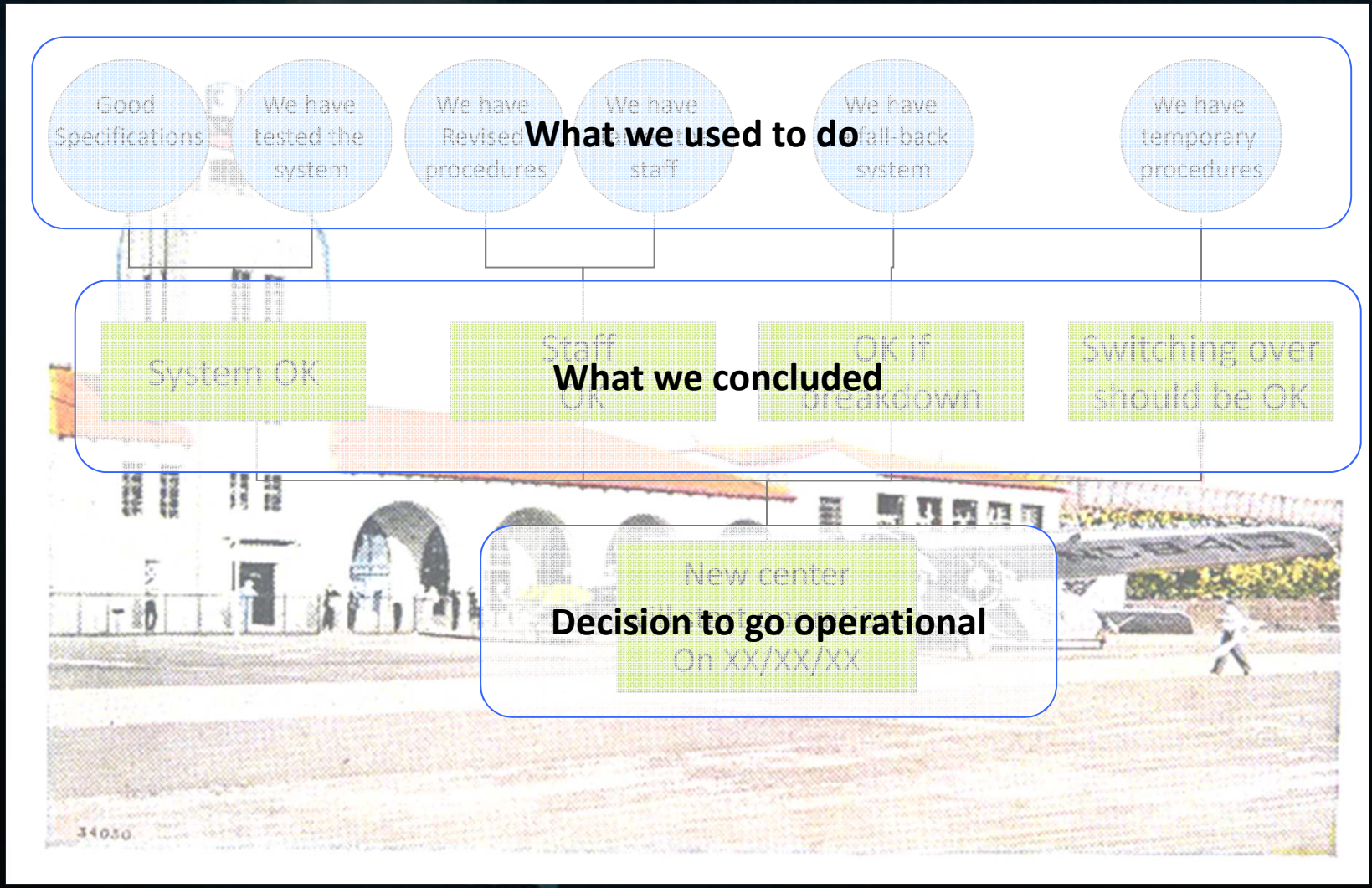
Safety considerations

Non change (replacement by same spare part same make, same model, same performance)	*Is this a change? I.e. elements added or taken out from existing system be it equipment, procedures or human related?*
Process based change (e.g. airways modification-ICAO)	*If not should there be one?*
Procedure based change (RWY change, maintenance procedures…)	*If not should there be one?*
Others?	*If answer yes to 1st question, and no to the two following ones go to next page* *If answer is yes to first question and yes to one of the following ones then prepare the process or procedure and assess it.* *If answer is not to first question write the safety considerations report with argumented rationale for not conducting an assessment*

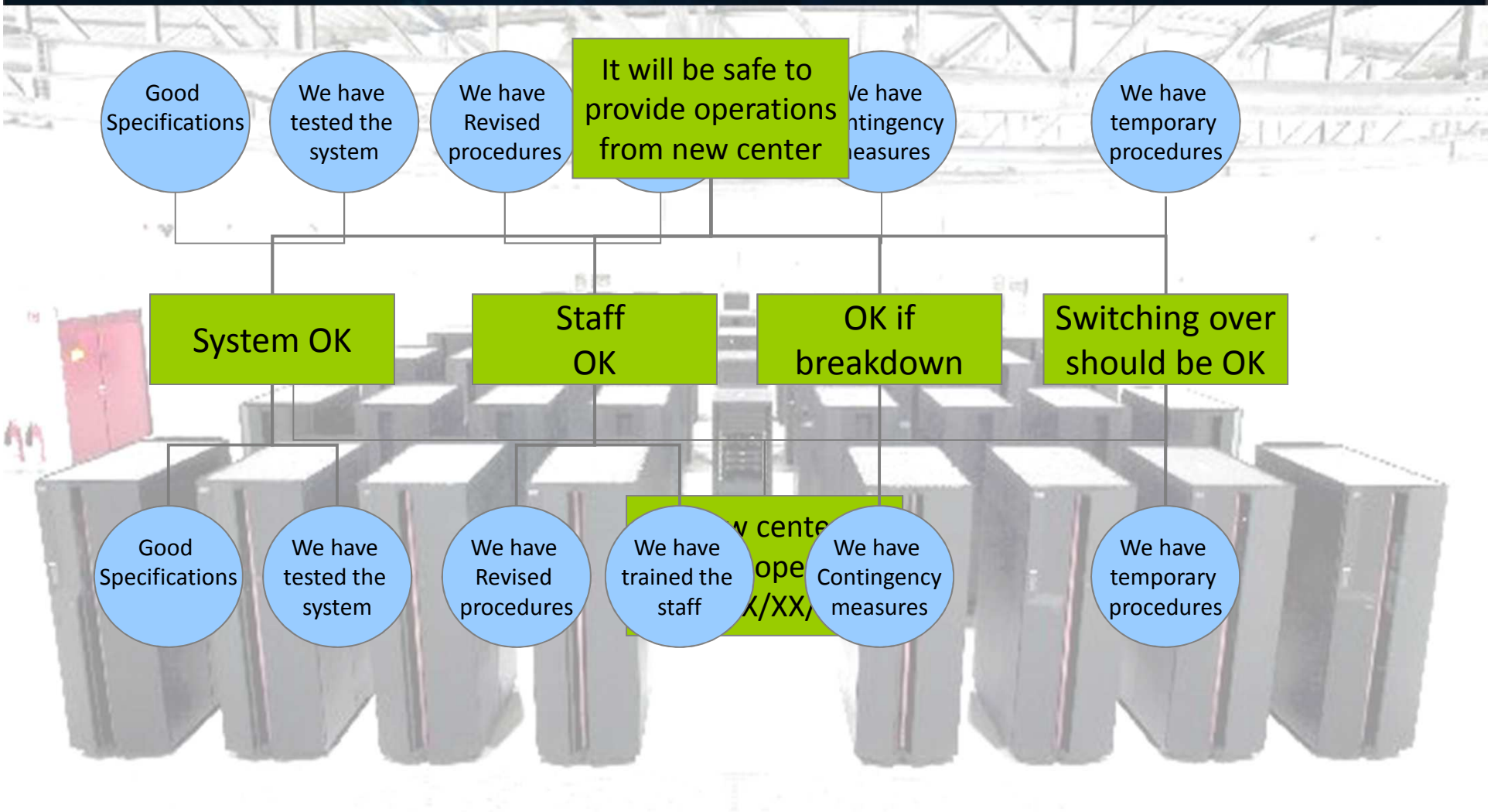
Safety considerations

No operational concept	*What are the needs for change?*
Scope unclear	*What are the new system boundaries? (OPS Concept)*
Missing assumptions	*Are there (initial) assumptions? (OPS Concept)*
Safety requirements unrealistic	*Are (Initial) Safety requirements realistic?*
Bad arguments	*Will it be possible to build an argument?*
Little or no evidence	*What evidence could be provided?*
Errors in calculations	*Would it feasible and beneficial to quantify?*
No concept of operations	*How shall the new system/change be operated?*
Impact at boundaries not addressed	*What are the interfaces? What impact foreseeable?*
Hazards classification questionable	*How and who will assess hazards?*
SAFETY BENEFITS OF NORMAL OPERATIONS?	***In what way is the proposed operational concept different from current one?***

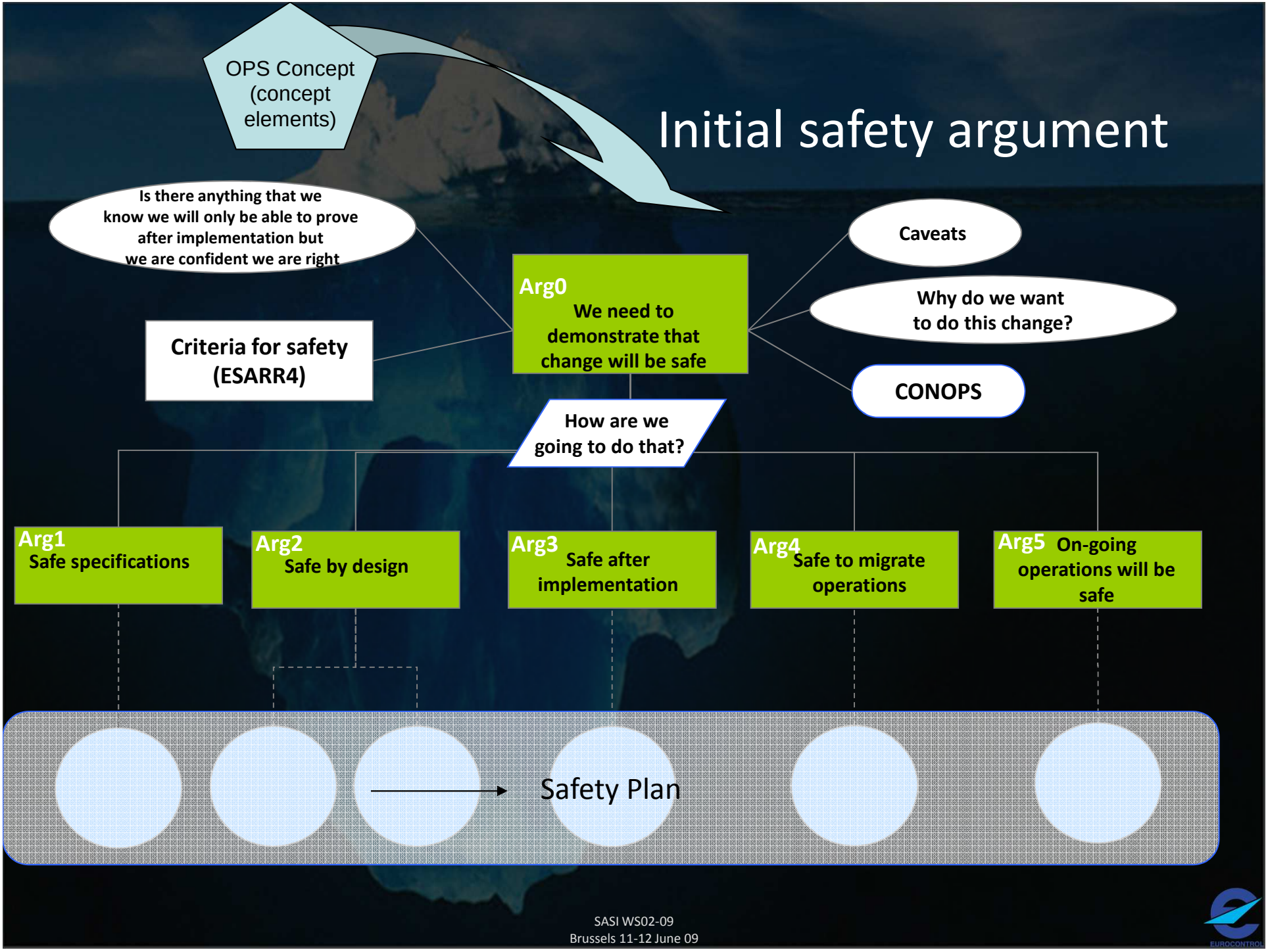
How did we do things so far?



What are we asked to do today?



Initial safety argument

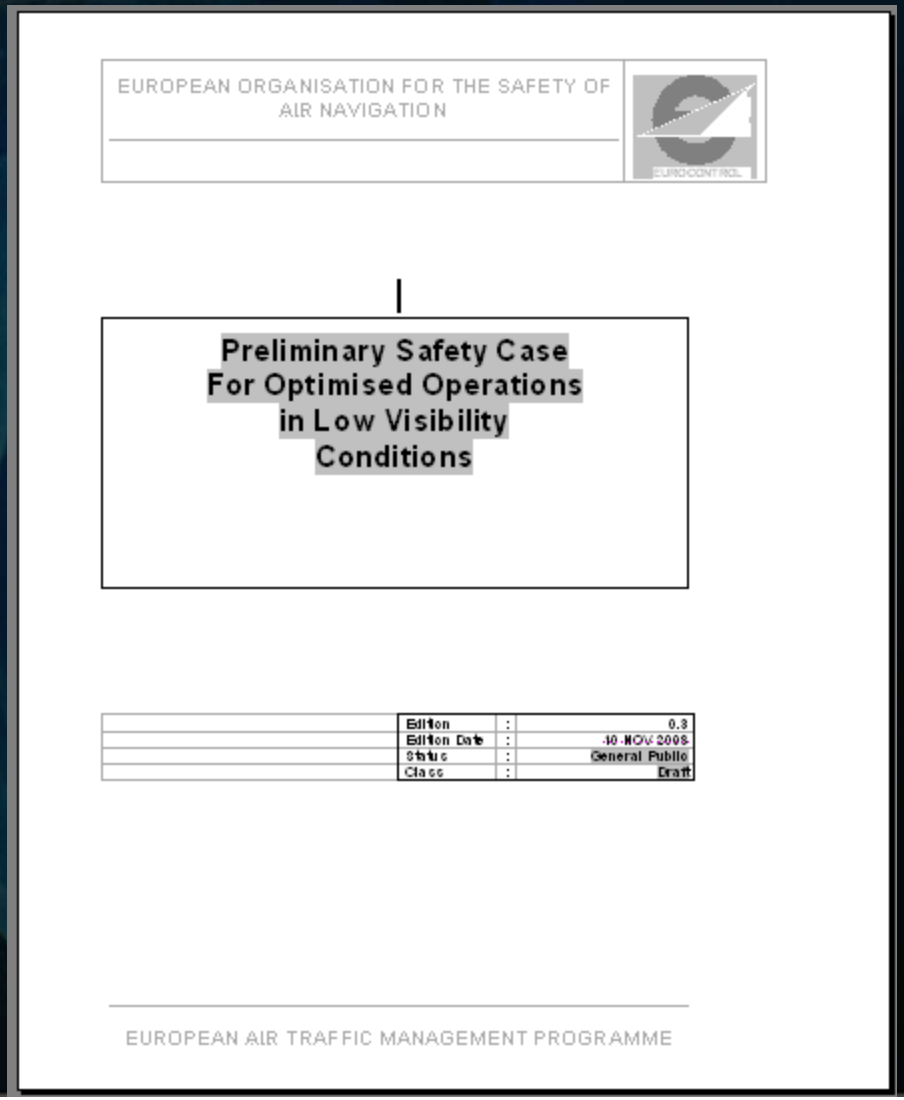


Safety Plan

System Life Cycle Phase: System Definition		Ref: EUROCONTROL SAM FHA Guidance Material				
Ref:	STCA Requirement	Assurance Activity	Evidence	Criteria for Success	Responsibility	Documentation
7.1.1 [Arg 0]	STCA will provide a substantive safety benefit in ATM operations	Show by comparison of ATM safety performance data with and without STCA Determine % of conflicts alerted with warning time of 30 seconds or more..	ATM safety performance data Results of analysis	X% of eligible conflicts alerted of which Y% have a warning time of 30 seconds or more.	L: ANSP Management D: ANSP Management C: Incident data base and other ANSPS I: Safety Manager	Documented safety performance data.
7.1.2 [Context 01]	Clear and unambiguous policy regarding use of STCA	Confirm by review that policy exists and that it is consistent with NSA regulatory requirements and EUROCONTROL specification	Written Policy Results from review	Published Policy endorsed by ANSP management and where necessary, the NSA Regulator.	L: ANSP Management D: ANSP Management C: NSAr I: Safety Manager	Documented and included in safety case
7.1.3 [Context 02]	Concept of operation, consistent with declared policy	Confirm by review that the concept of operation exists and that it is consistent ANSP policy for STCA. Confirm that it was developed in concert with operational staff and agreed with them	Written concept. Results from review	Documented concept of operation endorsed by ANSP management and where necessary, the NSA Regulator. No inconsistencies noted compared to policy.	L: ANSP Management D: ANSP Management C: NSA I: Safety Manager	Documented and included in safety case
7.1.4 [Arg 1.1]	Assumptions about system boundaries and operational environment defined	Confirm by review that assumptions are feasible for the planned system	Written assumptions Results from review	Documented assumptions confirmed by ATC and engineering as appropriate.	L: ANSP Management D: ANSP Management C: Operations Managers I: Safety Manager	Documented and included in safety case
7.1.5 [Arg 1.2]	STCA Functional & Performance requirements specified.	Confirm by review that the requirements are complete and correct, consistent with the concept of operation and compatible with the EUROCONTROL Specification.	Written specification Results from review Compliance Matrix	Compatible with EUROCONTROL Specification. Achievable.	L: ANSP Management D: ANSP Management C: Operations Managers & NSA I: Safety Manager	Documented and referenced in safety case
7.1.6 [Arg 1.3]	HMI requirements specified	Confirm by review that the requirements are feasible and compatible with the intended operational environment	Written requirements Review findings.	Acceptable to Controllers	L: ANSP Management D: ANSP Management C: HF Expert I: Safety Manager	Documented and referenced in safety case

TABLE 7.1 STRATEGY FOR ASSURANCE – SYSTEM DEFINITION

SAFETY CASE
Safety Case Report

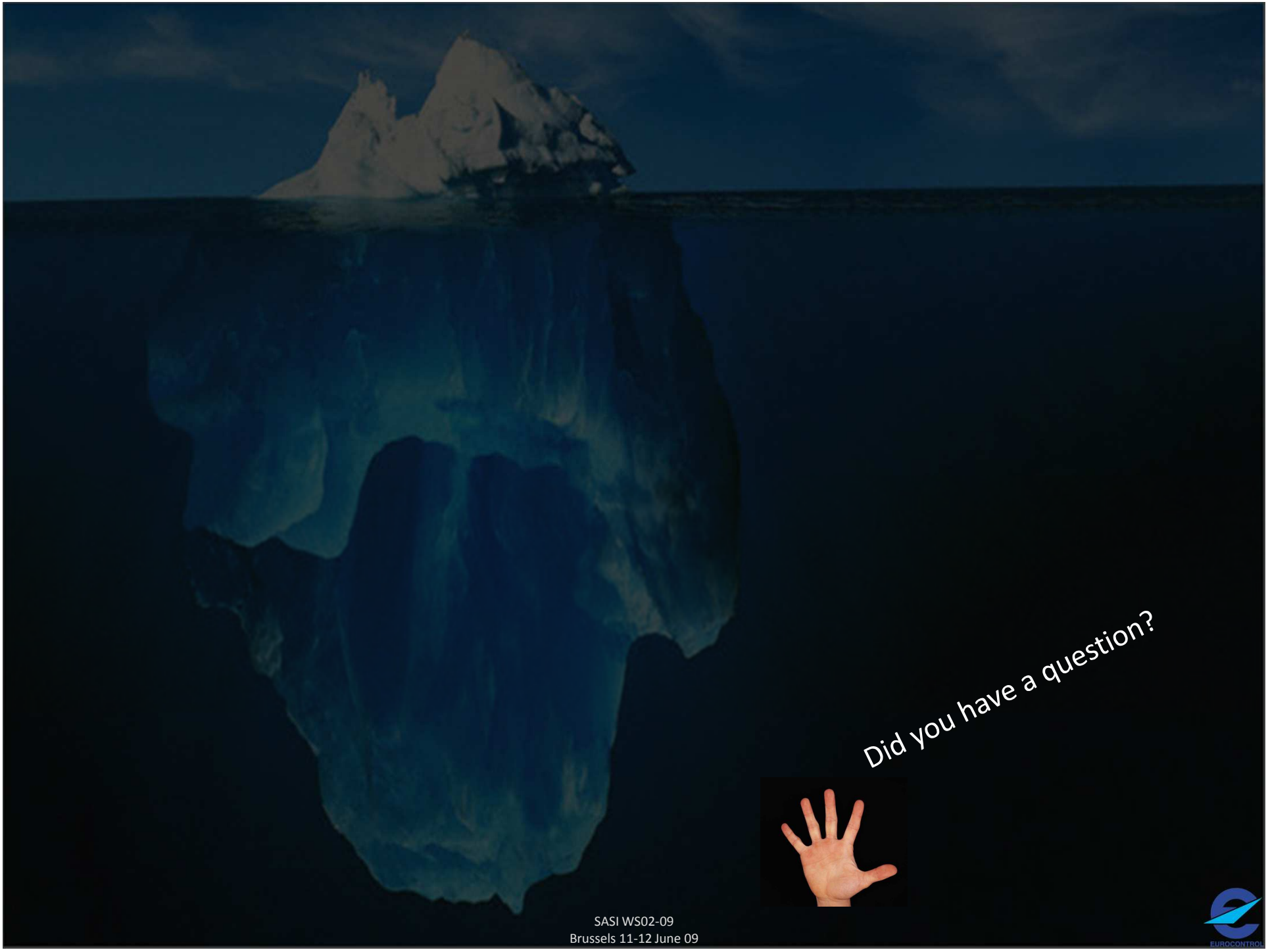


EUROPEAN ORGANISATION FOR THE SAFETY OF AIR NAVIGATION

Preliminary Safety Case For Optimised Operations in Low Visibility Conditions

Edition	:	0.3
Edition Date	:	10-NOV-2008
Status	:	General Public
Class	:	Draft

EUROPEAN AIR TRAFFIC MANAGEMENT PROGRAMME


Did you have a question?