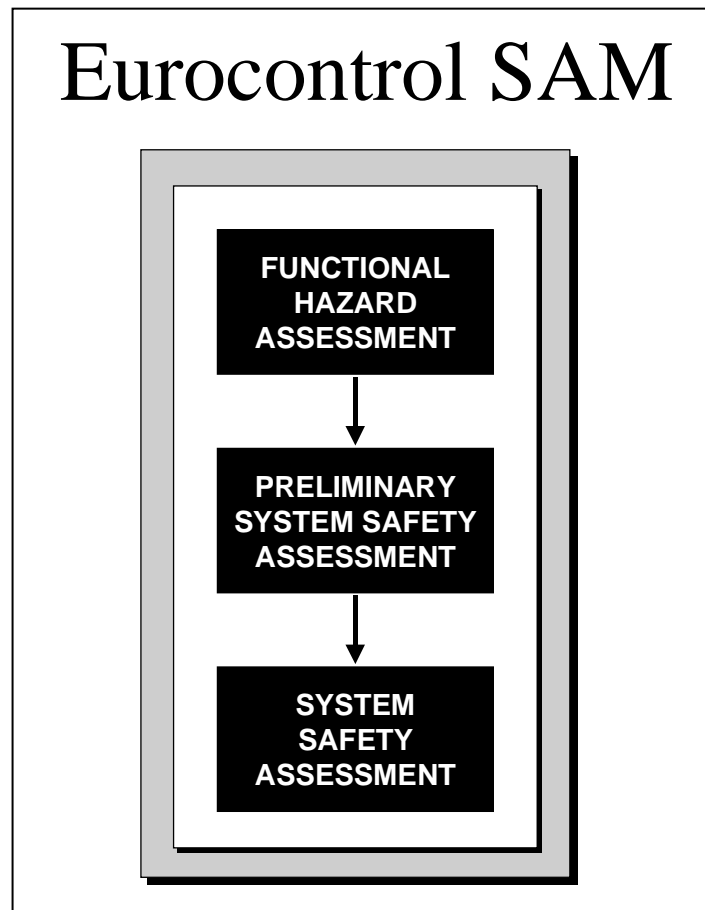
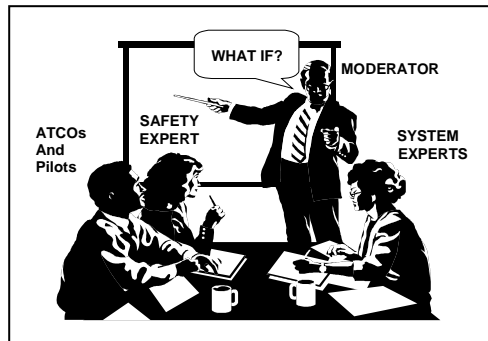
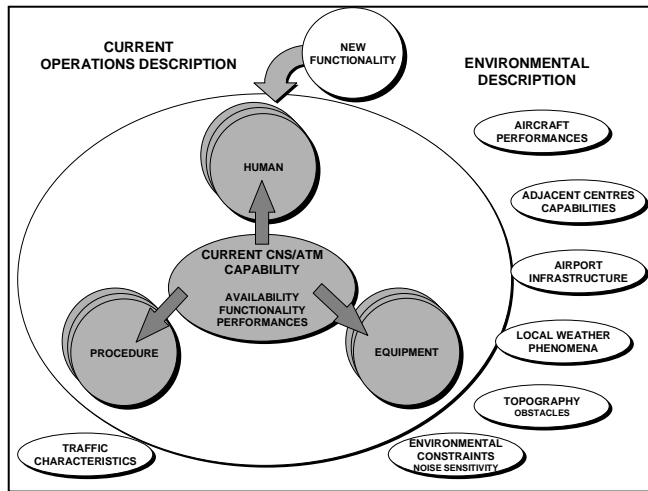

Operational Risk Assessment for Airspace Planning

The SAM Methodology



Limitation of the FHA



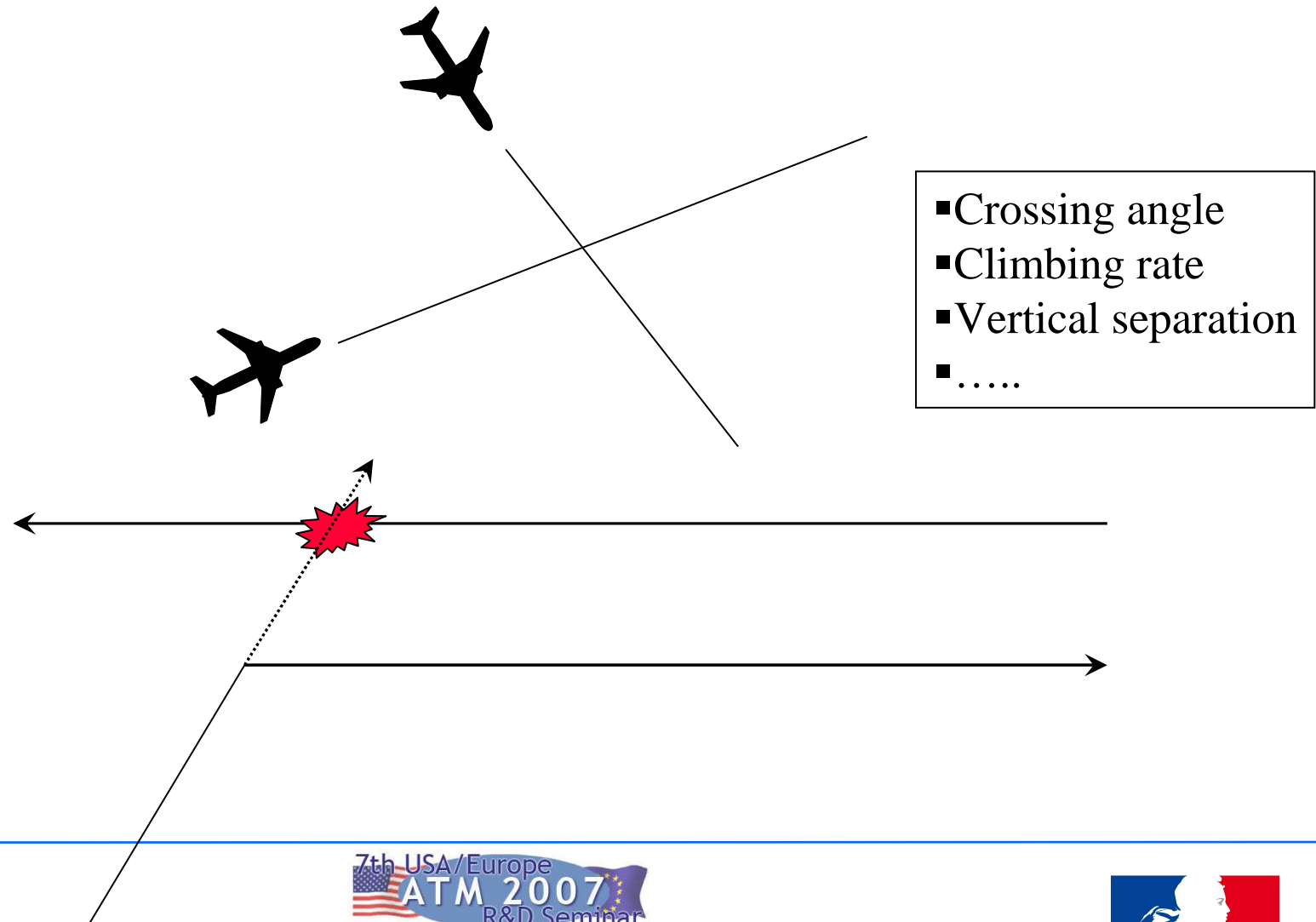
Safety objectives

Non RVSM approved aircraft indicated as RVSM approved	Flight crew recognises and notifies ATC of aircraft non RVSM status	No other aircraft in horizontal overlap	Other aircraft is RVSM approved	No vertical overlap with other aircraft	Consequence	Frequency
w=3.51e-4 Page 3	Q=1.00e-1	Q=1.00e-3	Q=1.50e-4	Q=1.00e-3		3.51e-4
Success: Notifies	Null	Null	Null		ATC apply 2000ft separation and clear aircraft out of RVSM airspace	3.16e-4
Failure: Does not notify	Success: No H overlap	Null	Null		Non RVSM approved aircraft passes through RVSM airspace unnoticed	3.51e-5
Failure: H overlap	Success: Approved	Failure: V overlap	Success: No V overlap		Non RVSM approved aircraft passes through RVSM airspace unnoticed	3.50e-8
	Failure: Non-approved	Null: V overlap	Failure: V overlap		Two aircraft in conflict (SC#1)	3.51e-11
			Failure: V overlap		Two aircraft in conflict (SC#1)	5.26e-12

Figure A.4: Hazard #5 - Risk Analysis

Context Dependant ?

Context associated to an operational hazard



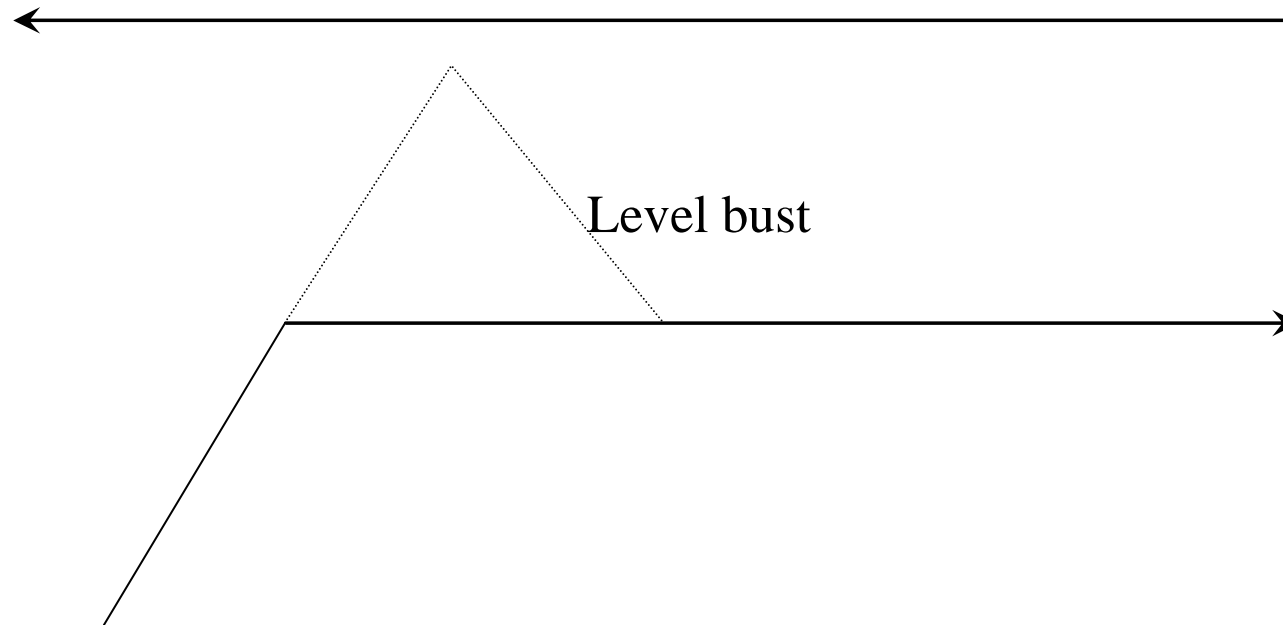
Limitation of the SSA

SSA versus FHA and PSSA

Life cycle phase FHA & PSSA	SSA-SAEC Process				
	System implementation & integration	Transfer to operations	Operation & maintenance	System Changes	Decommissioning
FHA-SOS - Hazard identification - Hazard Effects identification - Effects Severity classification - System Safety Objectives	Verification that system as implemented is able to meet its Safety Objectives Verification that risk is acceptable	- Verification of system as transferred to operation wrt Safety Objectives - Risk is acceptable - validation versus users expectations with respect to safety	- Data collection and monitoring of safety performances w.r.t. Safety Objectives and assumptions Ensure that risk is acceptable	Reiterate/update FHA.	Assess the safety impact on global ATC operations of the system withdrawing (during and after decommissioning)
PSSA-SRS -Functional breakdown -Refine sub-functions safety contribution -Evaluate system architectures -Apply Risk Mitigation Strategies -Apportion Safety Objectives into Safety Requirements to system elements	Verification that system elements (human, procedure and equipment) as implemented meet their Safety Requirements (including Assurance Levels)	Verification that system elements as transferred into operation meet their Safety Requirements (including Assurance Levels)	- Data collection and monitoring of safety performances w.r.t. Safety Requirements - Safety assessment of maintenance interventions	Reiterate/update PSSA	

Do reported incidents account for all «intermediate» errors?

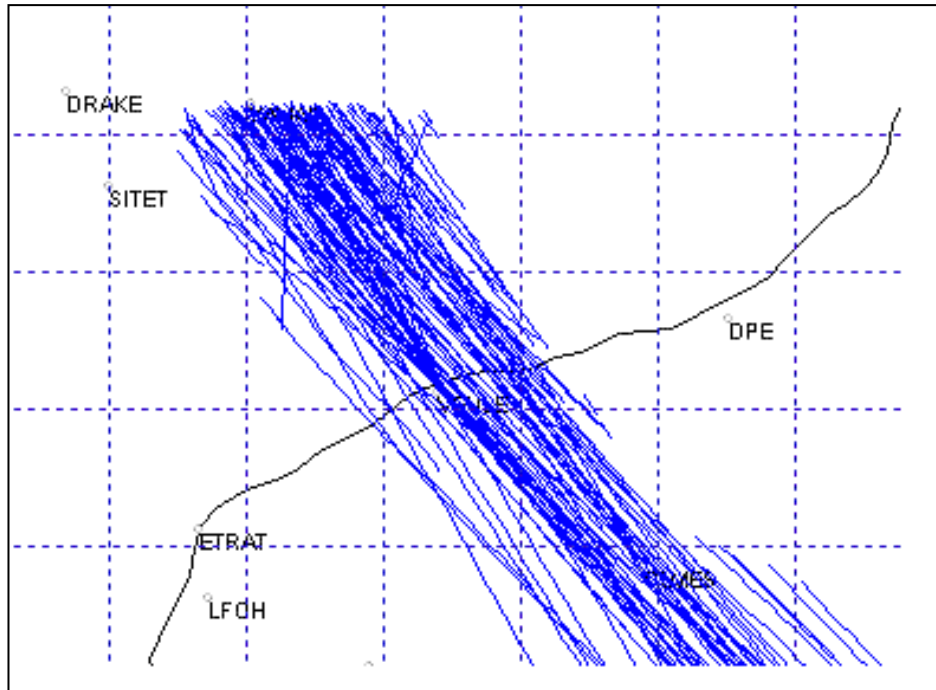
Example of undetected operational error



Part II

A methodology for operational risk assessment with radar surveillance

Specificity of radar surveillance (I)

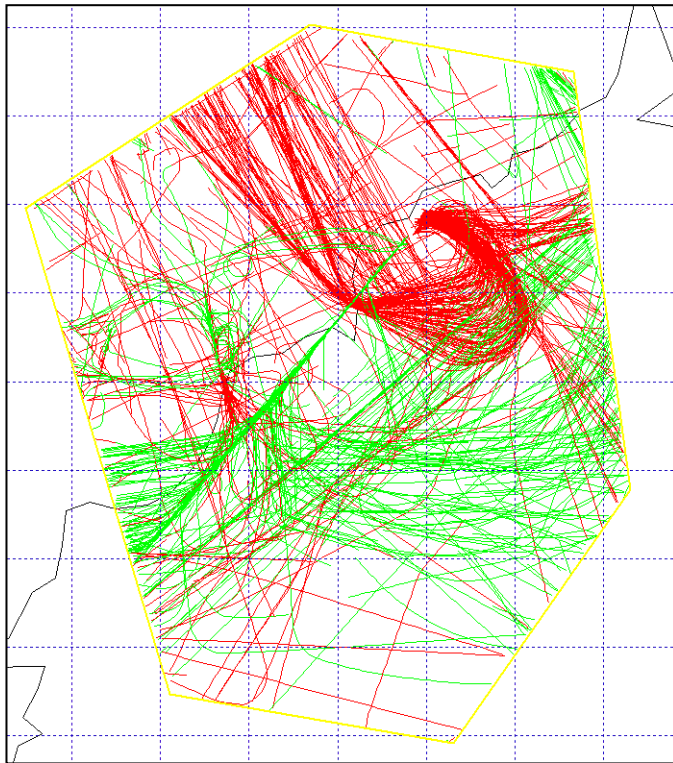


The concept of “assigned route” (with navigation error from this assigned route) is difficult to apply in continental airspace

Specificity of radar surveillance (II)

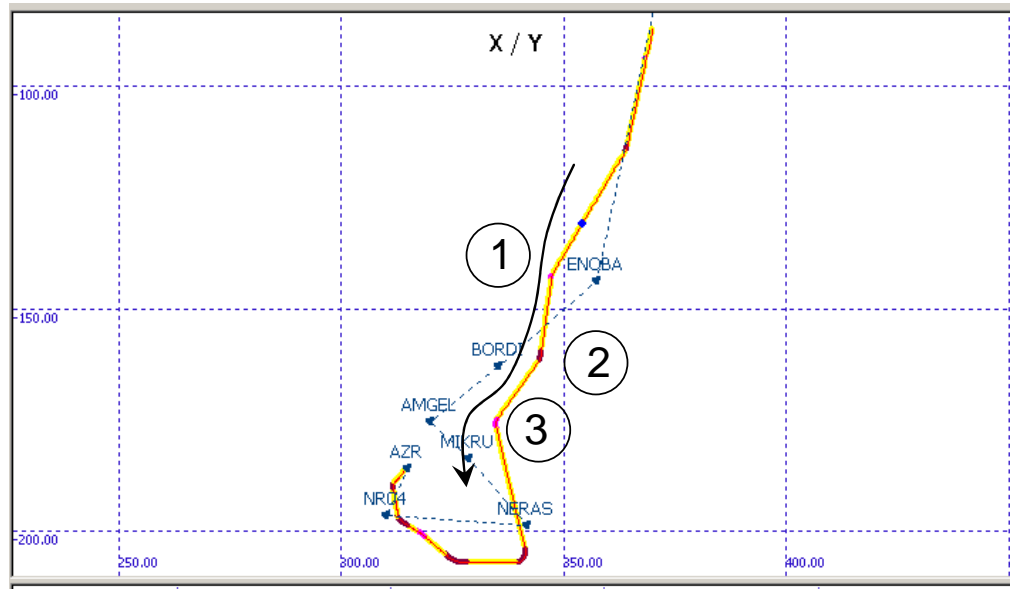
■ Descent

■ Climb



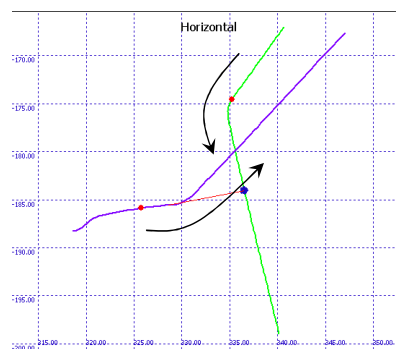
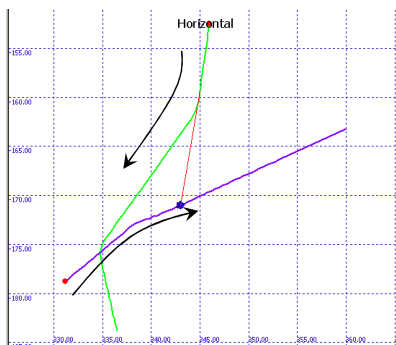
**The “straight line” assumption
does not always hold
(e.g. in TMA)**

Specificity of radar surveillance (III)



②

③



For horizontal manoeuvres, it is necessary to process flight plan in order to interpret the operational context

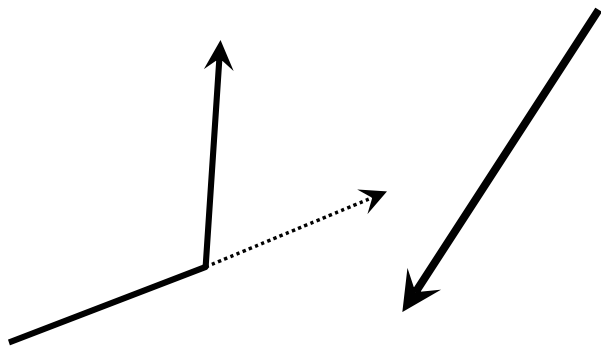
Analytical model

Modeling of operational errors

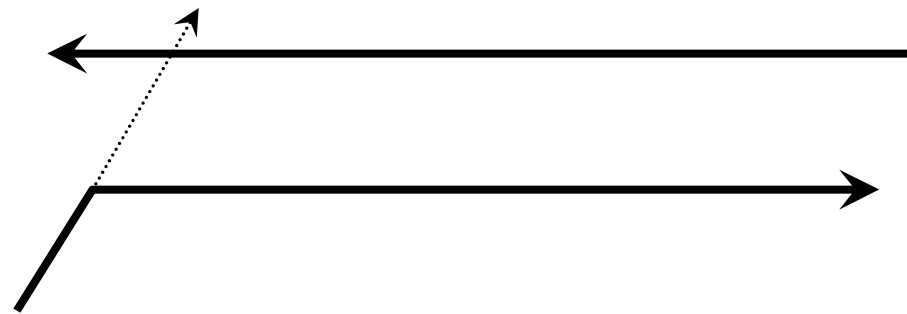
operational error:

any situation where the **controller's representation of the future trajectory** of an aircraft **does not correspond to the reality**

horizontal



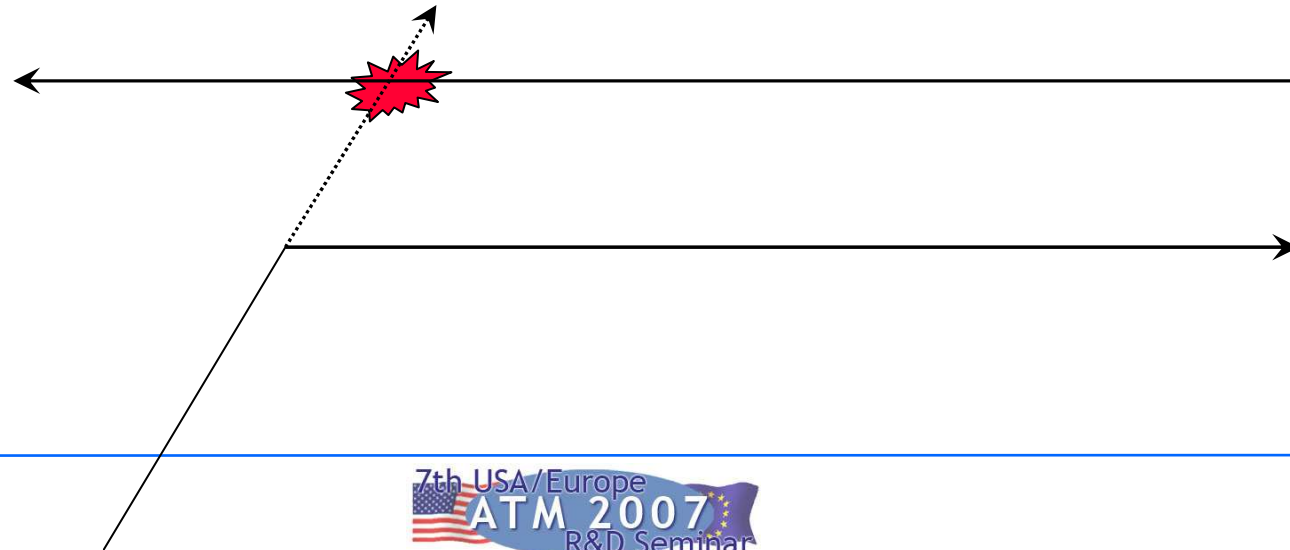
vertical



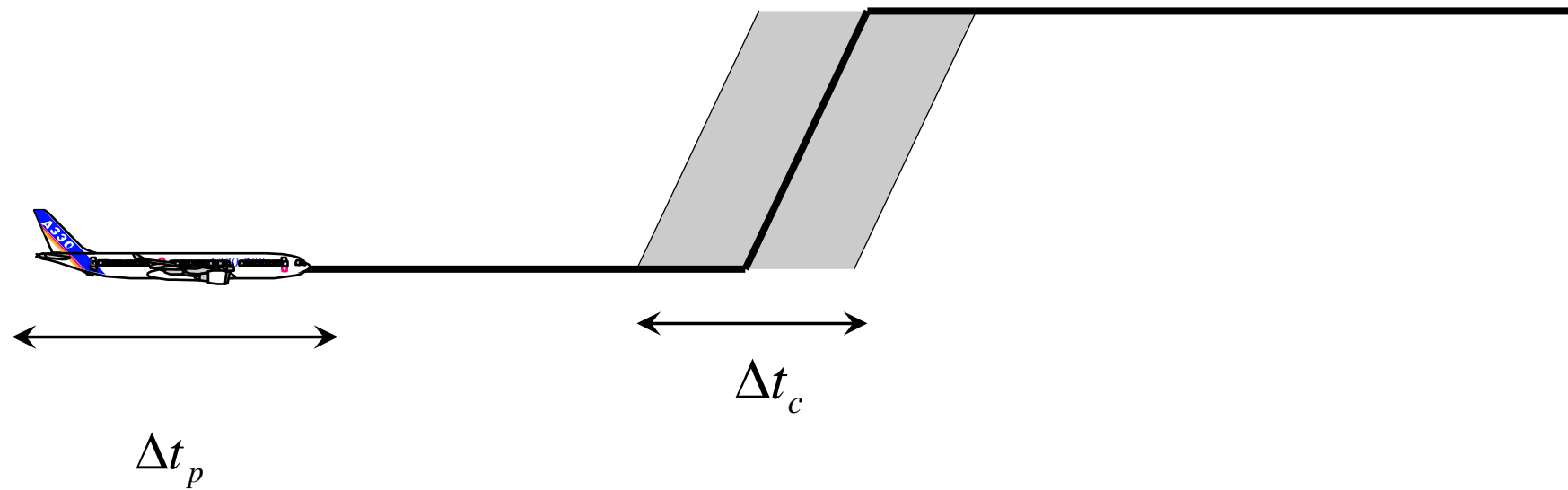
The “risk exposure” concept

Risk exposure associated to a scenario of operational error:

risk under the assumption that **whenever aircraft can fall into this scenario, they do.**



The “risk exposure” is time oriented



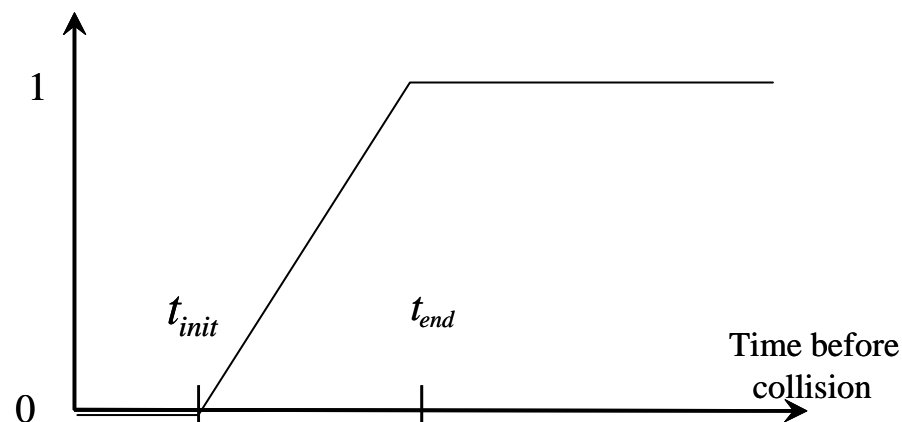
Modeling of controller's intervention

hazard rate

$$\lambda(t) = \lim_{dt \rightarrow 0} \frac{\Pr\{t + dt > T \geq t | T \geq t\}}{dt}$$

A conservative modelling for the detection delay is a **constant hazard rate**

Probability of solving



Beginning of operational error

Detection by the controller

Collision

Properties of the risk exposure concept

The risk exposure :

- ◆ Is estimated from radar archive data
- ◆ Returns all pairs likely to fall under an operational scenario
- ◆ Associate to all pairs a probability of incident/accident

Applications

Edition of encounters (I)

Current conflict parameters

Type de Conflit	FL	Fact coll
<input type="checkbox"/> VERT_DOWN	190.0	74.3
<input checked="" type="checkbox"/> VERT_DOWN	270.0	49.6
<input type="checkbox"/> VERT_DOWN	200.0	52.4
<input type="checkbox"/> VERT_DOWN	6.0	64.8
<input type="checkbox"/> VERT_DOWN	240.0	60.1
<input type="checkbox"/> VERT_DOWN	120.0	78.5
<input type="checkbox"/> VERT_DOWN	100.0	100.5
<input type="checkbox"/> VERT_DOWN	190.0	43.6
<input type="checkbox"/> VERT_DOWN	260.0	63.7
<input type="checkbox"/> VERT_DOWN	80.0	102.2
<input type="checkbox"/> VERT_DOWN	210.0	27.1

Horizontal view

Vertical view

Current aircraft positions

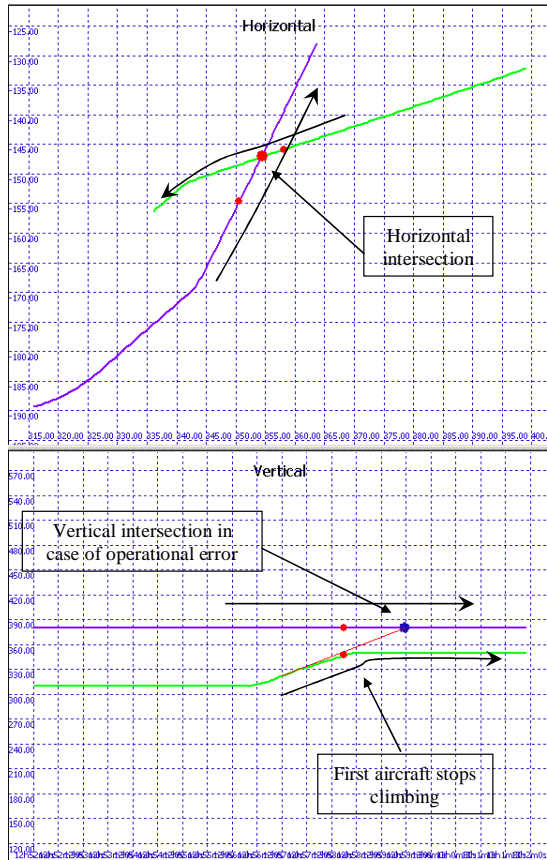
Displayed fields

Conflict fields to display

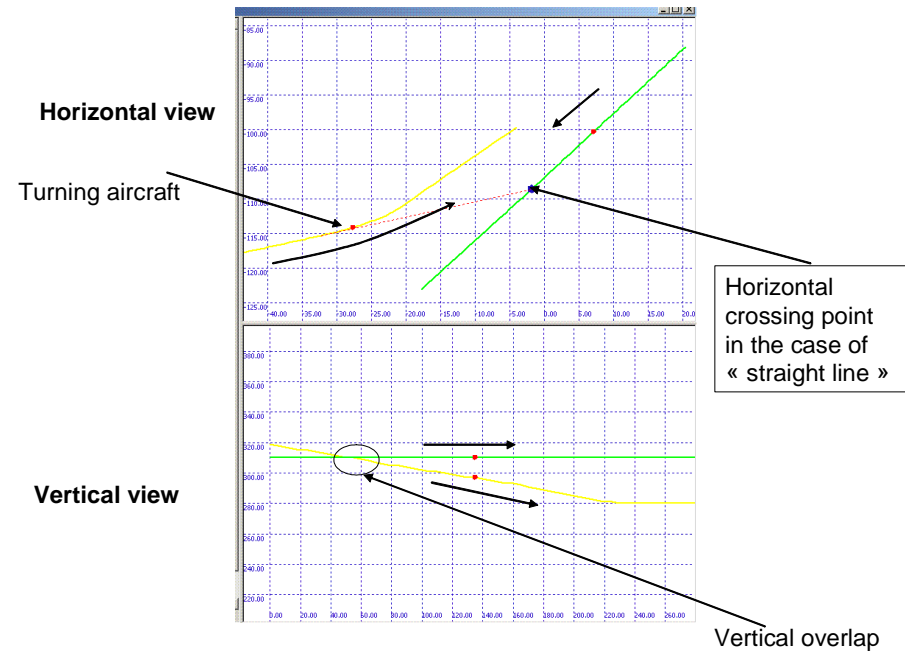
Time slider

Current flight parameters

Edition of encounters (II)

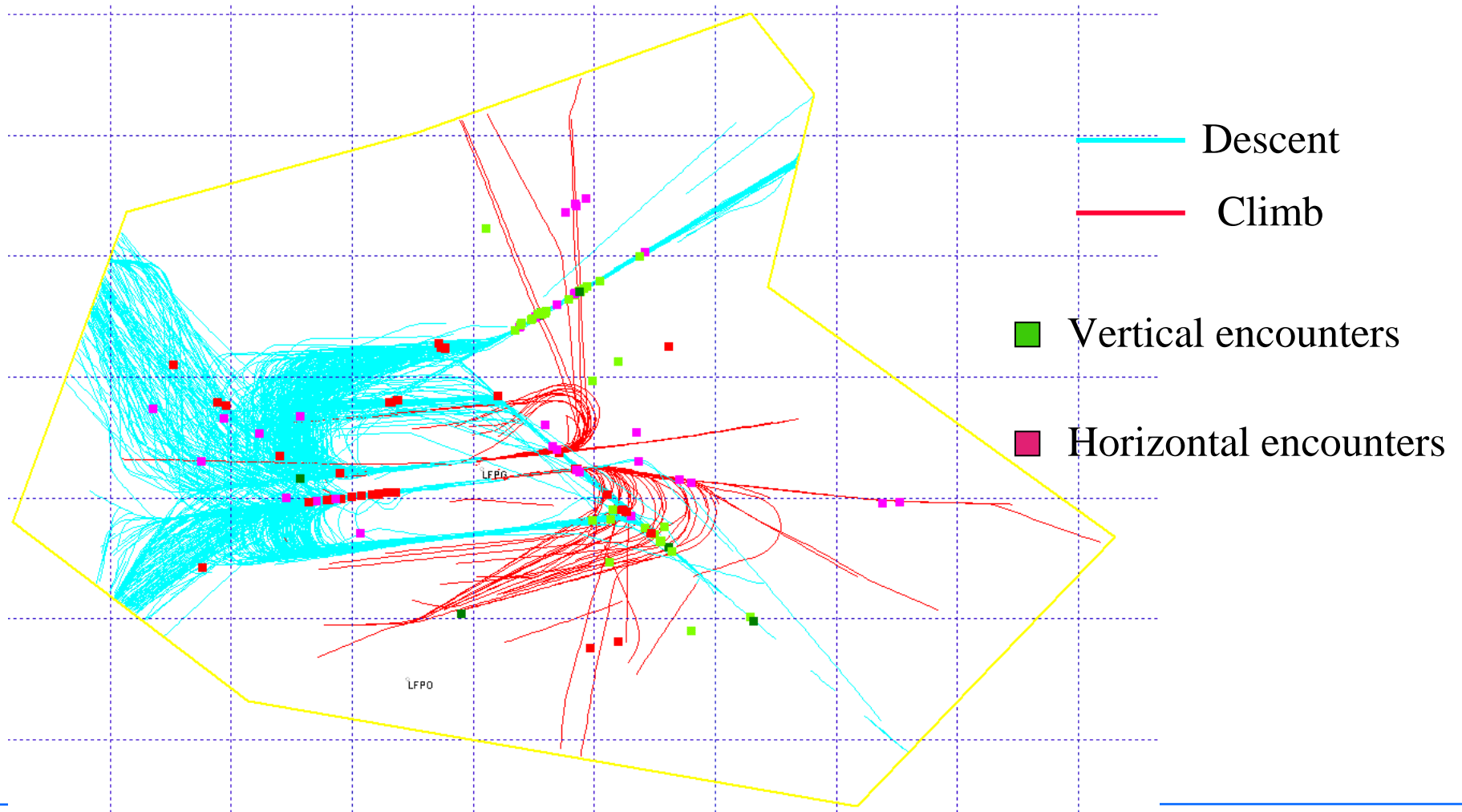


Vertical scenario



Horizontal scenario

Identification of operational risk



Risk estimation

