



NLR Air Transport Safety Institute

Research & Consultancy

# *Studying hazards for resilience modelling in ATM*

## *SESAR WP-E project: MAREA*

**Sybert Stroeve, Mariken Everdij, Henk Blom**

**SESAR Innovation Days, Toulouse, France,  
29 Nov – 1 Dec 2011**

SUPPORTED BY

**SESAR**

JOINT UNDERTAKING



# Contents

**Background and aim of MAREA**

**A generalized set of hazards in ATM**

**How humans deal with hazards in ATM**

**Hazard modelling for resilience analysis**

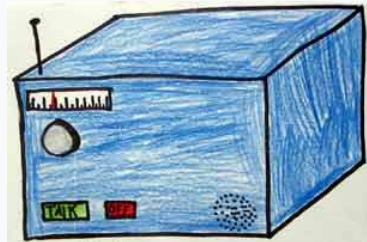
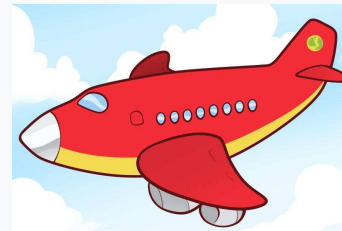
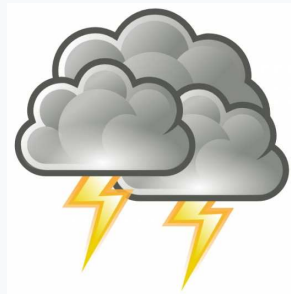
- What is covered?
- What is not covered?

**Conclusions and future research**

# Mastering the complex ATM system safely

## Complexity and performance variability in ATM

- Distributed human operators and technical systems
- Considerable interconnectivity between the agents
- Internal and external uncertainties and disturbances
- Human role is important to cope efficiently with uncertainties and disturbances



# Resilience Engineering

**Design of socio-technical systems that are able to resist a wide variety of demands, variations, degradations and disruptions**



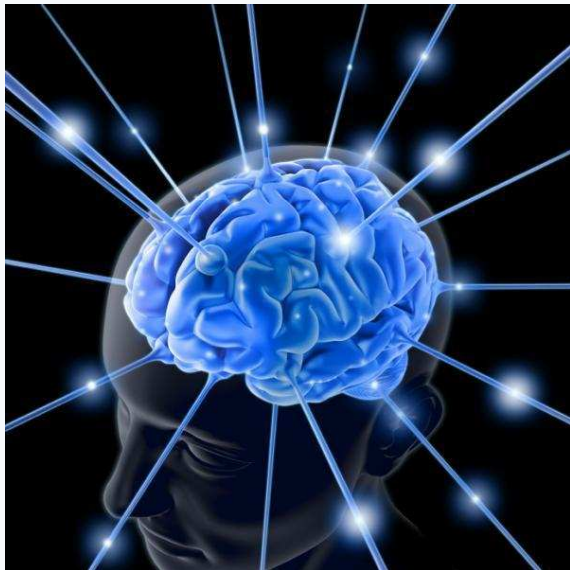
**Human flexibility and system oversight are essential**

- Away from error-thinking
- Towards a broad view on human performance in an overall system context

# Mathematical Approach towards Resilience Engineering in ATM (MAREA)

## Aim

To develop a mathematical modelling and analysis approach that allows to bring Resilience Engineering at work for the complex ATM system



## Focus on human performance

- Humans dealing with uncertainties and non-nominal conditions
- Psychological and organizational models

# MAREA research streams

- Development and validation of a mathematical modelling approach towards Resilience Engineering
- Analysis of SESAR 2020 scenarios using this mathematical modelling approach
- Evaluation of the novel approach versus other approaches and integration in the design cycle



University of L'Aquila

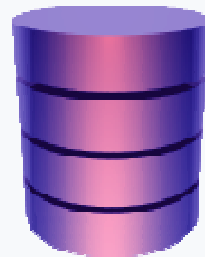
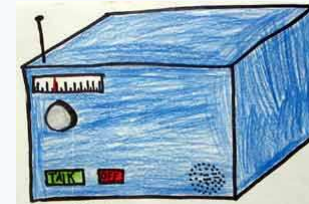
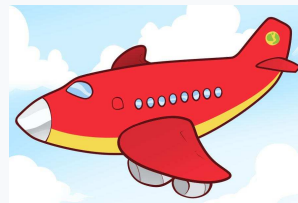
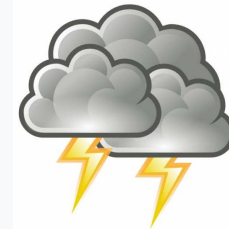
SUPPORTED BY  
**SESAR**  
JOINT UNDERTAKING



# Identification of hazards

**Hazard = “Anything that may influence safety”**

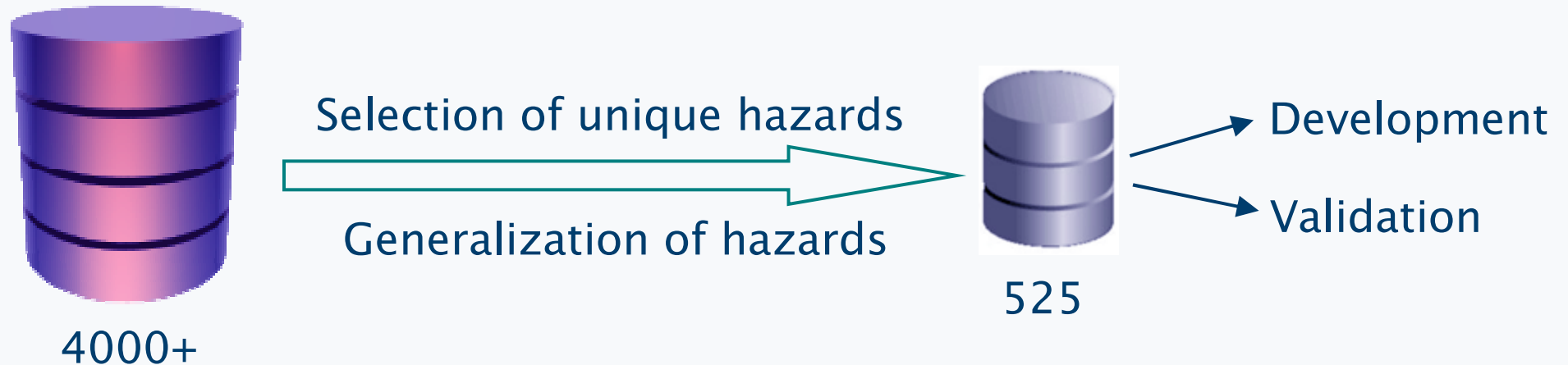
- Events / conditions / performance aspects
- Humans / systems / environment
- Interactions



## **NLR ATM Hazard Database**

- ATM safety assessments
- Hazard brainstorm sessions
- 4000+ hazards

# A set of generalized hazards



Pilot mixes up ATC clearances

Flight plans of ATC system and FMS differ

wrong way

Pilot validates without checking

Weather forecast is wrong

in

Alert causes attentional tunneling

Resolution of conflict leads to other conflicts

HMI

Risk of a conflict is underestimated

Fals Animals on the runway

Fals

Controller has wrong SA about intent of aircraft

Contingency procedures have not been tested



# Interviews with pilots and controllers: How do they deal with hazards?



5 Controllers  
(ACC / Approach / Tower)



2 Airline pilots

**Interviews were conducted face-to-face or by phone and structured by questionnaire forms**

## **Types of questions**

- How may the operator or others detect and interpret the situation?
- What impact has the situation of the behaviour of the operator?
- In what ways may the operator or others deal with the situation?
- What are related written procedures?

# Results of the interviews

**Extensive overview of manifestations of practical performance variability as results of hazards in ATM**

- 101 hazards were discussed
- 79 pages of interview reporting



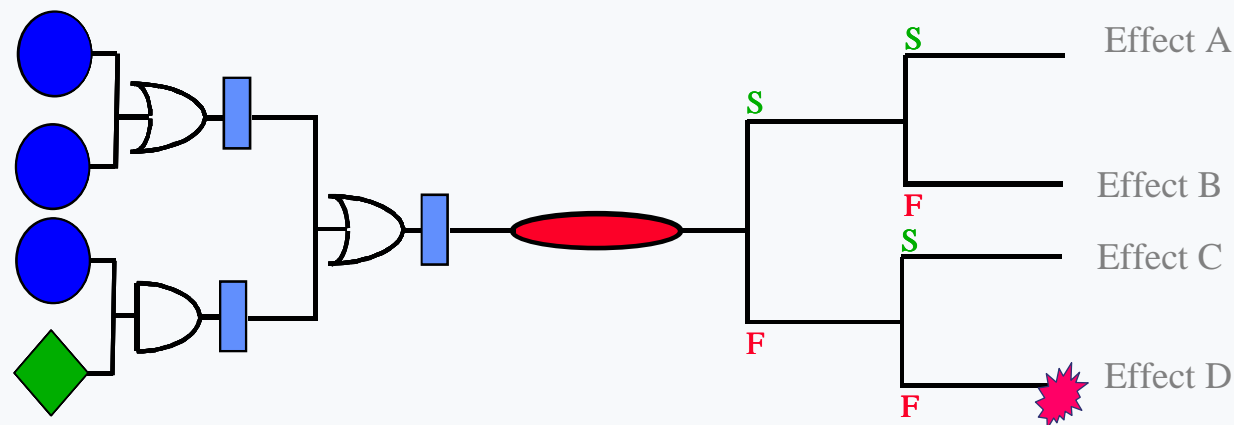
**A key result is that for a lot of hazards there are no written procedures**

- Pilots and controllers react in various ways based upon their training, experience and what they regard as ‘normal work’

# How to model hazards for resilience analysis?

## Fault and event trees

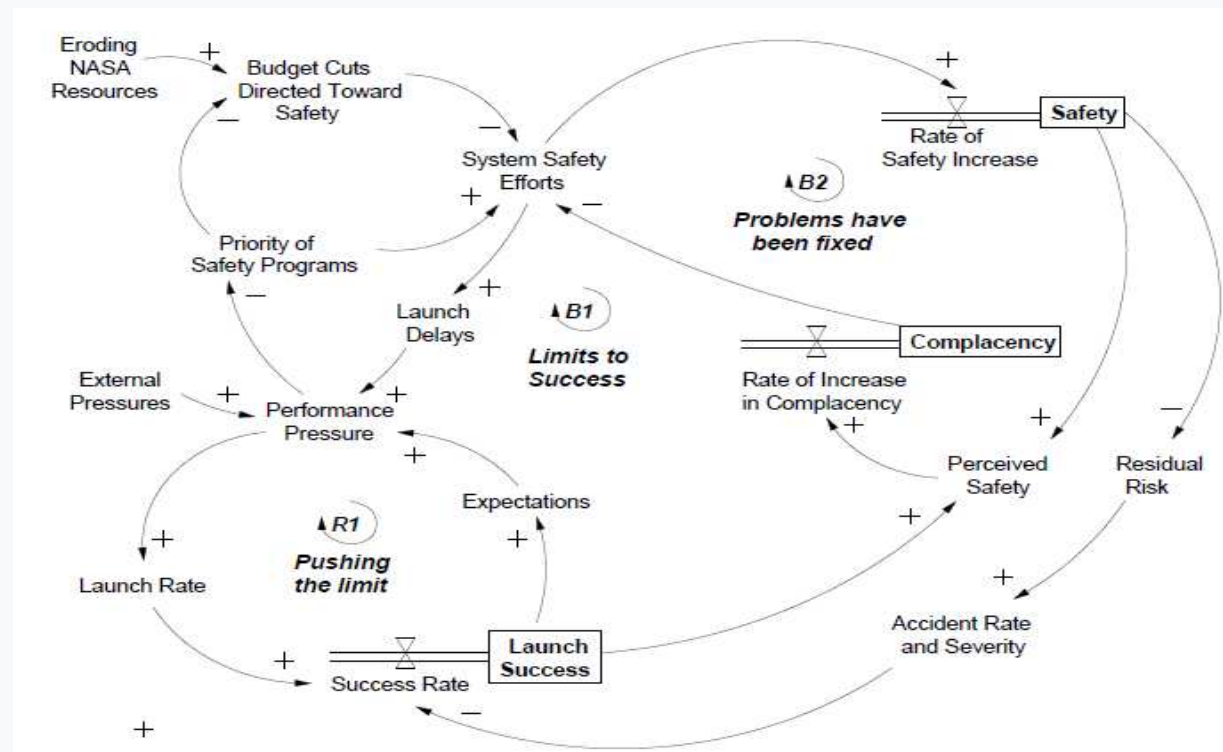
- Dominant technique in reliability engineering
- Very generic model construct: events/conditions
- Little insight in safety of socio-technical systems and resilience implications of hazards



# How to model hazards for resilience analysis?

## STAMP

- Models based on system dynamics for control processes
- Focus on organizational processes at the blunt end
- Human performance at the sharp end has not yet been included

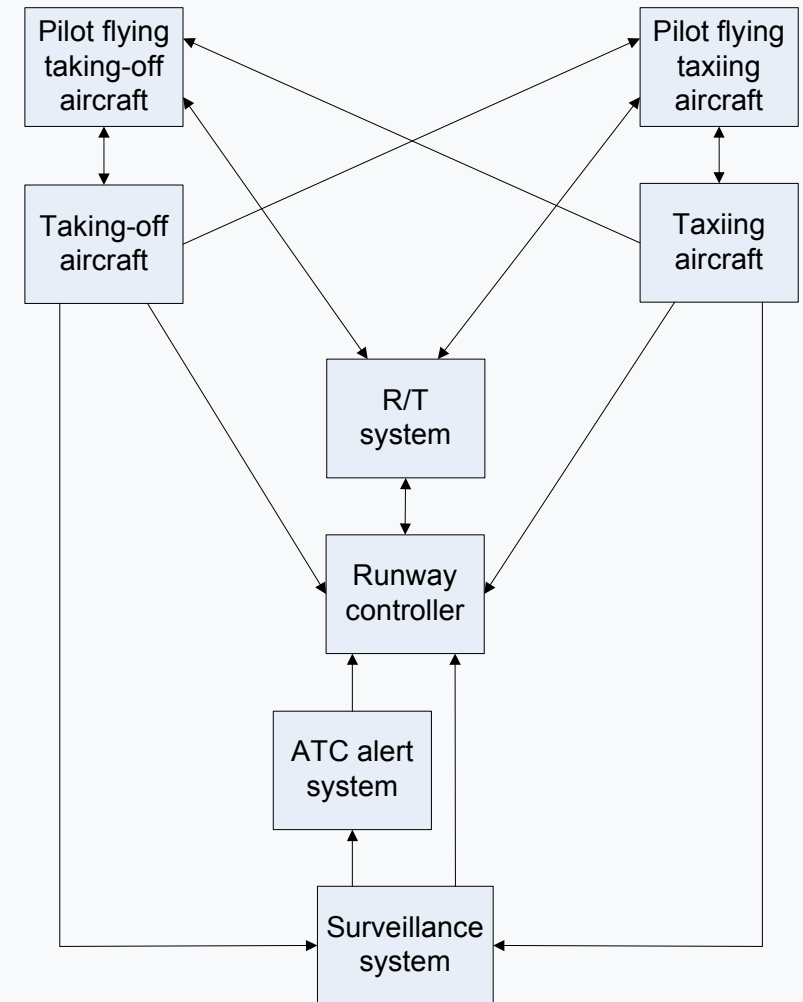




# How to model hazards for resilience analysis?

## Multi-agent dynamic risk modelling

- Stochastic dynamic models of humans, systems and interactions
- Systematic evaluation of risk, risk sensitivity, risk uncertainty and risk contributions by agents in complex sociotechnical systems
- Viable method for systematic evaluation of safety and resilience in complex sociotechnical systems

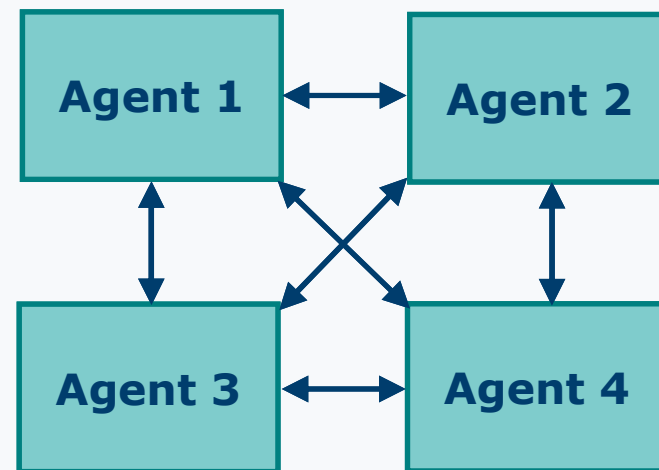


# Model constructs for hazard coverage in multi-agent DRM

- Human information processing loop
- Multi-agent situation awareness
- Task identification
- Task scheduling
- Task execution
- Cognitive control mode
- Task load
- Human error
- Decision making
- System mode
- Dynamic variability
- Stochastic variability
- Contextual condition

Situation awareness of agent  $k$  at time  $t$  about agent  $j$

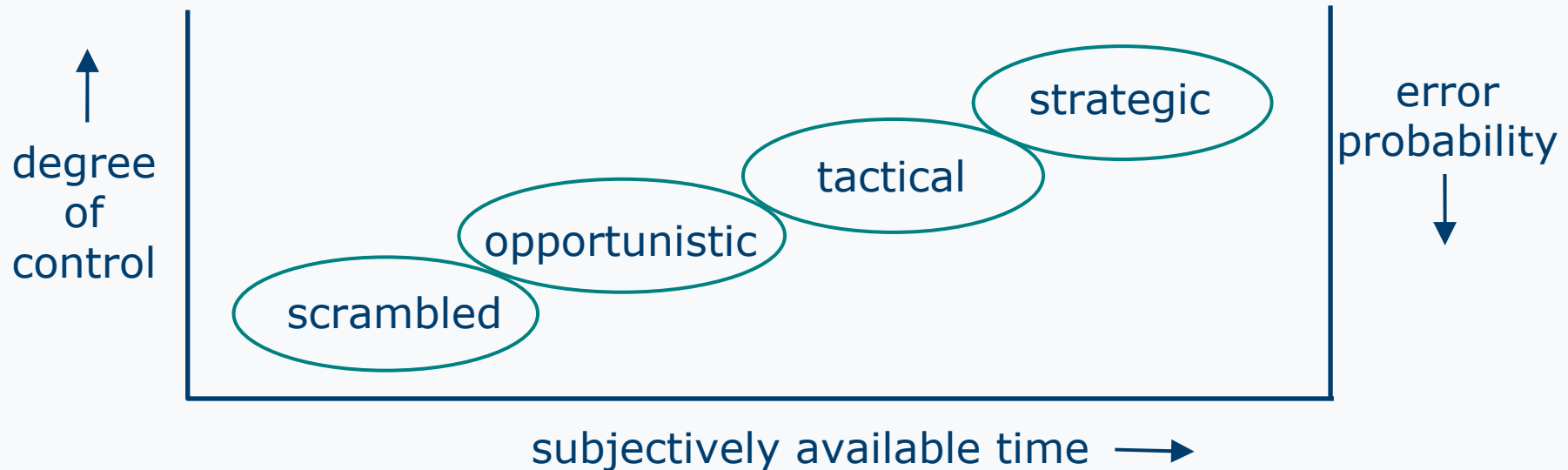
$$\sigma_{t,k}^j = \begin{pmatrix} \text{identity} \\ \text{state} \\ \text{mode} \\ \text{intent} \end{pmatrix}$$



# Model constructs for hazard coverage in multi-agent DRM

- Human information processing loop
- Multi-agent situation awareness
- Task identification
- Task scheduling
- Task execution
- Cognitive control mode
- Task load
- Human error
- Decision making
- System mode
- Dynamic variability
- Stochastic variability
- Contextual condition

## Cognitive control mode





# Coverage of hazards by current model constructs

## Cultural differences between airlines

- ...

## Controller is fatigued and sleepy

- ...

## Lack of experience in degraded modes

- ...

## Procedure change → confusion

- Multi-agent SA
- Decision making
- ...

## Controller ignores an alert

- Multi-agent SA
- ...

## Controller makes a reading error

- Human error
- Multi-agent SA

## Failure of GPS system

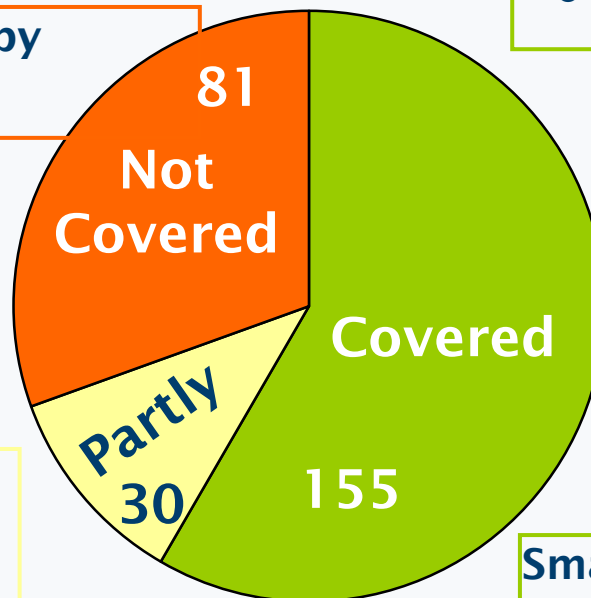
- System mode

## Pilot reports wrong position

- Human error
- Multi-agent SA

## Smaller spacing leads to more time pressure

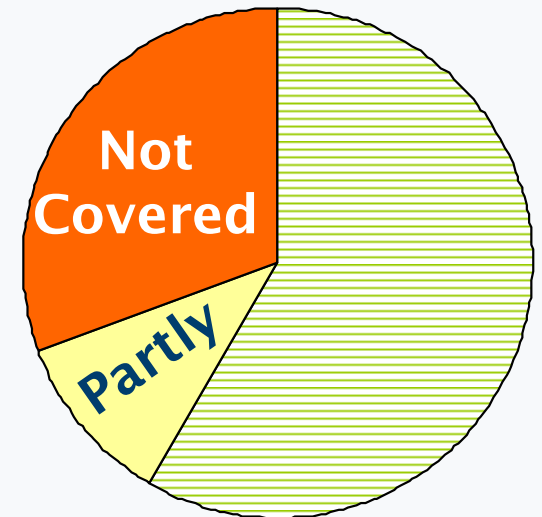
- Task scheduling
- Task execution
- Cognitive control mode



# Groups of hazards not or partly covered

40

- Handling of inconsistent, confusing or uncertain information by a human operator
- The trust by a human in a system and the effect on the performance of the human
- Bad weather or weather change
- Bending rules to gain some advantage
- Complex or unclear procedures leading to confusion
- Changes or differences in procedures leading to confusion or lack of operational fluency
- Lack of experience, training or testing with degraded modes or contingency procedures
- Cultural or language differences
- Organizational changes or problems
- Negotiation processes
- Causes and effect of fatigue and sleepiness
- Attention tunnelling
- ...



# Conclusions

**We identified a set of 525 generalized hazards in ATM**

- Many related to human roles

**We interviewed controllers and pilots to obtain insight in the ways that humans deal with hazards in ATM**

**We studied approaches for analysis of resilience in ATM**

- Multi-agent approach has most potential
- Psychological perspective in FRAM will also be studied further

**We identified hazards that are not or only partly covered by current model constructs in multi-agent DRM**

# Future research

**Identification of new model constructs for hazard coverage**

**Mathematical formalisation of new model constructs**

**Validation of model constructs**

**Application to SESAR 2020 conops**

**Assessment of the applicability of the newly designed approaches in safety analysis and design**

# Questions / Discussion

