

Third SESAR Innovation Days

26–28 November 2013, KTH, Stockholm, Sweden



Safety Criticality Analysis of Air Traffic Management Systems: A Compositional Bisimulation Approach

Elena De Santis, Maria Domenica Di Benedetto,
Mariken Everdij, Davide Pezzuti,
Giordano Pola and Luca Scarciolla

University of L'Aquila (Italy) and NLR (The Netherlands)

giordano.pola@univaq.it



WP-E MAREA Project

- ❑ Project: **Mathematical approach towards resilience engineering in ATM**
- ❑ Acronym: **MAREA**
- ❑ Theme: **Mastering Complex Systems Safely**
- ❑ Project type: **Medium**
- ❑ Duration: **30 months**
- ❑ Coordinator: **NLR**
- ❑ Consortium members: **NLR, University of l'Aquila, VU University of Amsterdam**

Outline

- ❑ Mathematical framework for modelling and analysing complex ATM systems
 - Modelling
 - Analysis of hazards and MASA inconsistencies
 - Complexity reduction
- ❑ Application to the Terminal Manoeuvring Area (TMA) T1 operation
- ❑ Conclusion

Outline

- ❑ **Mathematical framework for modelling and analysing complex ATM systems**
 - **Modelling**
 - **Analysis of hazards and MASA inconsistencies**
 - **Complexity reduction**
- ❑ **Application to the Terminal Manoeuvring Area (TMA) T1 operation**
- ❑ **Conclusion**

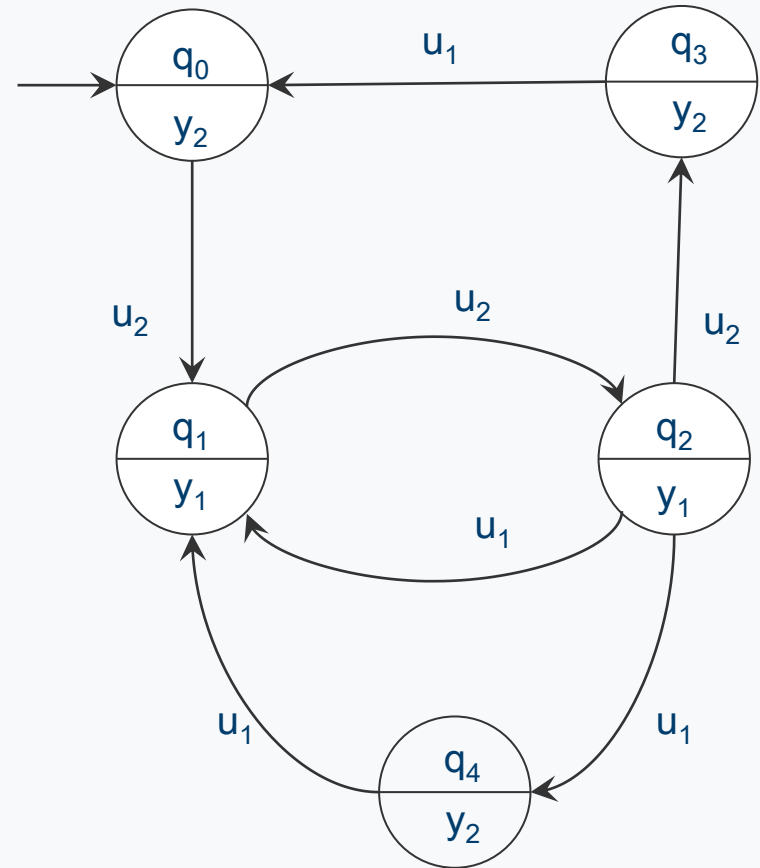
Mathematical Framework: Modelling

A **Finite State Machine (FSM)** is a tuple

$$M = (Q, q^0, U, Y, H, \Delta),$$

where:

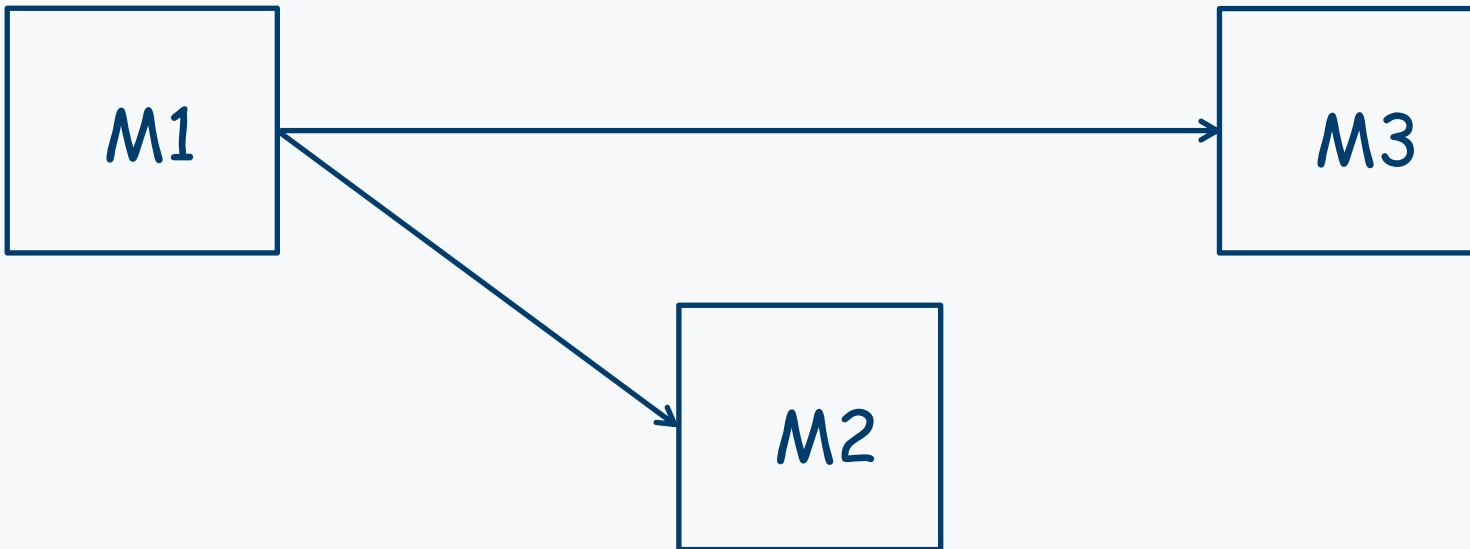
- Q is a finite set of states
- q^0 is the initial state
- U is a finite set of input symbols
- Y is a finite set of output symbols
- $H : Q \rightarrow Y$ is an output map
- $\Delta \subseteq Q \times U \times Q$ is a transition relation



Mathematical Framework: Modelling

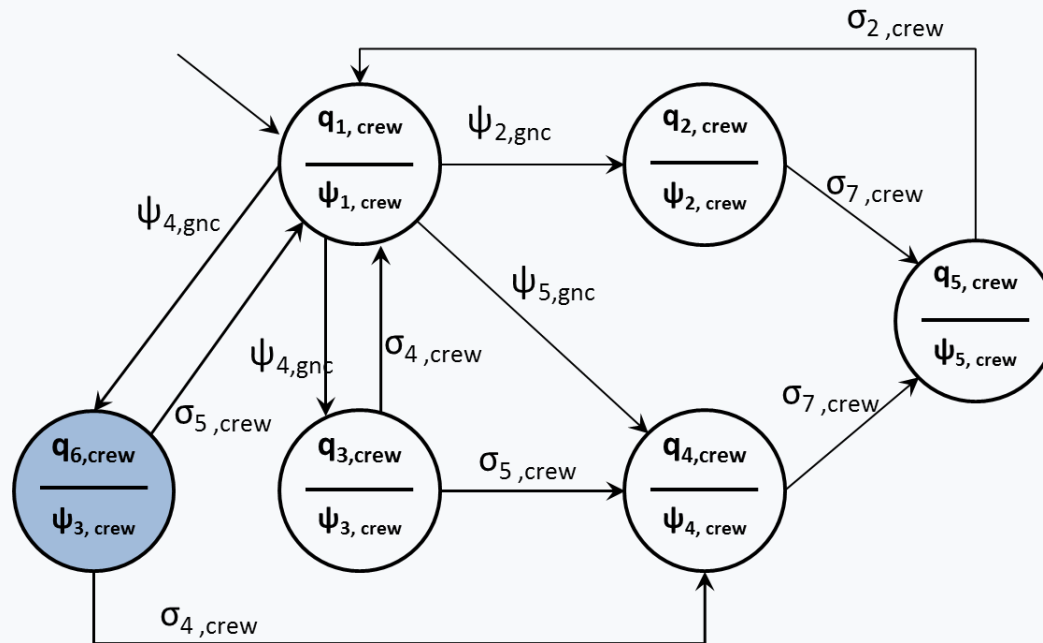
An **Arena of Finite State Machines** (AFSM) is specified by a directed graph $A = (V, E)$, where:

- V is a collection of N FSMs $M_i = (Q_i, q_i^0, U_i, Y_i, H_i, \Delta_i)$
- $E \subseteq V \times V$ describes the communication network of FSMs M_i



Mathematical Framework: Modelling

- ❑ Modelling of hazards and MASA inconsistencies can be approached by resorting to the notion of critical states
- ❑ Let $R \subset Q$ be the set of critical states of a FSM H

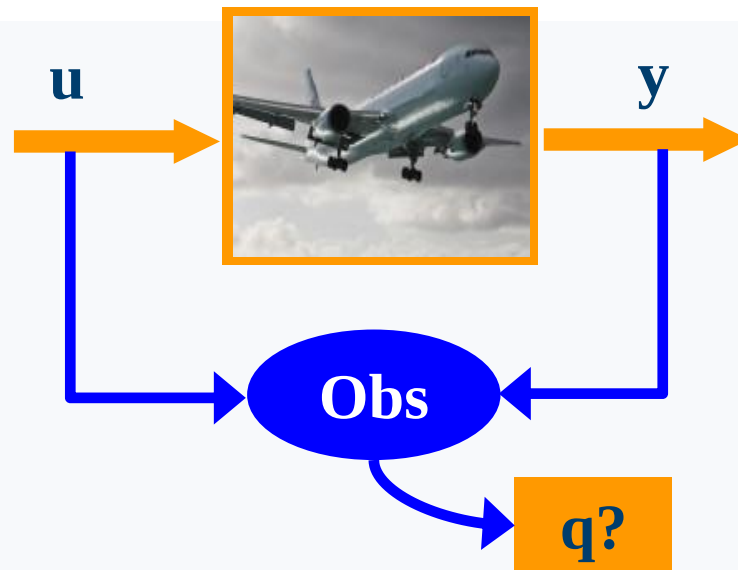


Blue state: Critical State

Mathematical Framework: Analysis

Goal: Study the possibility of detecting the occurrence of unsafe and/or unallowed operations in a FSM M

Consider a FSM M and a set R of critical states. M is R -critically observable if it is possible to construct a critical observer that is able to detect if $q \in R$ or not on the basis of inputs and outputs



Mathematical Framework: Analysis

Critical observability of FSMs naturally extends to AFSMs by appropriately defining a critical relation that extends the set of critical states to a collection of FSMs in an AFSM.

Given an AFSM $A = (V, E)$, consider the following tuple

$$\mathcal{R}_c = (\mathcal{R}_c^1, \mathcal{R}_c^2, \dots, \mathcal{R}_c^N)$$

where:

- $\mathcal{R}_c^1$ is the collection of sets $\mathcal{R}_{i1} \subseteq Q_{i1}$ of critical states for M_{i1}
- $\mathcal{R}_c^2$ is the collection of sets $\mathcal{R}_{i1,i2} \subseteq Q_{i1} \times Q_{i2}$ of critical states arising from the interaction of M_{i1} and M_{i2}
- ...
- $\mathcal{R}_c^N$ is the collection of sets $\mathcal{R}_{i1,\dots,iN} \subseteq Q_{i1} \times Q_{i2} \times \dots \times Q_{iN}$ of critical states arising from the interaction of M_{ij} with $j = 1, 2, \dots, N$

Mathematical Framework: Complexity reduction

Critical compositional bisimulation groups agents that are equivalent

Two agents are equivalent if

- ❑ They are of the same "type" (e.g. two aircraft)
- ❑ They have the same role in the procedure (e.g. two aircraft performing a Standard Instrument Departure (SID))
- ❑ They communicate with equivalent agents
- ❑ They share critical situations with equivalent agents

If AFSMs A^1 and A^2 are $(\mathcal{R}_{c1}, \mathcal{R}_{c2})$ -critically compositionally bisimilar, then A^1 is $\mathcal{R}_{c1}$ -critically observable if and only if A^2 is $\mathcal{R}_{c2}$ -critically observable

Outline

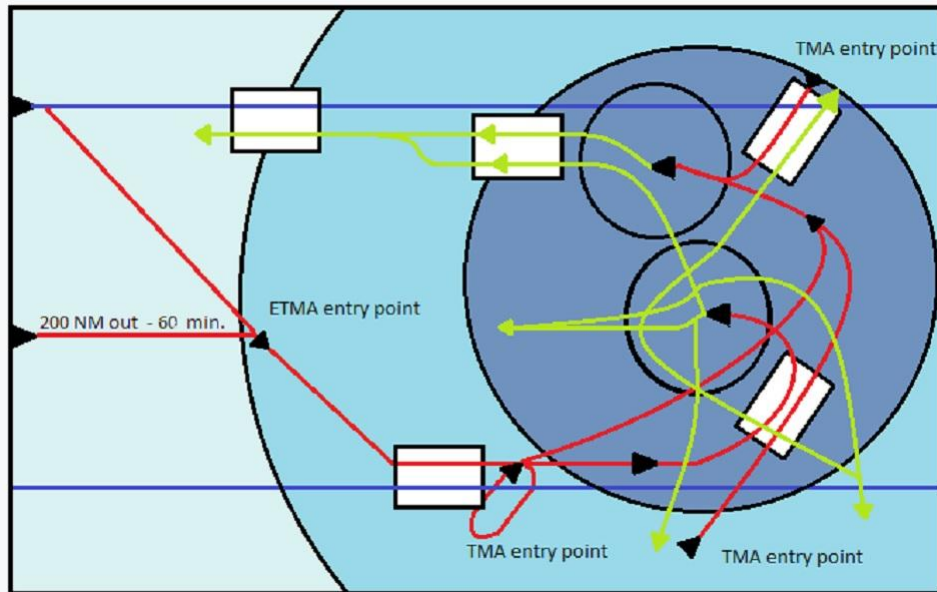
- ❑ Mathematical framework for modelling and analysing complex ATM systems
 - Modelling
 - Analysis of hazards and MASA inconsistencies
 - Complexity reduction
- ❑ **Application to the Terminal Manoeuvring Area (TMA) T1 operation**
- ❑ Conclusion

TMA T1 operation

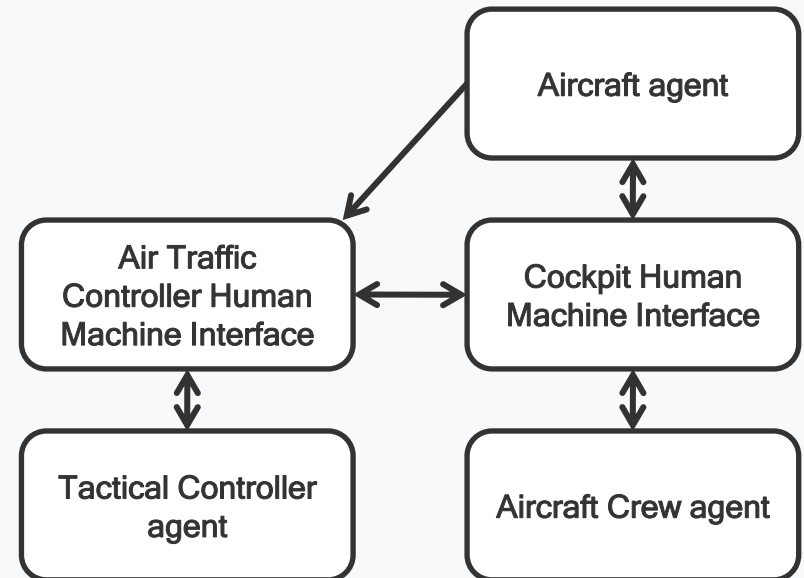
- ❑ The aim of the **SESAR** (Single European Sky Air Traffic Management Research) Programme is to improve efficiency in future ATM
- ❑ In the SESAR 2020 Concept of Operations (ConOps) a 4D trajectory planning based operation is assumed, which is implemented through the exchange of Reference Business Trajectories (**RBTs**)
- ❑ The use of RBTs allows pilots to follow their assigned trajectories with a sensible reduction of the controller interventions
- ❑ We chose the Terminal Manoeuvring Area (**TMA**) T1 operation as a meaningful case study, since it exhibits most of the key features that arise in the SESAR 2020 ConOps
- ❑ Here, **T1** refers to the reduction of separation minima in the TMA

TMA T1 operation

In the TMA T1 operation, routes are typically Standard Instrument Departure (**SID**) routes, Standard Terminal Arrival Routes (**STAR**) and also **cruise routes** at a lower flight level.



Agent involved in the
TMA T1 scenario:



TMA T1 operation

Assumptions:

- ☐ The two pilots of each aircraft are represented as one crew agent
- ☐ All aircraft flight-plans/RBTs are according to the STAR, SID or Cruise route on which the respective aircraft fly
- ☐ There is no explicit negotiation of RBTs in the model
- ☐ The model only considers the tactical air traffic controller, i.e. traffic flow and capacity management is not considered
- ☐ Conflicts between two aircraft can be detected by the air traffic controller through the Short Term Conflict Alert (STCA)

TMA T1 operation

Selection of hazards from MAREA deliverable D2.1 (NLR):

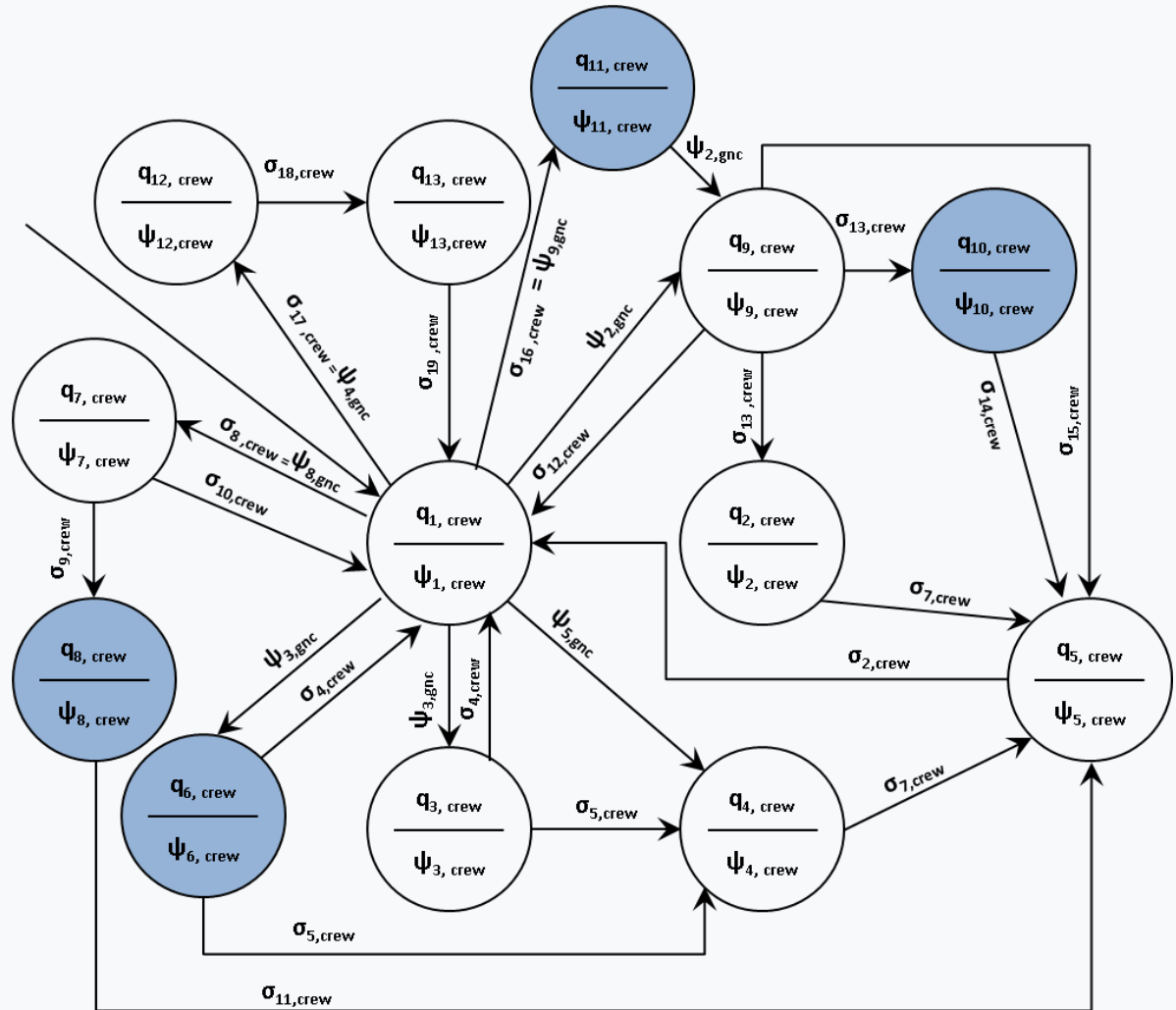
- ☐ Failure of Flight Management System (FMS) (hazard no. 19)
- ☐ Failure of cockpit display and failure of the Controller Pilot Data Link Communications (CPDLC) (hazards no. 5, 63, 115 and 137)
- ☐ False alert of an airborne system (hazard no. 21)
- ☐ Short Term Conflict Alert (STCA) or conflict alert is underestimated or ignored by the ATCo (hazards no. 254, 322 and 326)
- ☐ Misunderstanding of controller instruction by pilot (hazard no. 292)

TMA T1 operation

The Crew Agent:

Critical states considered:

- ❑ $q_{6,crew}$ - Crew updates flight trajectory data. Situation awareness incorrect wrt his RBT
- ❑ $q_{8,crew}$ – Heavy workload
- ❑ $q_{10,crew}$ - Pilot misinterprets communication (hazard no. 292)
- ❑ $q_{11,crew}$ - Pilot does not realize a warning (hazard no. 137)



TMA T1 operation

Aircraft dynamics:



$$f(x, u) = \begin{cases} \dot{x}_1 = x_4 \cos(x_5) \cos(x_6) \\ \dot{x}_2 = x_4 \sin(x_5) \cos(x_6) \\ \dot{x}_3 = x_4 \sin(\alpha) \\ \dot{x}_4 = \frac{1}{m} [u_1 \cos(\alpha) - D - mg \sin(x_6)] \\ \dot{x}_5 = \frac{1}{mx_4} [L \sin(u_2) + u_1 \sin(\alpha) \sin(u_2)] \\ \dot{x}_6 = \frac{1}{mx_4} [(L + u_1 \sin(\alpha)) \cos(u_2) - mg \cos(x_6)] \end{cases}$$

where:

- x_1 and x_2 indicate the horizontal position.
- x_3 is the altitude.
- x_4 is the true airspeed.
- x_5 is the heading angle.
- x_6 is the angle of climb/descent.
- u_1 is the engine thrust.
- u_2 is the bank angle.
- u_3 is the angle of climb/descent.

TMA T1 operation

Selected Scenario

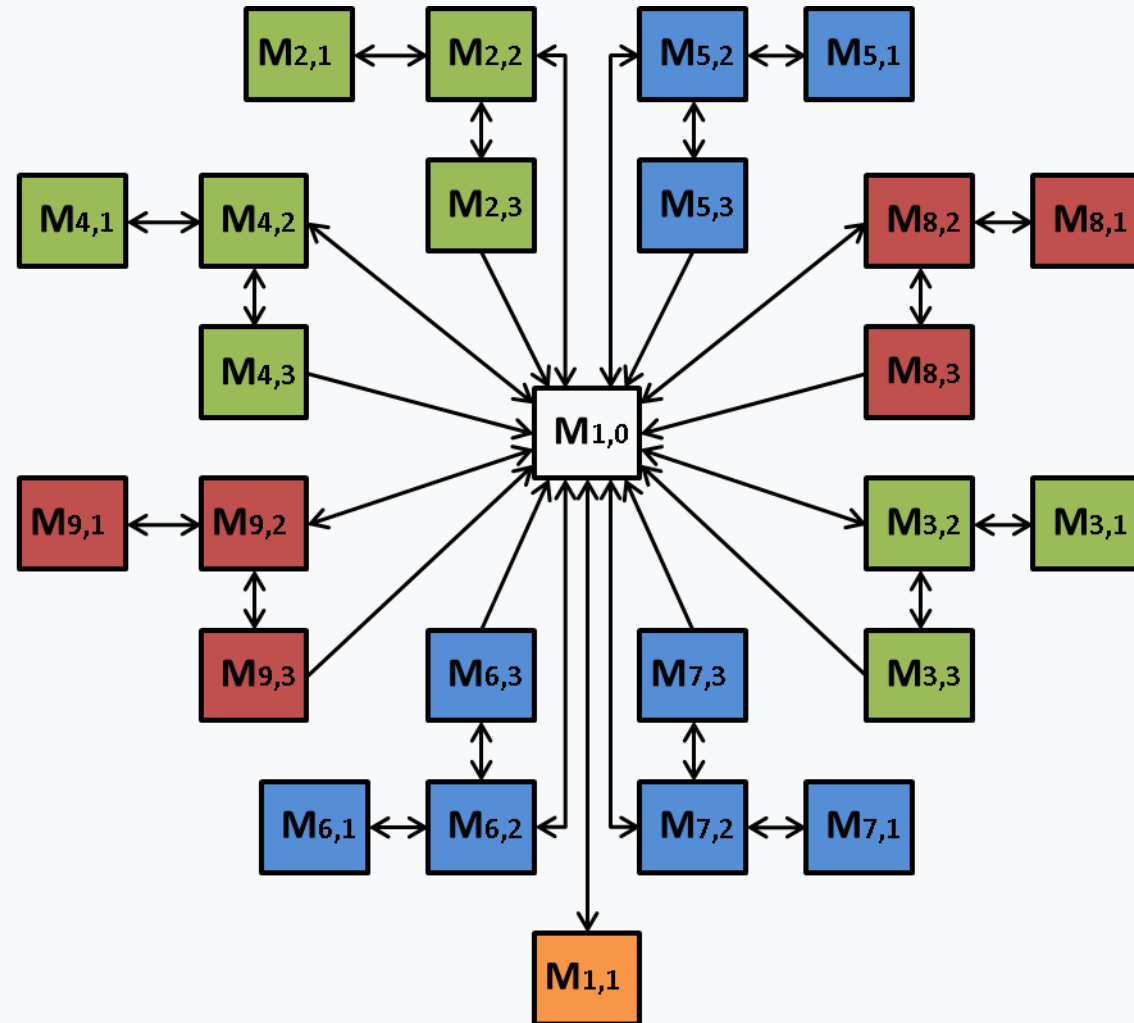
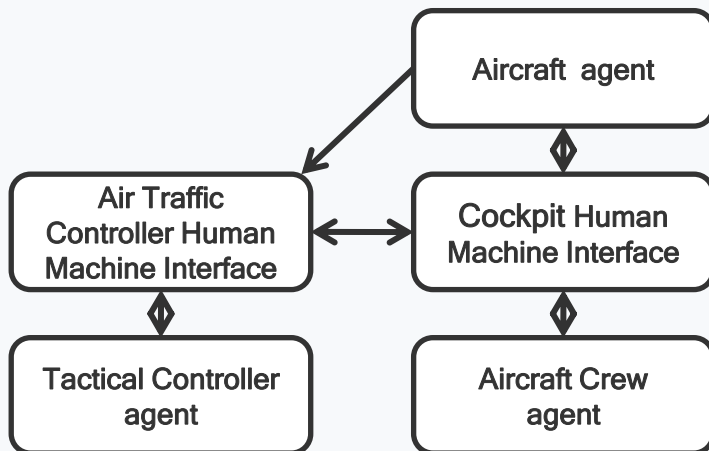
3 SIDs aircraft

2 STARs aircraft

3 CRUISE ROUTES aircraft

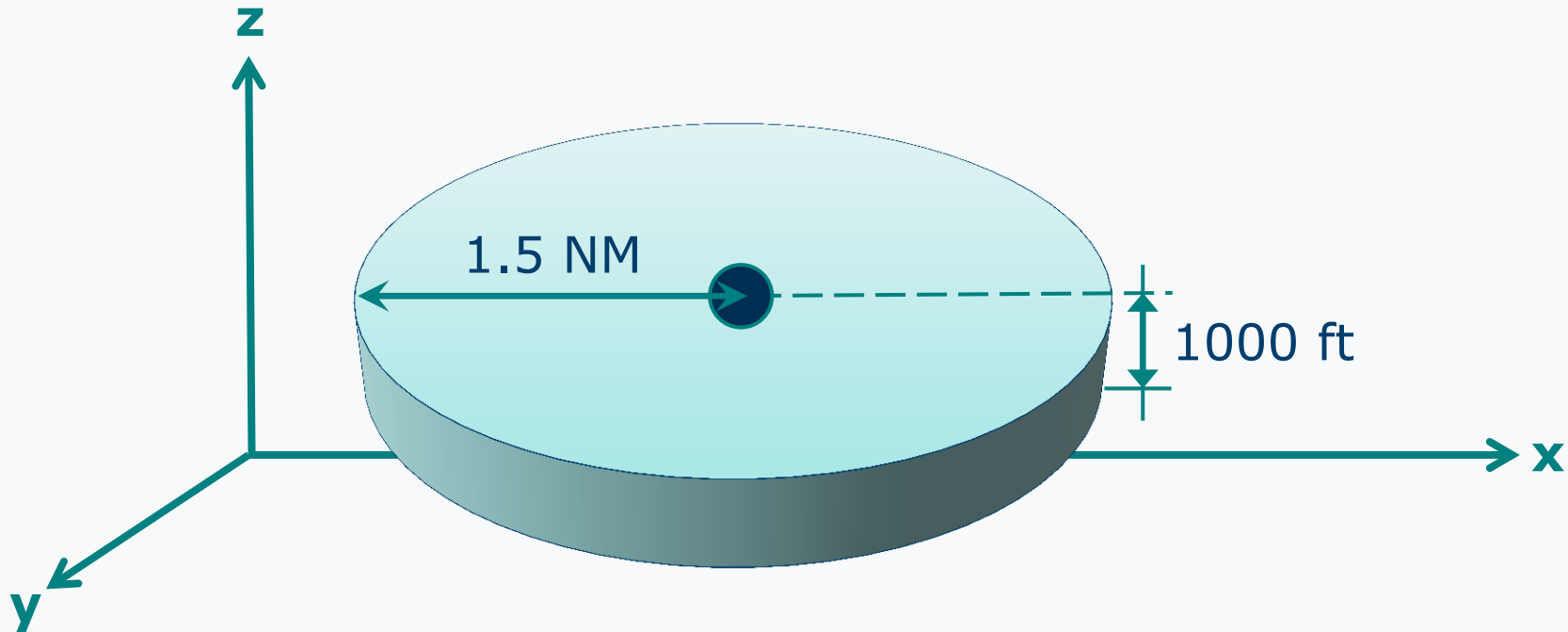
1 ATCo HMI

1 ATCo



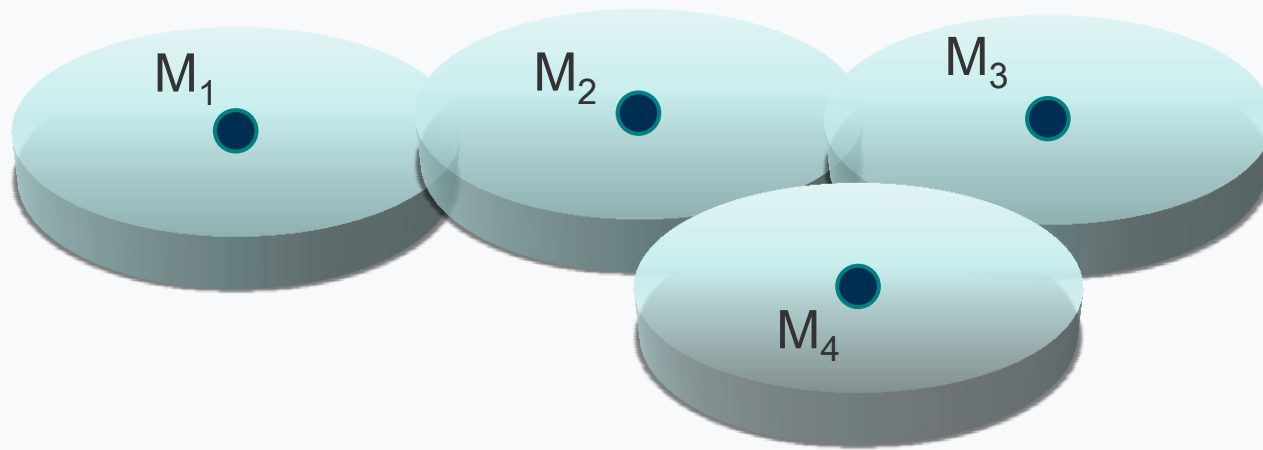
Analysis of Critical Situations

- Whenever two aircraft are closer than 3NM apart in horizontal direction while being closer than 1000ft apart in vertical direction, they are said to be in conflict



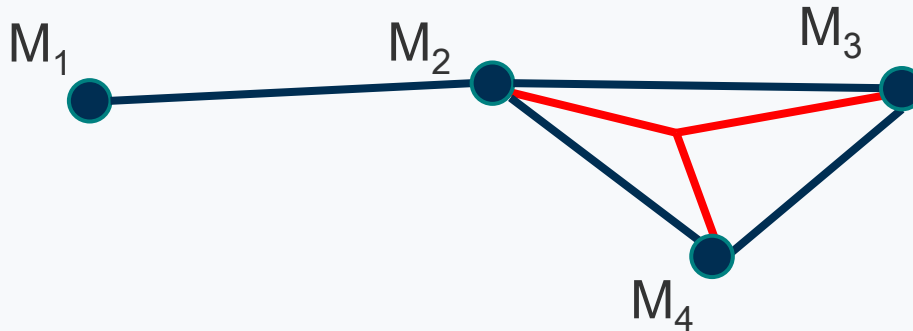
Analysis of Critical Situations

- Whenever two aircraft are closer than 3NM apart in horizontal direction while being closer than 1000ft apart in vertical direction, they are said to be in conflict



Analysis of Critical Situations

- Whenever two aircraft are closer than 3NM apart in horizontal direction while being closer than 1000ft apart in vertical direction, they are said to be in conflict



$$R = (R_{12}, R_{23}, R_{24}, R_{34}, R_{234})$$

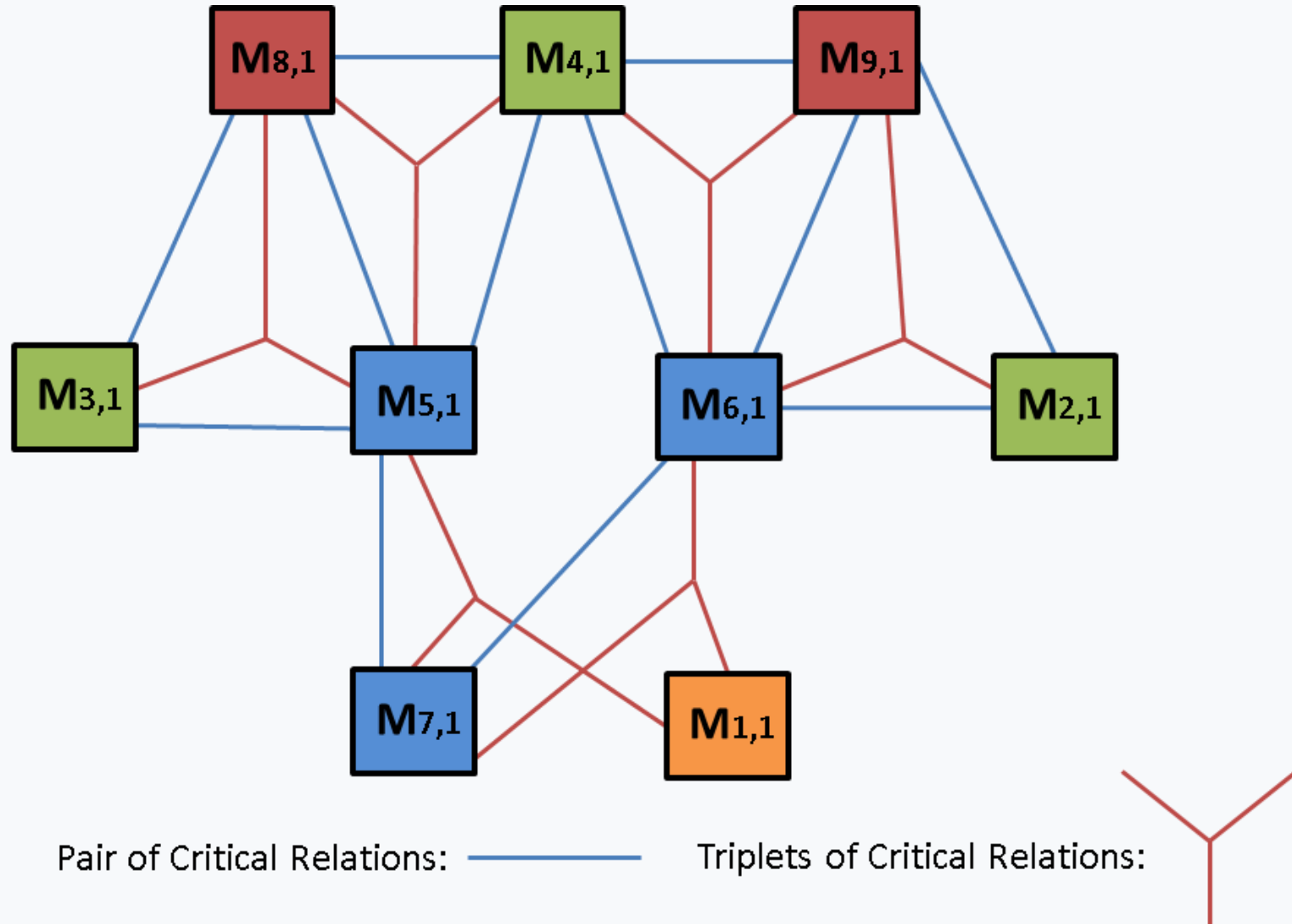
MASA Inconsistencies

- ❑ $(q_{2,crew1}, q_{2,crew2})$ a simultaneous conflict resolution manoeuvre of two aircraft that are flying in each other's vicinity
- ❑ $(q_{4,crew1}, q_{4,crew2})$ a simultaneous flight-plan deviation avoidance manoeuvre of two aircraft that are flying in each other's vicinity
- ❑ $(q_{2,crew1}, q_{4,crew2})$ and $(q_{4,crew1}, q_{2,crew2})$ one of the two aircraft that are flying in each other's vicinity, performs a conflict resolution manoeuvre and the other one performs a flight-plan deviation avoidance manoeuvre and vice-versa
- ❑ $(q_{1,crew1}, q_{2,crew2})$ and $(q_{2,crew1}, q_{1,crew2})$ one of the two aircraft that are flying in each other's vicinity, performs a conflict resolution manoeuvre and the other one is in the monitoring state and vice-versa
- ❑ $(q_{1,crew1}, q_{4,crew2})$ and $(q_{4,crew1}, q_{1,crew2})$ one of the two aircraft that are flying in each other's vicinity, performs a flight-plan deviation avoidance manoeuvre and the other one is in the monitoring state and vice-versa

MASA Inconsistencies

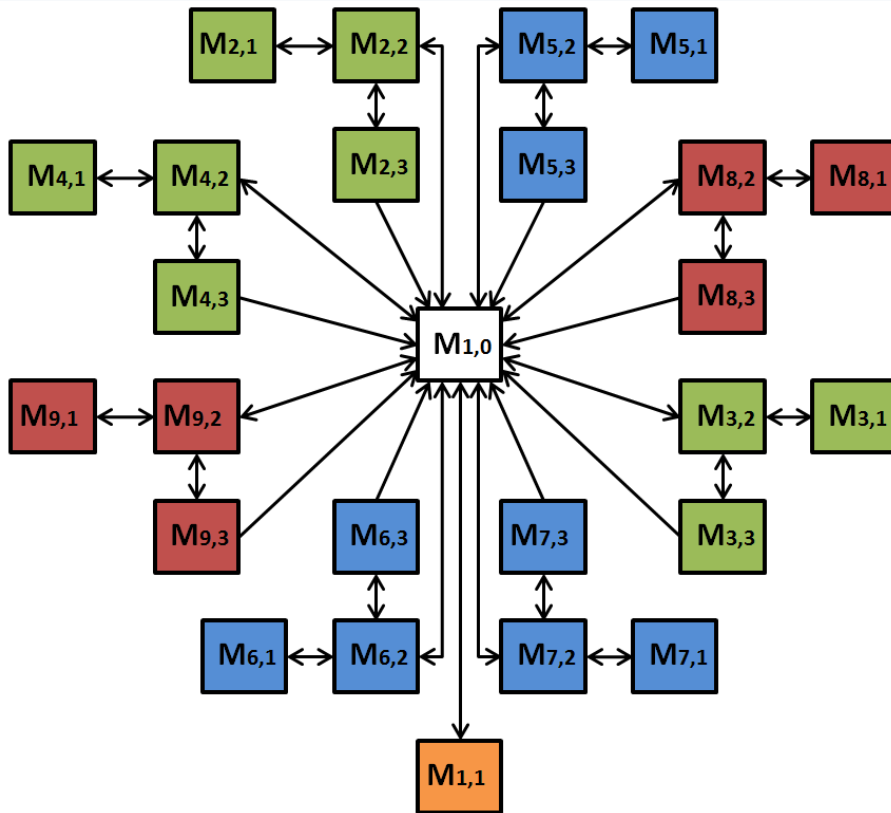
- ❑ **(q5,crew1,q5,crew2,q5,atco)** two crews of aircraft that are flying in each other's vicinity, simultaneously require a radio communication but the controller is engaged in another radio communication of sending radar vectors to a third crew. This situation may lead to a delay that may cause conflicts
- ❑ **(q5,crew1,q5,crew2,q3,atco)** two crews of aircraft that are flying in each other's vicinity, simultaneously require a radio communication but the controller is engaged in another radio communication of manoeuvre conflict resolution; this situation may lead to a delay that may cause conflicts
- ❑ **(q2,crew1,q2,crew2,q2,crew3)** three aircraft performing deviation from their corresponding RBTs while flying in each other's vicinity

Analysis of Critical Situations

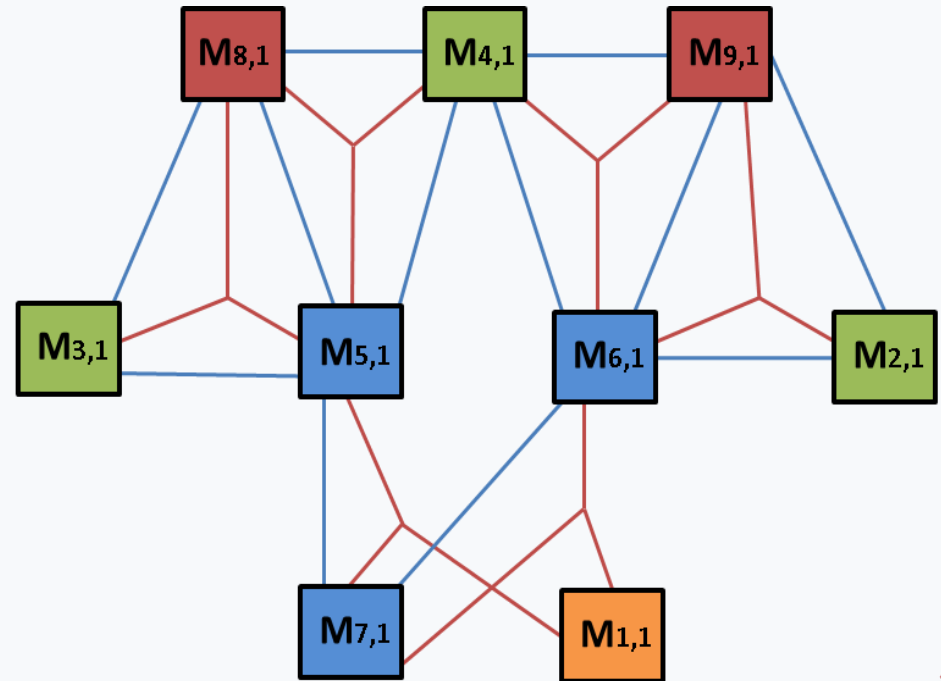


Analysis of Critical Situations

AFSM:



Critical Relation among the agents:



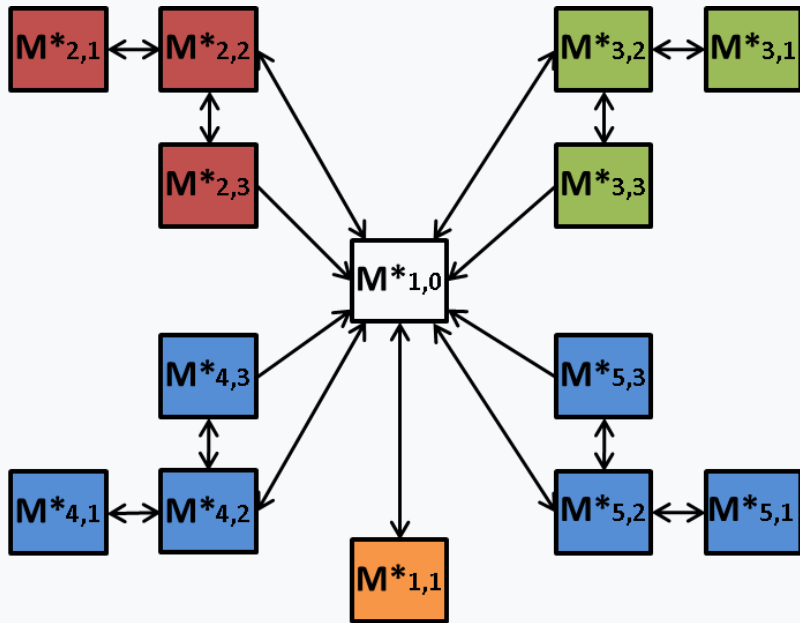
Pair of Critical Relations: — Triplets of Critical Relations: —

Space complexity:

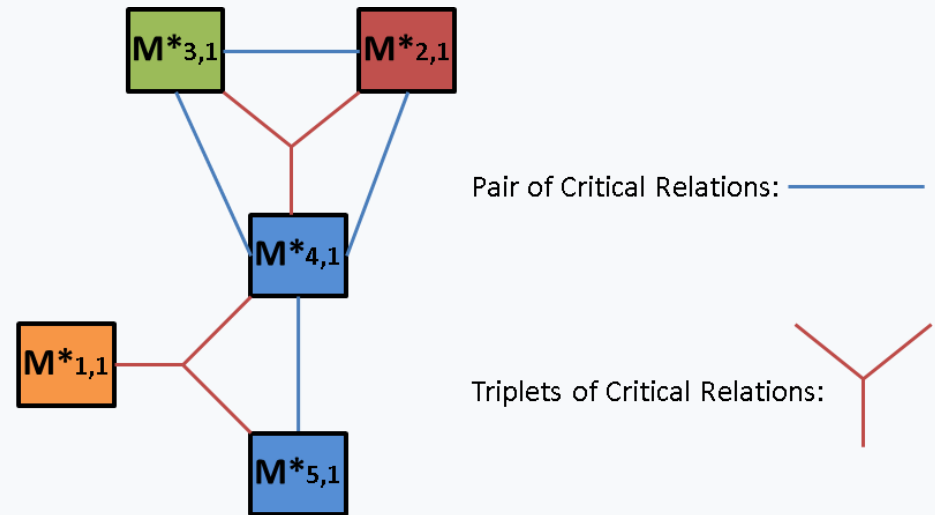
$$\prod_{i=1,2,\dots,8} |Q_{crew}^i| \cdot \prod_{i=1,2,\dots,8} |Q_{gnc}^i| \cdot |Q_{atco}| \cdot |Q_{sys}| = 13^8 \cdot 9^8 \cdot 6 \cdot 8 \simeq 1.68 \cdot 10^{18}$$

Analysis of Critical Situations

Reduced AFSM $\hat{A}$:



Critical Relation among the agents:



Pair of Critical Relations: —

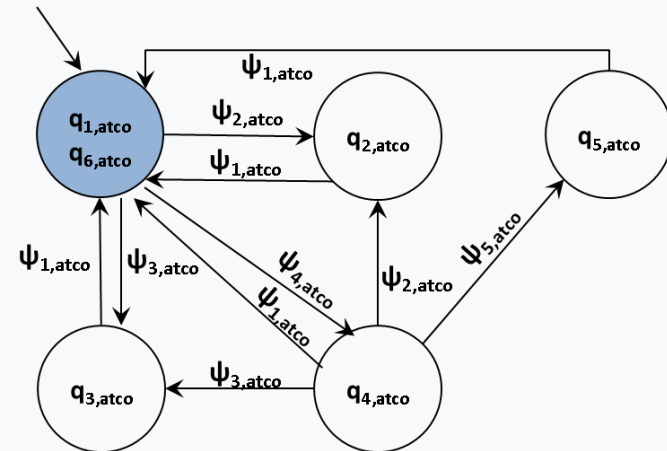
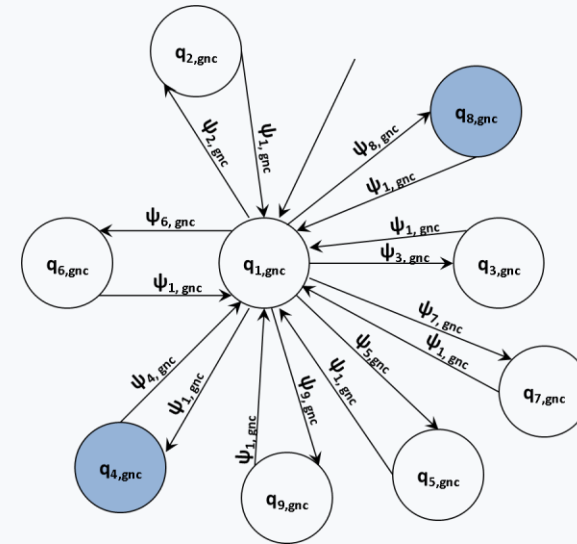
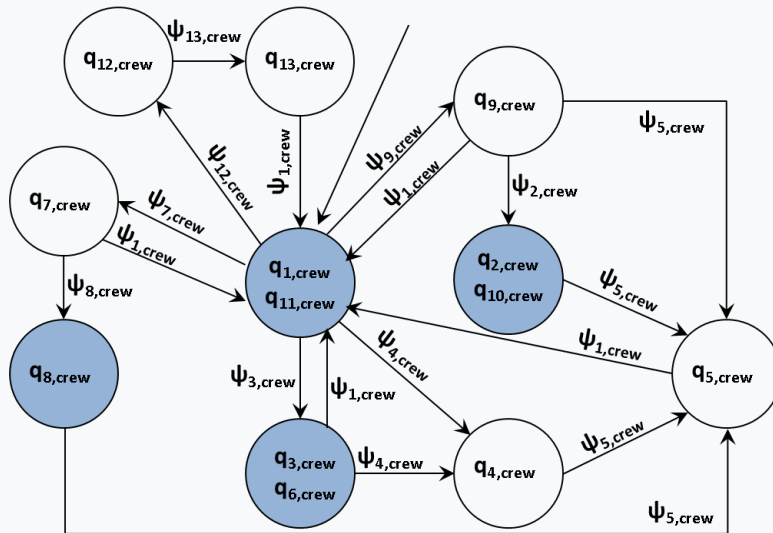
Triplets of Critical Relations: 

Space complexity:

$$\prod_{i=1,2,\dots,4} |Q_{crew}^i| \cdot \prod_{i=1,2,\dots,4} |Q_{gnc}^i| \cdot |Q_{atco}| \cdot |Q_{sys}| = 13^4 \cdot 9^4 \cdot 6 \cdot 8 \simeq 8,99 \cdot 10^9$$

Analysis of Critical Situations

Critical Observers



Outcome of the analysis

Hazards that **can be detected (in the sense of critical observability):**

- ☐ Failure of FMS (hazard no. 19)
- ☐ False alert of an airborne system (hazard no. 21)

Hazards that **cannot be detected:**

- ☐ Failure of cockpit display and failure of the CPDLC (hazards no. 5, 63, 115 and 137)
- ☐ STCA or conflict alert is underestimated or ignored by the ATCo (hazards no. 254, 322 and 326)
- ☐ Misunderstanding of controller instruction by pilot (hazard no. 292)

Outcome of the analysis

MASA inconsistencies that can be detected (in the sense of critical observability):

- ❑ Pairs of crew agents corresponding to aircraft that simultaneously perform a flight plan deviation avoidance manoeuvre while flying in each other's vicinity
- ❑ Triplets of agents, one of which is the ATCo agent, and two of which are the Crew agents that correspond with two aircraft flying in each other's vicinity while requiring a radio communication with the ATCo to receive instructions, but the ATCo is busy doing other activities

Outcome of the analysis

MASA inconsistencies that **cannot be detected**:

- ❑ Pairs of crew agents corresponding with aircraft that simultaneously perform a conflict resolution manoeuvre while flying in each other's vicinity, or where one of the aircraft performs a conflict resolution manoeuvre while the other one performs a flight-plan deviation avoidance manoeuvre while flying in each other's vicinity, or where one aircraft performs a conflict resolution manoeuvre while the other one is in the monitoring state while flying in each other's vicinity, or where one aircraft performs a flight-plan deviation avoidance manoeuvre while the other one is in the monitoring state while flying in each other's vicinity.
- ❑ Triplets of Crew agents, corresponding with three aircraft performing deviations from their corresponding RBTs while flying in each other's vicinity.

Outline

- ❑ Mathematical framework for modelling and analysing complex ATM systems
 - Modelling
 - Analysis of hazards and MASA inconsistencies
 - Complexity reduction
- ❑ Application to the Terminal Manoeuvring Area (TMA) T1 operation
- ❑ **Conclusion**

Conclusion

❑ Modeling and analysis of safety critical ATM operations

A mathematical framework that appropriately models each agent acting in ATM procedures

A compositional framework, based on arenas of finite state machines, that appropriately models the interaction among the agents involved in ATM procedures

A mathematical framework, based on critical observability, to analyze hazards and MASA inconsistencies

❑ Complexity reduction for large-scale ATM systems

Efficient algorithms, based on critical compositional bisimulation, for the reduction of the computational complexity arising in the analysis of realistic ATM scenarios involving a large number of agents

❑ To validate our approach we analyzed the TMA T1 operation and showed that not all hazards and MASA inconsistencies can be detected