



# Modeling Safety Case Evolution

Examples from the Air Traffic Management Domain

**Massimo Felici**

LFCS, School of Informatics  
The University of Edinburgh  
mfelici@inf.ed.ac.uk

<http://homepages.inf.ed.ac.uk/mfelici>

Grand Challenge 6 Workshop on  
Dependable Systems Evolution  
FM05, University of Newcastle upon Tyne, UK



# Overview



- What's happening in the **Air Traffic Management** (ATM) domain?
  - How complex is the ATM domain? Other domains?
- **Safety Analysis** (in ATM)
  - Limitations
- **Evolutionary Safety Analysis**
  - **Safety Case Changes**
    - Examples
  - **Modeling Safety Case Evolution**
- **Conclusions and Future Work**



# What's happening in ATM?



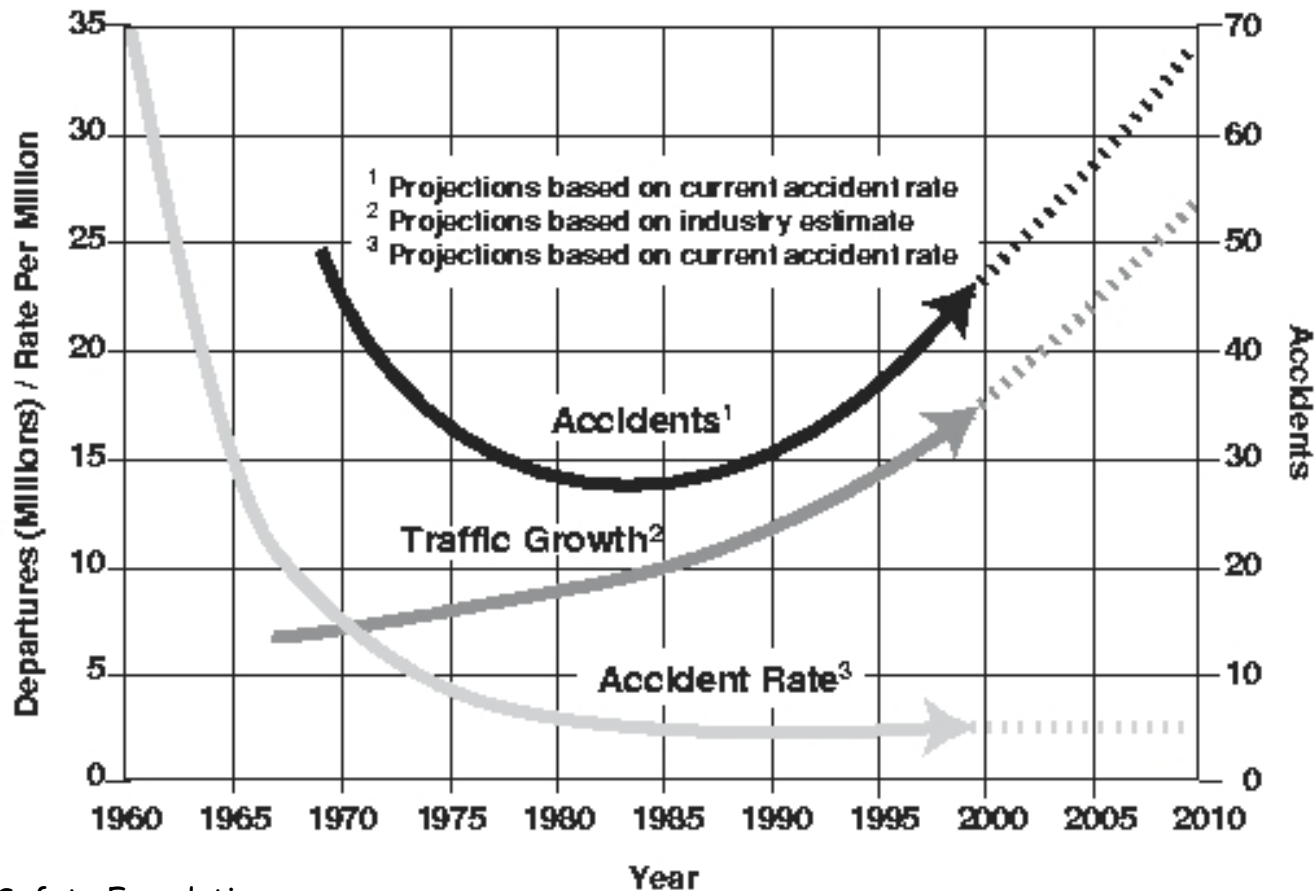
- The EUROCONTROL ATM 2000+ Strategy
- The EU Single European Sky Initiative
- The over all objective is, "for all phases of flight, to enable the **safe, economic, expeditious** and orderly flow of traffic through the provision of ATM services, which are **adaptable** and **scalable** to the requirements of all users and areas of European airspace."
- New ATM concept (ATC -> ATM), new system approach, cultural and structural revision of ATM processes,...
  - Reduced Vertical Separation Minima Requirement, Free Flight, Gate-to-Gate, Medium-Term and Long-term Conflict Detection/Projection,...



# Safety vs. Performance: the way ahead?

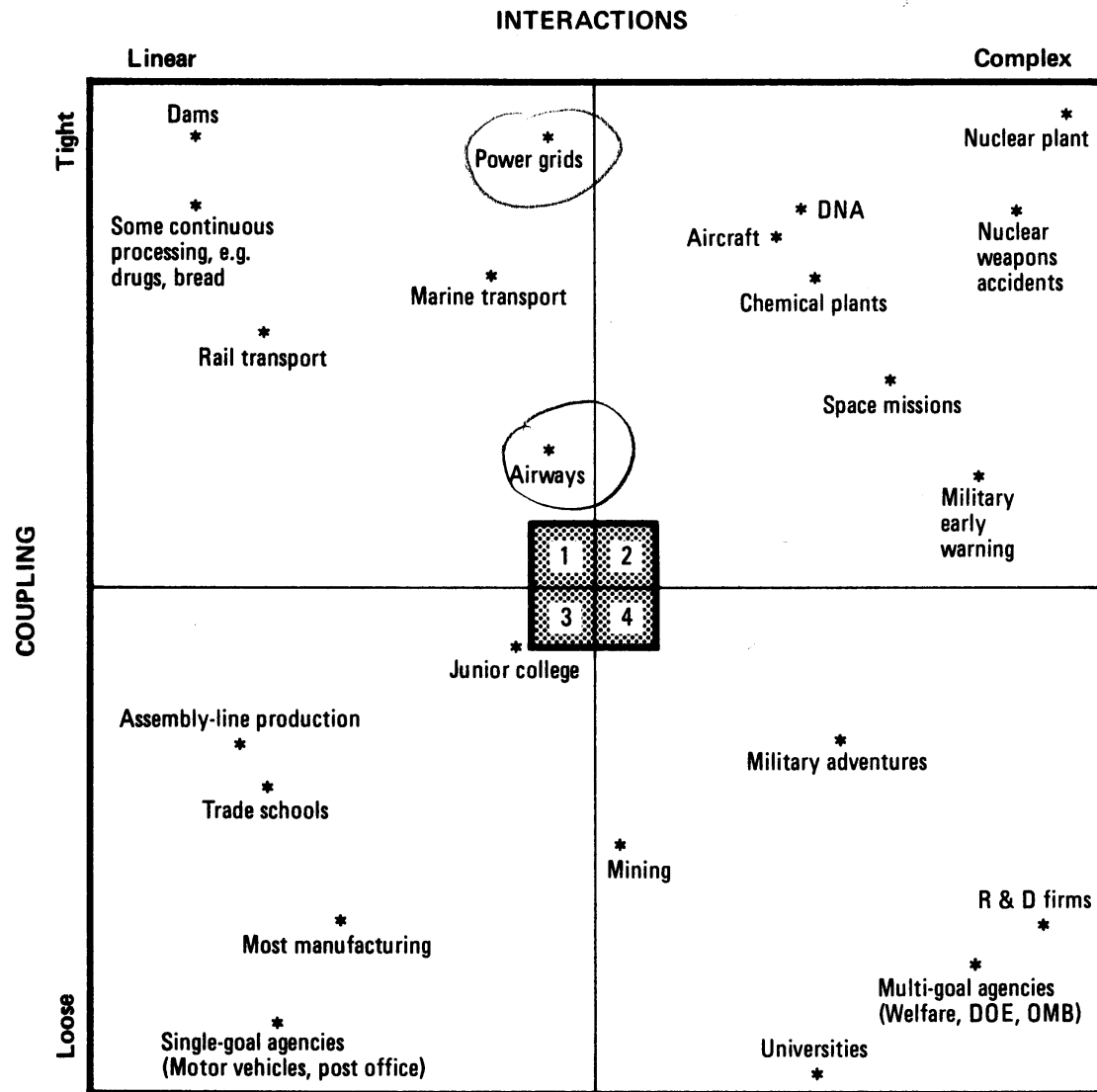


Effect of Static Accident Rate and  
Accompanying Traffic Growth on the Number of Accidents



Source: Flight Safety Foundation

# Coupling vs. Interactions



Perrow, 1999

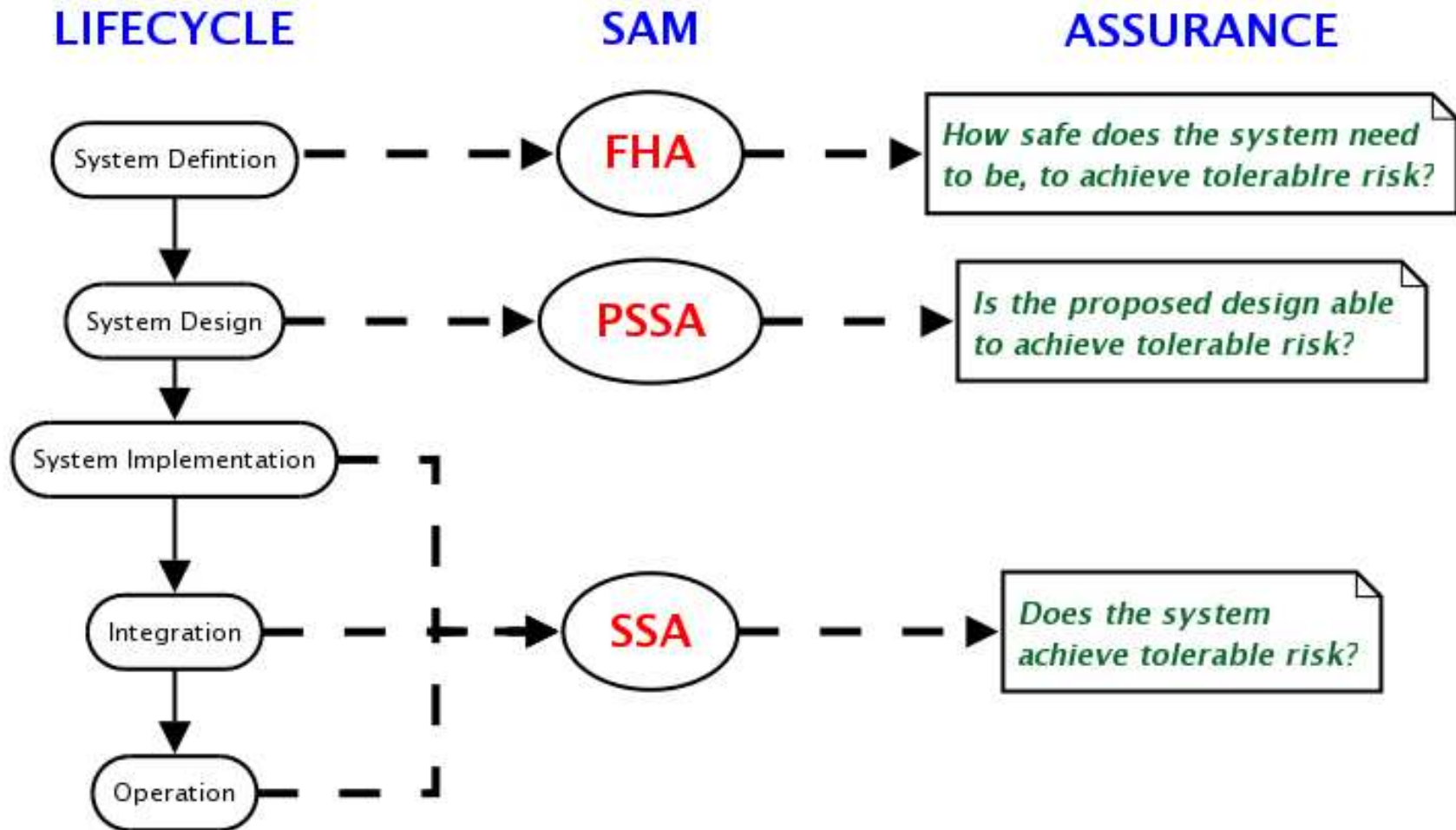
# Safety Analysis in ATM - ESARR4



- **hazard** identification as well as **risk** assessment and **mitigation** are systematically conducted for any **changes**
- hazard identification, risk assessment and mitigation processes shall include:
  - determination of the scope
  - determination of the safety objectives (e.g., hazards, failure conditions, severity and tolerability)
  - Identification of risk mitigation strategies



# Safety Assessment Methodology (SAM)



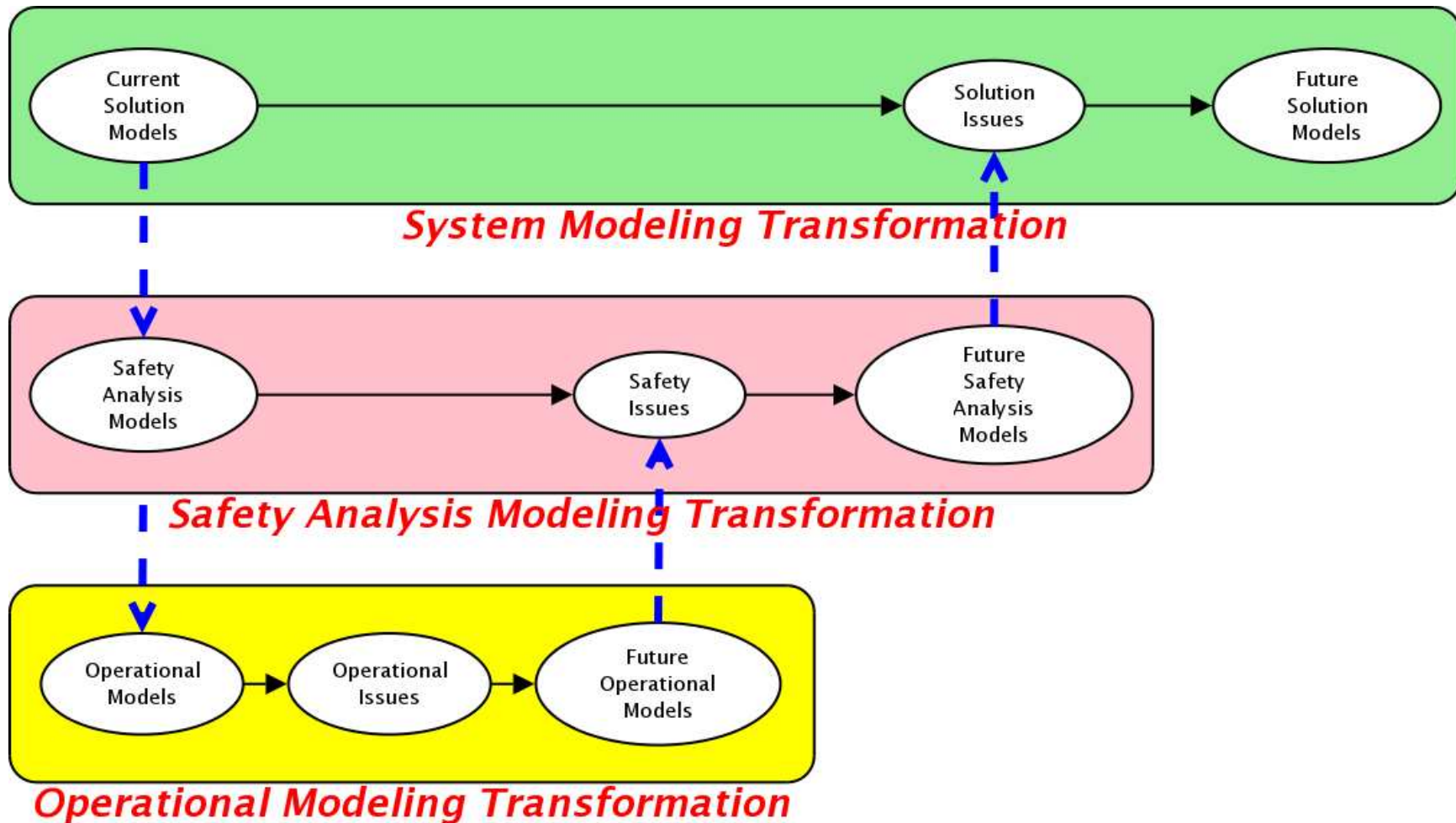
# Exposed Limitations



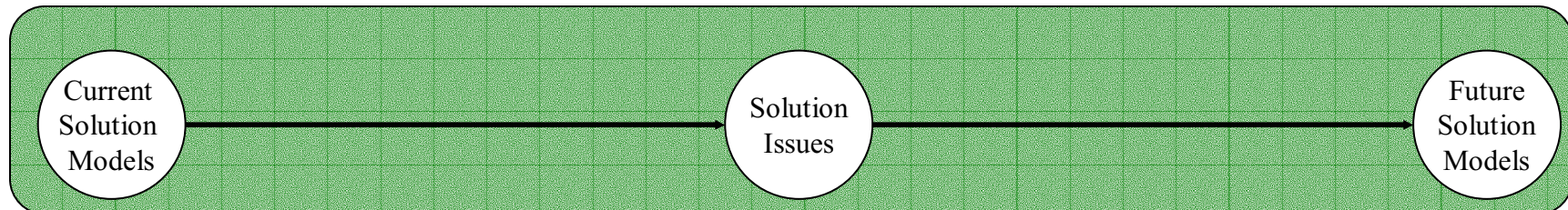
- (unsafe) complex interaction between aircraft and ATM safety functions
- Humans using complex language and procedures mediate this interaction
- Work practice and systems evolve rapidly in response to demand and a culture of continuous improvements
- (Dis)Trust in technology



# Evolutionary Safety Analysis [Felici, SAFECOMP 2005]



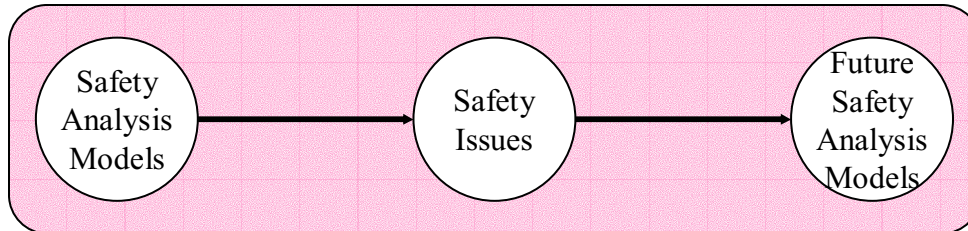
# System Modeling Transformation



- **Requirements**, as mappings between socio-technical solutions and problems, represent an account of the history of socio-technical issues arising and being solved within industrial settings
- The formal extension of these mappings (or solution space transformations) identifies a framework to model and capture **evolutionary system features** (e.g., requirements evolution, evolutionary dependencies, etc.) [Felici 2004]



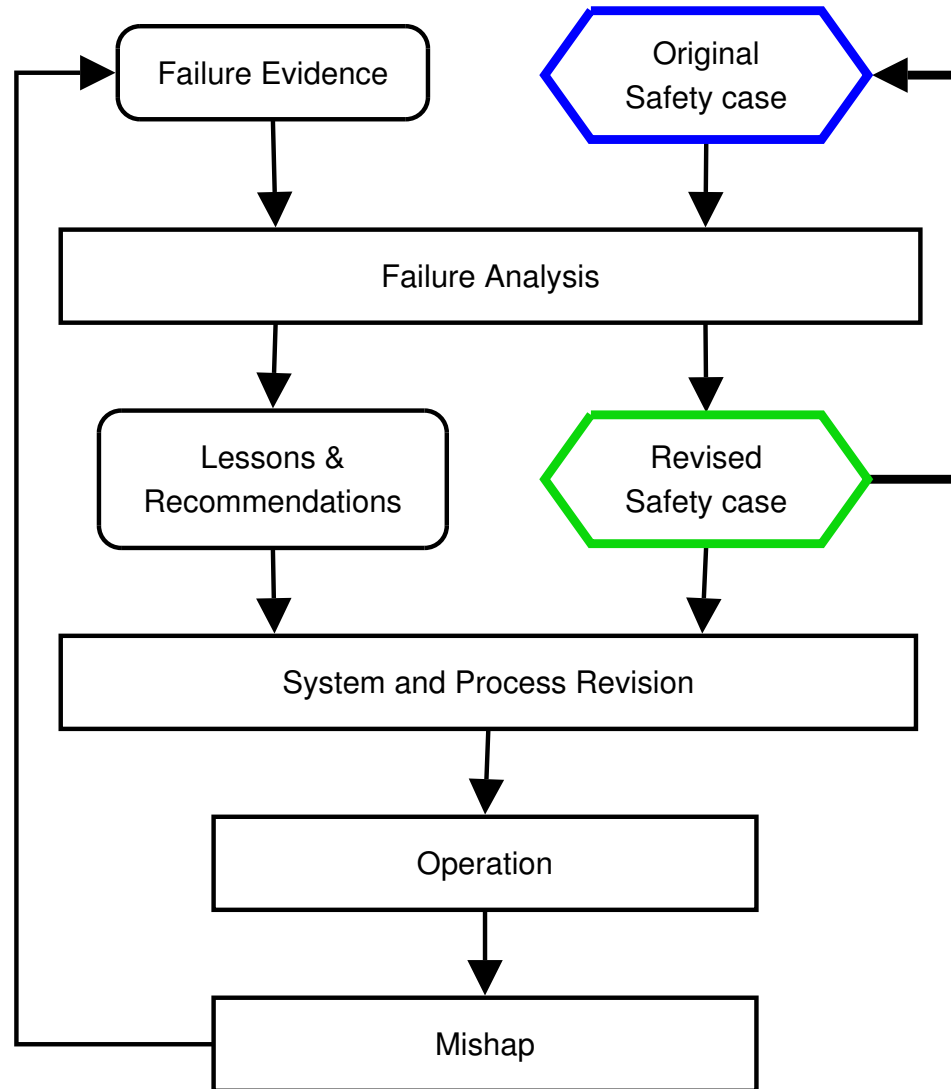
# Safety Analysis Modeling Transformation



- Safety arguments change, too
- Safety arguments may eventually become unclear
- Structured Safety arguments (e.g., GSN)



# A Safety-case Lifecycle [Greenwell, Strunk and Knight, 2004]



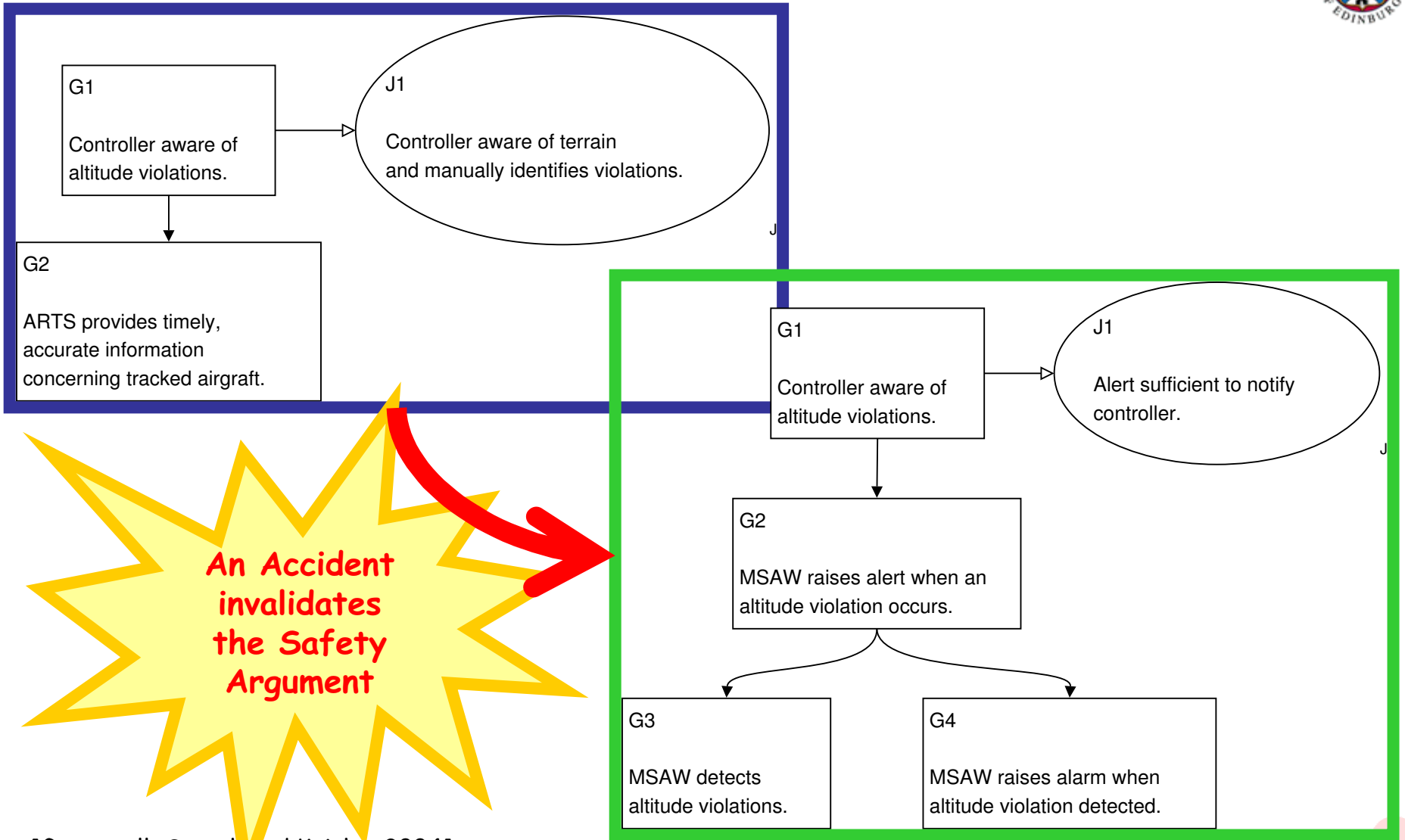
[Greenwell, Strunk and Knight, 2004]

© Massimo Felici 2005

Grand Challenge Workshop on Dependable Systems Evolution



# Safety Case Changes



**An Accident  
invalidates  
the Safety  
Argument**

[Greenwell, Strunk and Knight, 2004]

© Massimo Felici 2005

Grand Challenge Workshop on  
Dependable Systems Evolution

# Safety Case Changes in Practice



## A Difference Report

### Node differences

**Please note:** When analysing changes in Node narratives (HTML Content), only new and deleted sentences are shown. Formatting changes, moved sentences and copied/duplicated sentences are **not shown**.

#### Node N7737803 (N7737803 - J1) was changed

Node HTML narrative content was changed/edited.

Removed sentences	Inserted sentences
Controller aware of terrain and manually identifies violations. (approx 0% into document)	Alert sufficient to notify controller. (approx 0% into document)

#### Node N1813777 (N1813777 - G2) was changed

Node HTML narrative content was changed/edited.

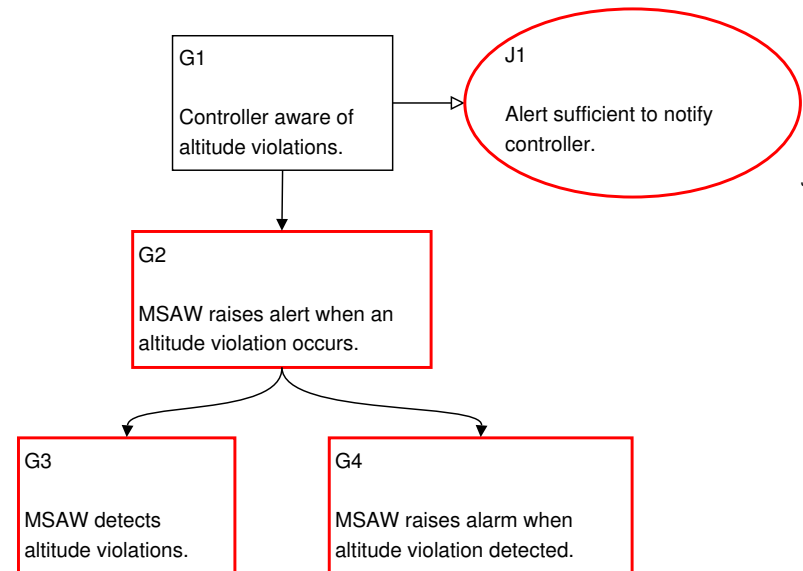
Removed sentences	Inserted sentences
ARTS provides timely, accurate information concerning tracked aircraft. (approx 0% into document)	MSAW raises alert when an altitude violation occurs. (approx 0% into document)

Supporting Link (type = [1]) from Node [N7822475 - G3] was added.  
Supporting Link (type = [1]) from Node [N8116556 - G4] was added.

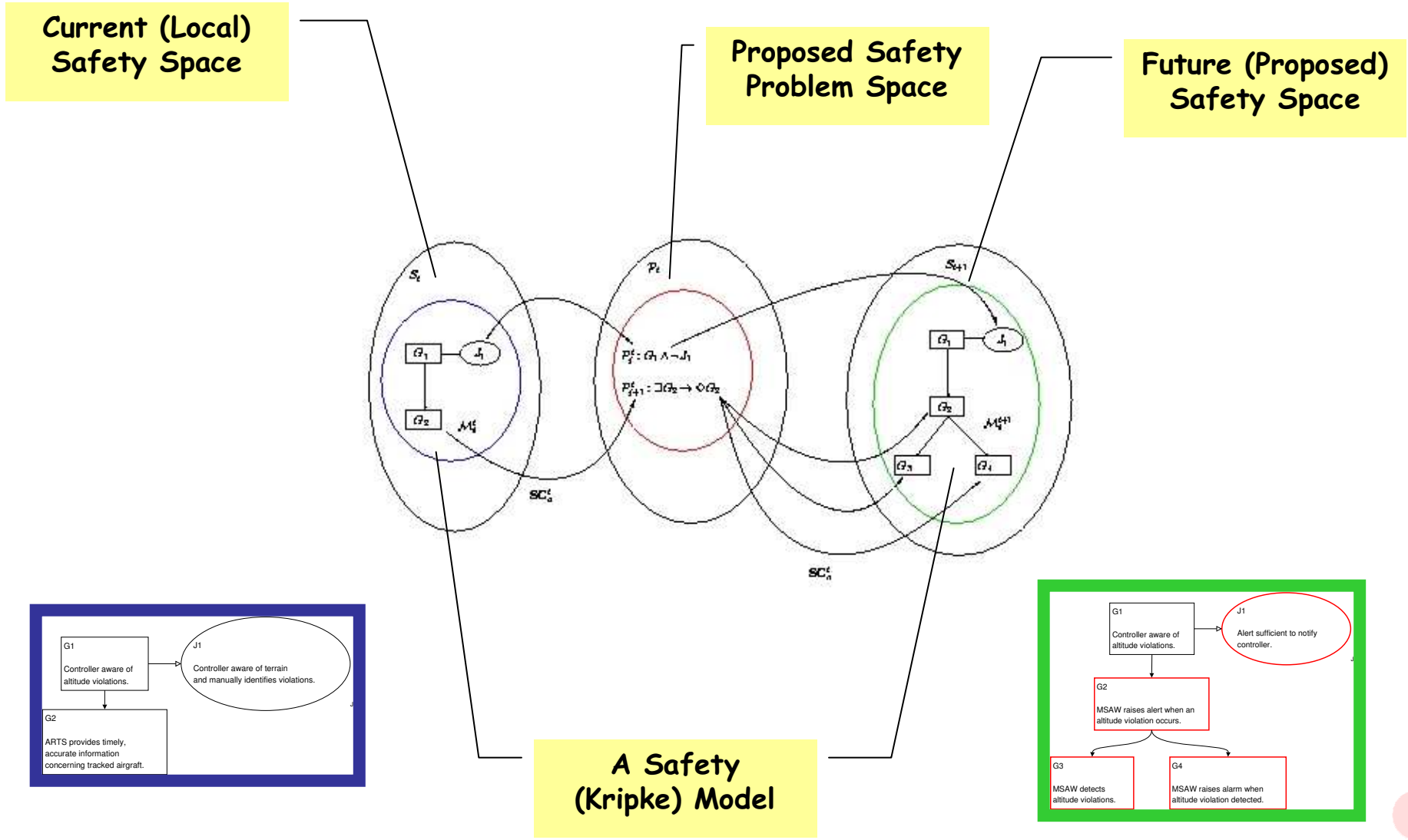
#### Node N7822475 (N7822475 - G3) was added.

#### Node N8116556 (N8116556 - G4) was added.

- The Adelard ASCE™ Difference Tool v1.1
  - ASCE: Assurance and Safety Case Environment
- Safety Case Changes



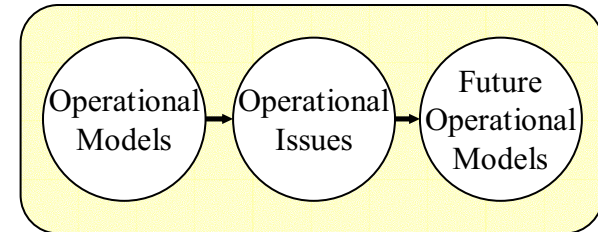
# Modeling Safety Case Changes



# Operational Modeling Transformation



- Structured Scenarios
- Pattern of interaction (changes)
- Work practice changes (e.g., workaround)



Problem Areas	Controller Reports	TCAS II Incidents
ATC Facility	2	
ATC Human Performance	44	39
Flight Crew Human Performance	26	40
Cabin Crew Human Performance	1	
Aircraft	3	10
Weather	4	3
Environmental Factor	8	6
Airspace Structure	5	18
Navigational Facility	6	4
Airport	5	5
FAA	3	5
Chart or Publication	1	
Maintenance Human Performance	1	
Company		1



# Operational Modeling Transformation



- Technically, **operational observations** are reported anomalies (or faults), which may trigger errors eventually resulting in failures
- **Erroneous actions** (Hollnagel, 1993): ``An erroneous action can be defined as an action which fails to produce the expected result and/or which produces an unwanted consequence''
  - In the context of socio-technical systems, erroneous actions usually occur in the interfaces or interactions (e.g., man-machine interactions).
  - The cause of erroneous actions can logically lie with either human beings, systems and/or conditions when actions were carried out
  - Erroneous actions can occur on all system levels and at any stage of the lifecycle.
- In a continuously changing environment like ATM, **adaption** enhances the coupling between man and machine (Hollnagel, 1995)
  - Adaption Through Design
  - Adaption through Performance
  - Adaption through Management



# Conclusions and Future Work



## → Modeling Safety Case Evolution

- Modeling Safety Case Evolution
- Formal Toll Extensions

## → Evolutionary Safety Analysis

- Support for Guidelines and Work Practice
- Organizational Knowledge and Safety Judgment

## Future work...

- Implementing an ASCE plugin that implements the Modeling Safety Case Changes
- What About Trust? How to understand the relationship between Trust, Risk and Knowledge (in ATM)?

