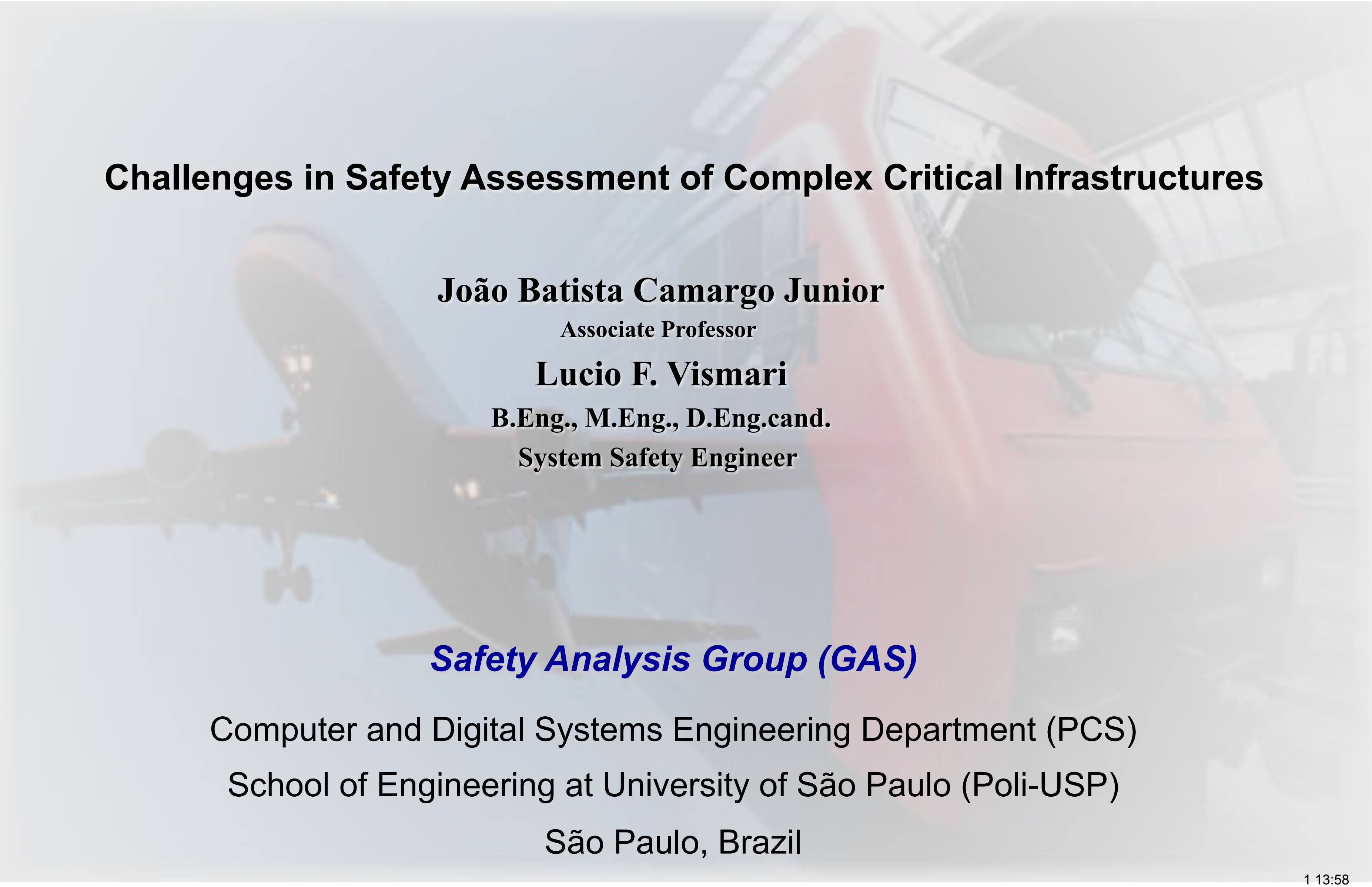


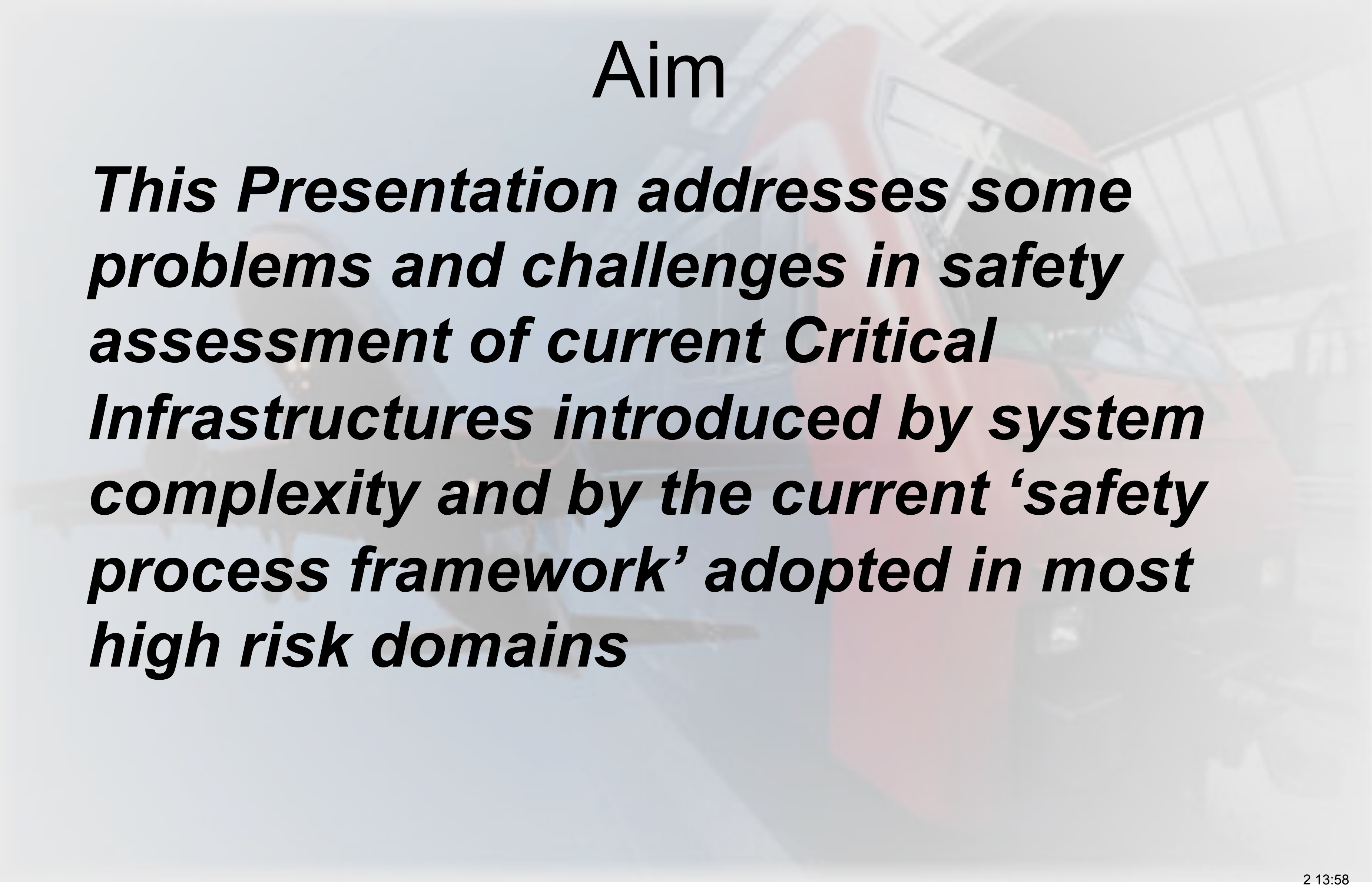
Challenges in Safety Assessment of Complex Critical Infrastructures

João Batista Camargo Junior
Associate Professor

Lucio F. Vismari
B.Eng., M.Eng., D.Eng.cand.
System Safety Engineer

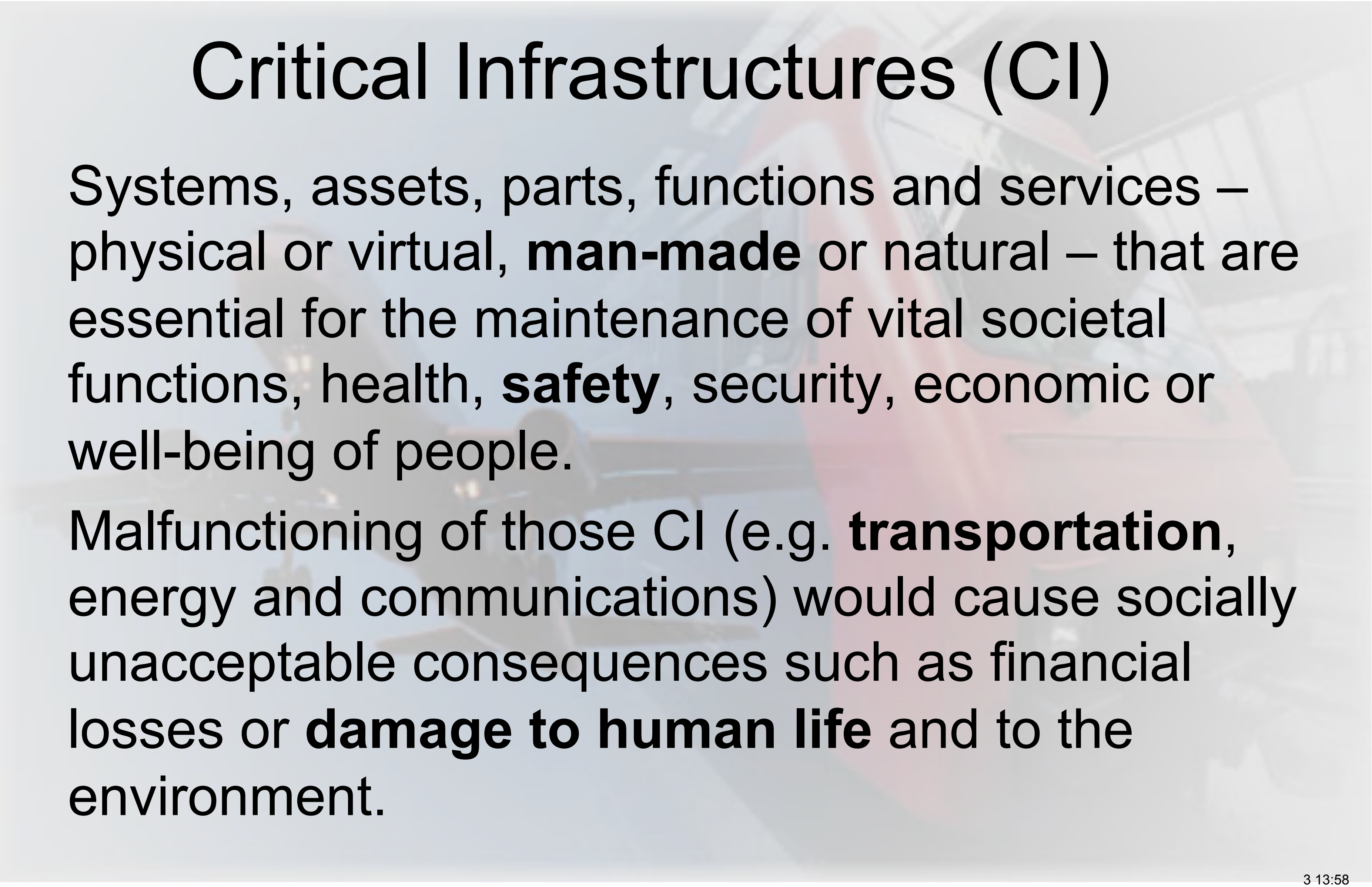
Safety Analysis Group (GAS)

Computer and Digital Systems Engineering Department (PCS)
School of Engineering at University of São Paulo (Poli-USP)
São Paulo, Brazil



Aim

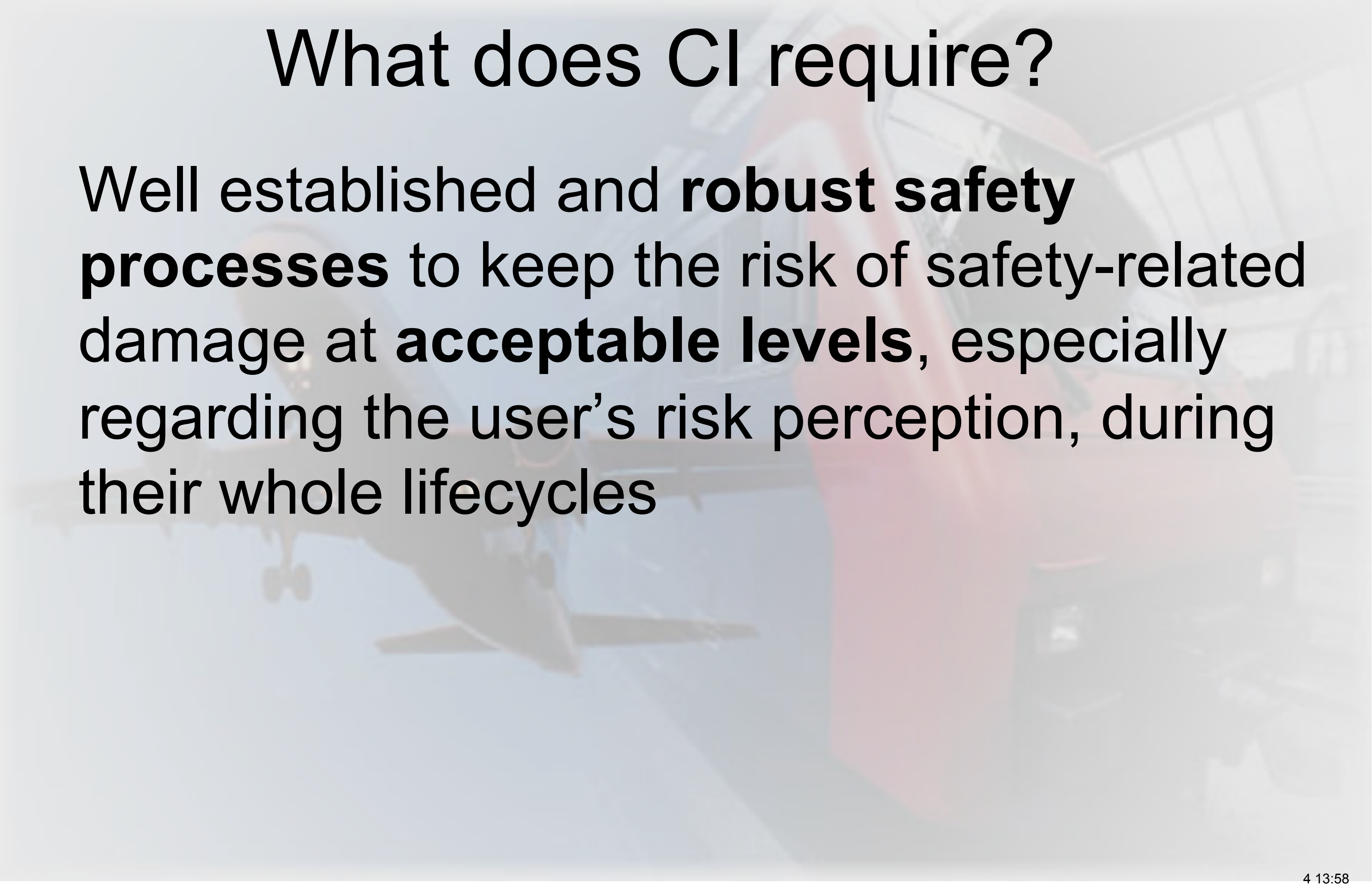
This Presentation addresses some problems and challenges in safety assessment of current Critical Infrastructures introduced by system complexity and by the current 'safety process framework' adopted in most high risk domains



Critical Infrastructures (CI)

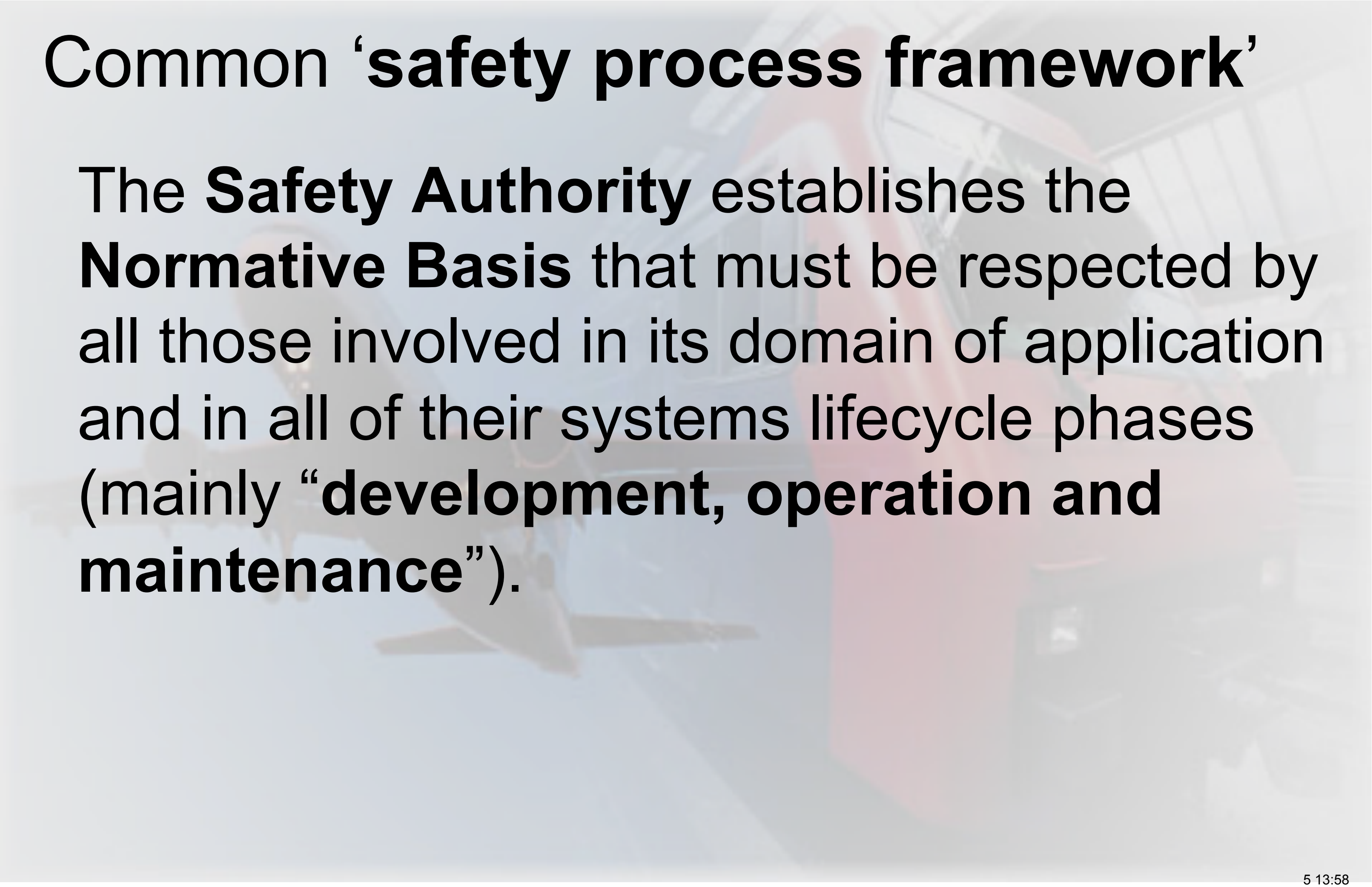
Systems, assets, parts, functions and services – physical or virtual, **man-made** or natural – that are essential for the maintenance of vital societal functions, health, **safety**, security, economic or well-being of people.

Malfunctioning of those CI (e.g. **transportation**, energy and communications) would cause socially unacceptable consequences such as financial losses or **damage to human life** and to the environment.



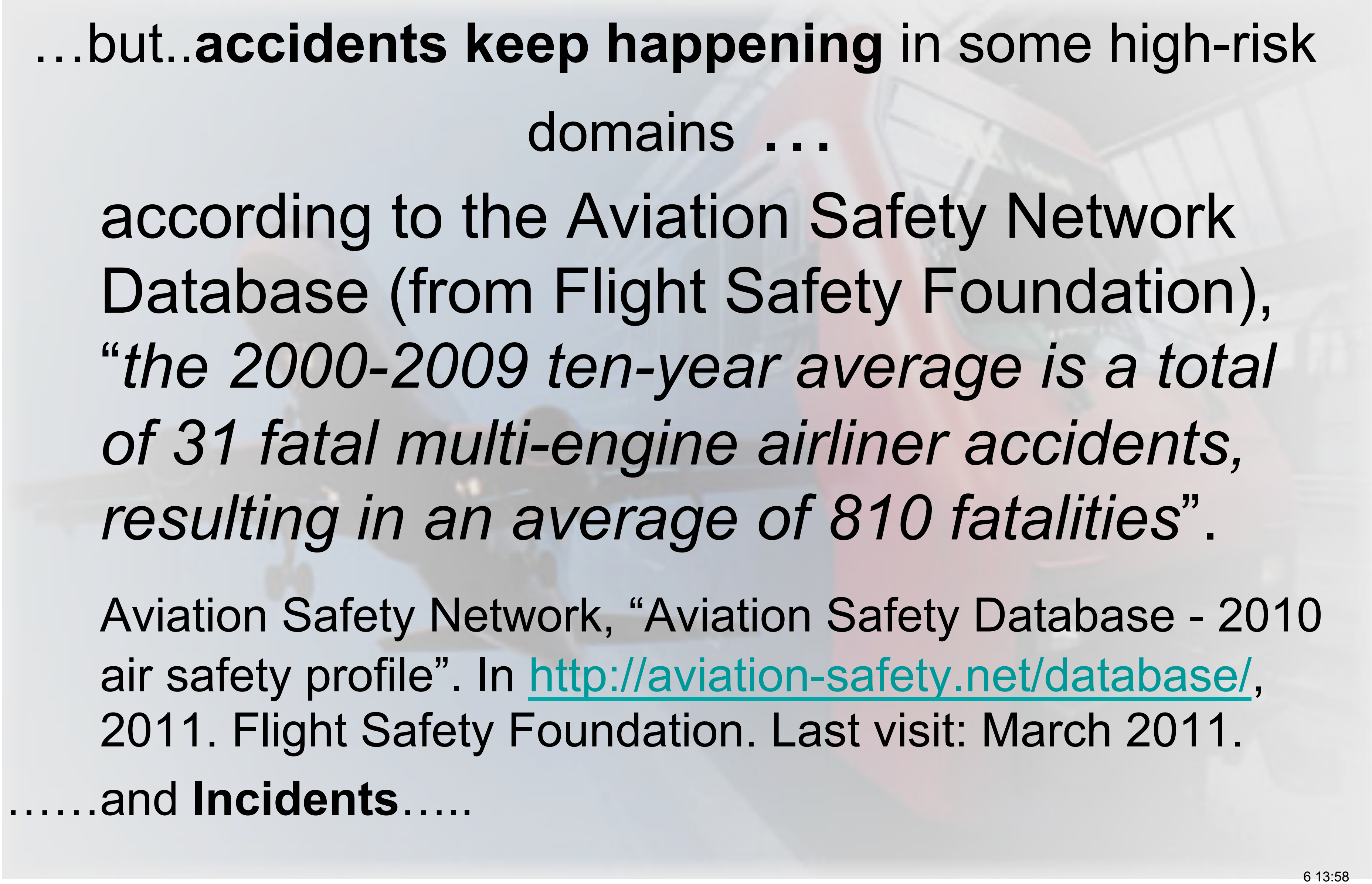
What does CI require?

Well established and **robust safety processes** to keep the risk of safety-related damage at **acceptable levels**, especially regarding the user’s risk perception, during their whole lifecycles



Common ‘**safety process framework**’

The **Safety Authority** establishes the **Normative Basis** that must be respected by all those involved in its domain of application and in all of their systems lifecycle phases (mainly “**development, operation and maintenance**”).

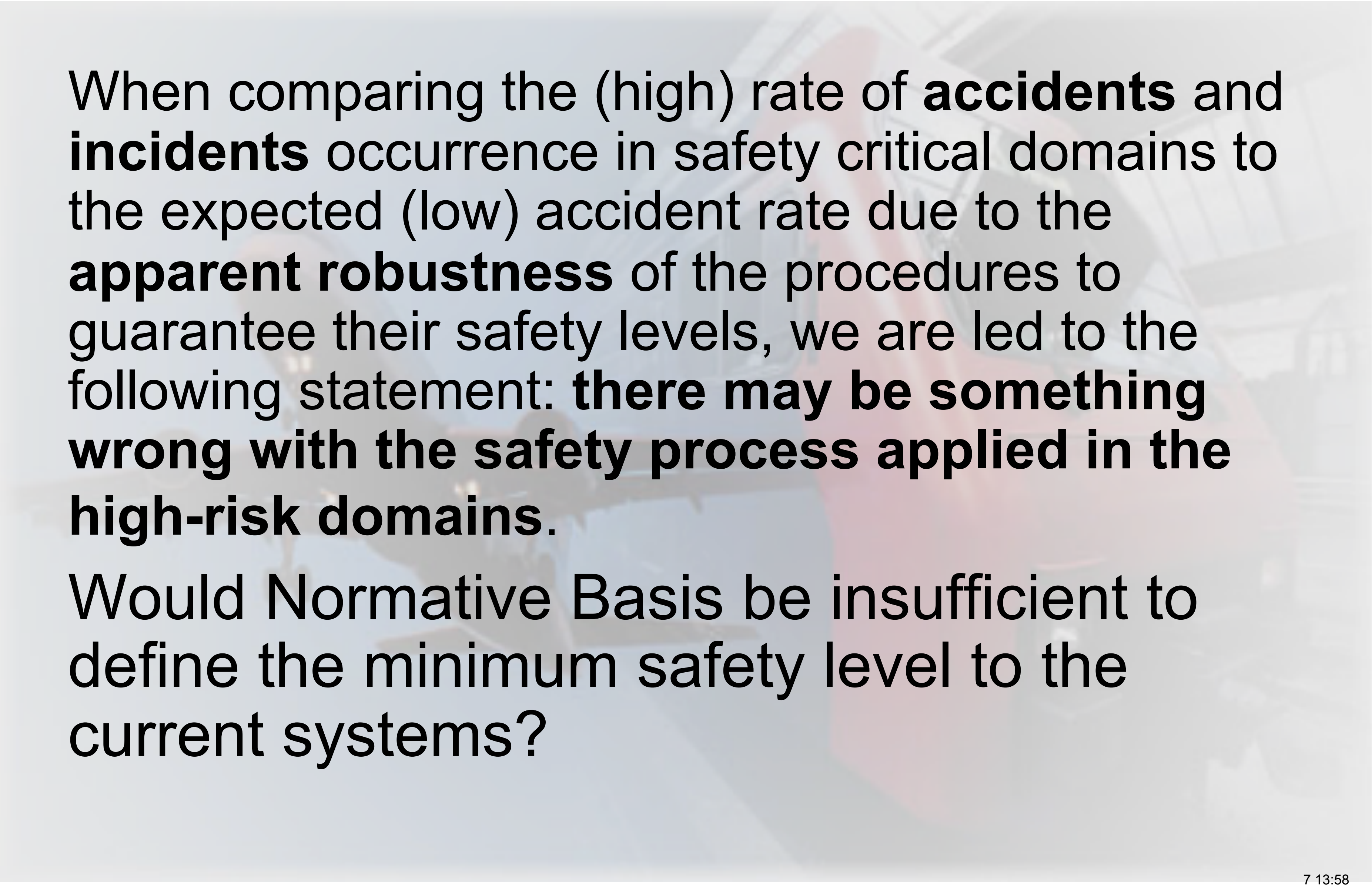


…but..**accidents keep happening** in some high-risk domains …

according to the Aviation Safety Network Database (from Flight Safety Foundation), "*the 2000-2009 ten-year average is a total of 31 fatal multi-engine airliner accidents, resulting in an average of 810 fatalities*".

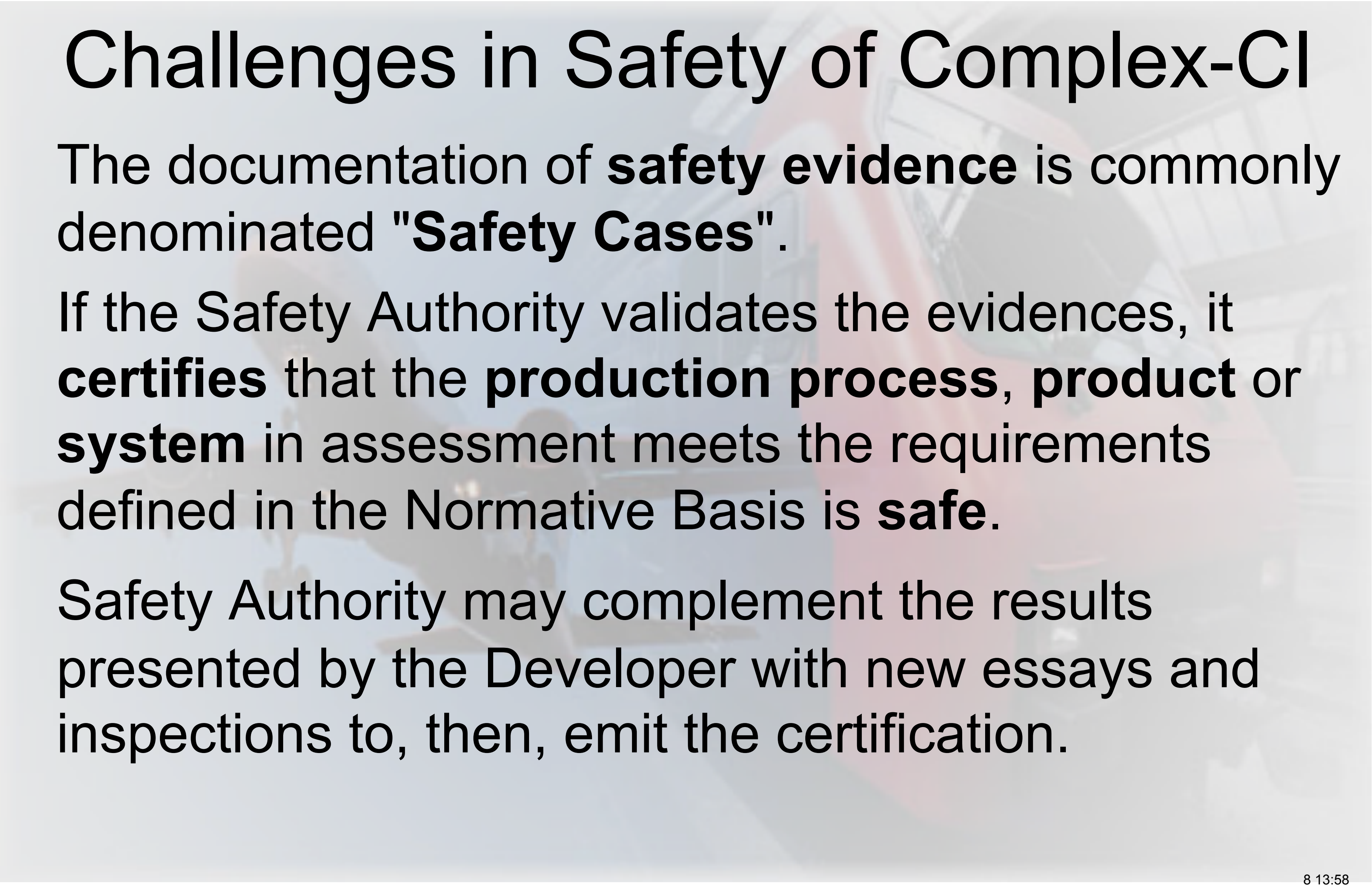
Aviation Safety Network, "Aviation Safety Database - 2010 air safety profile". In http://aviation-safety.net/database/, 2011. Flight Safety Foundation. Last visit: March 2011.

……and **Incidents**…..



When comparing the (high) rate of **accidents** and **incidents** occurrence in safety critical domains to the expected (low) accident rate due to the **apparent robustness** of the procedures to guarantee their safety levels, we are led to the following statement: **there may be something wrong with the safety process applied in the high-risk domains**.

Would Normative Basis be insufficient to define the minimum safety level to the current systems?

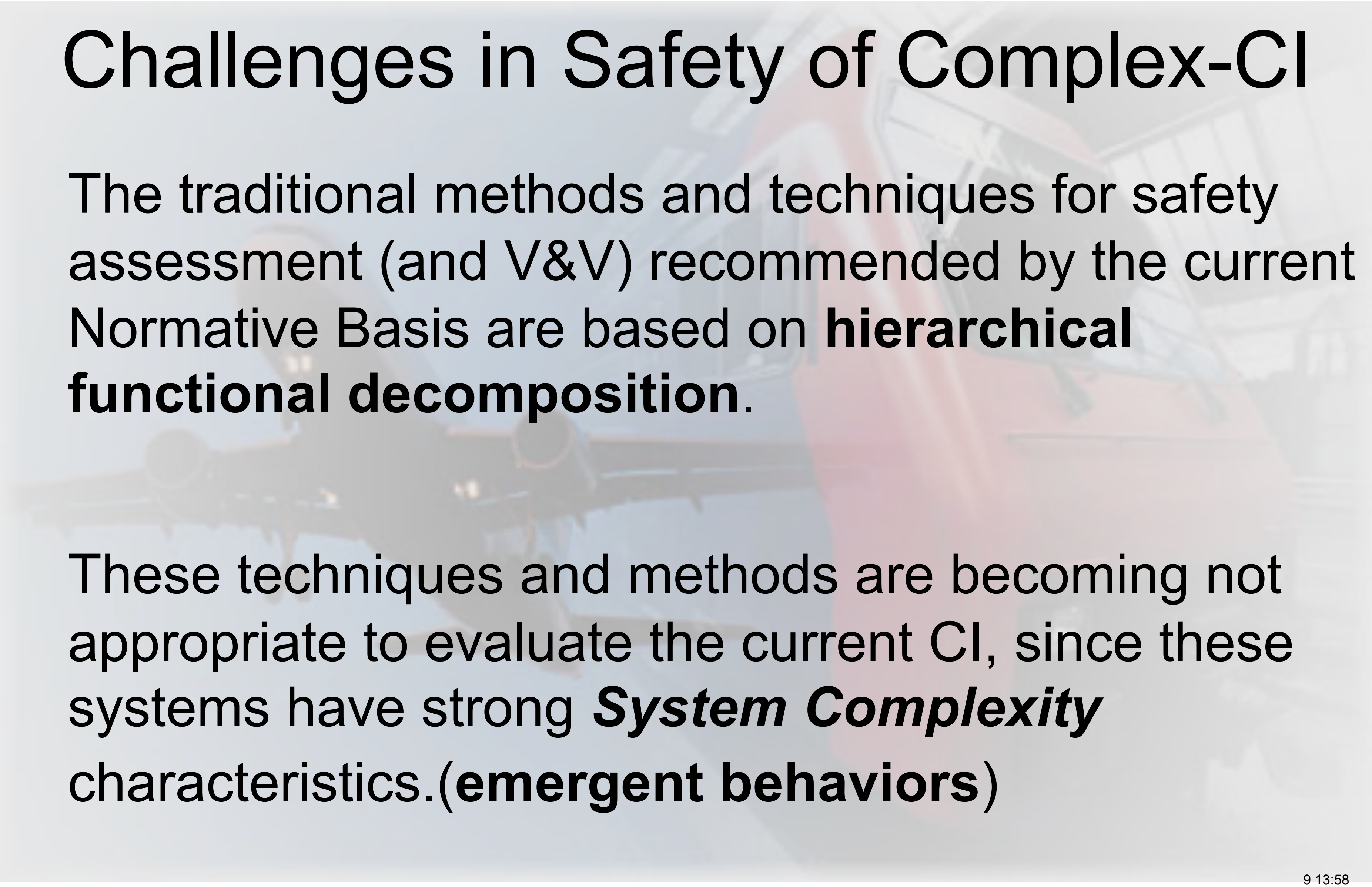


Challenges in Safety of Complex-CI

The documentation of **safety evidence** is commonly denominated "**Safety Cases**".

If the Safety Authority validates the evidences, it **certifies** that the **production process**, **product** or **system** in assessment meets the requirements defined in the Normative Basis is **safe**.

Safety Authority may complement the results presented by the Developer with new essays and inspections to, then, emit the certification.

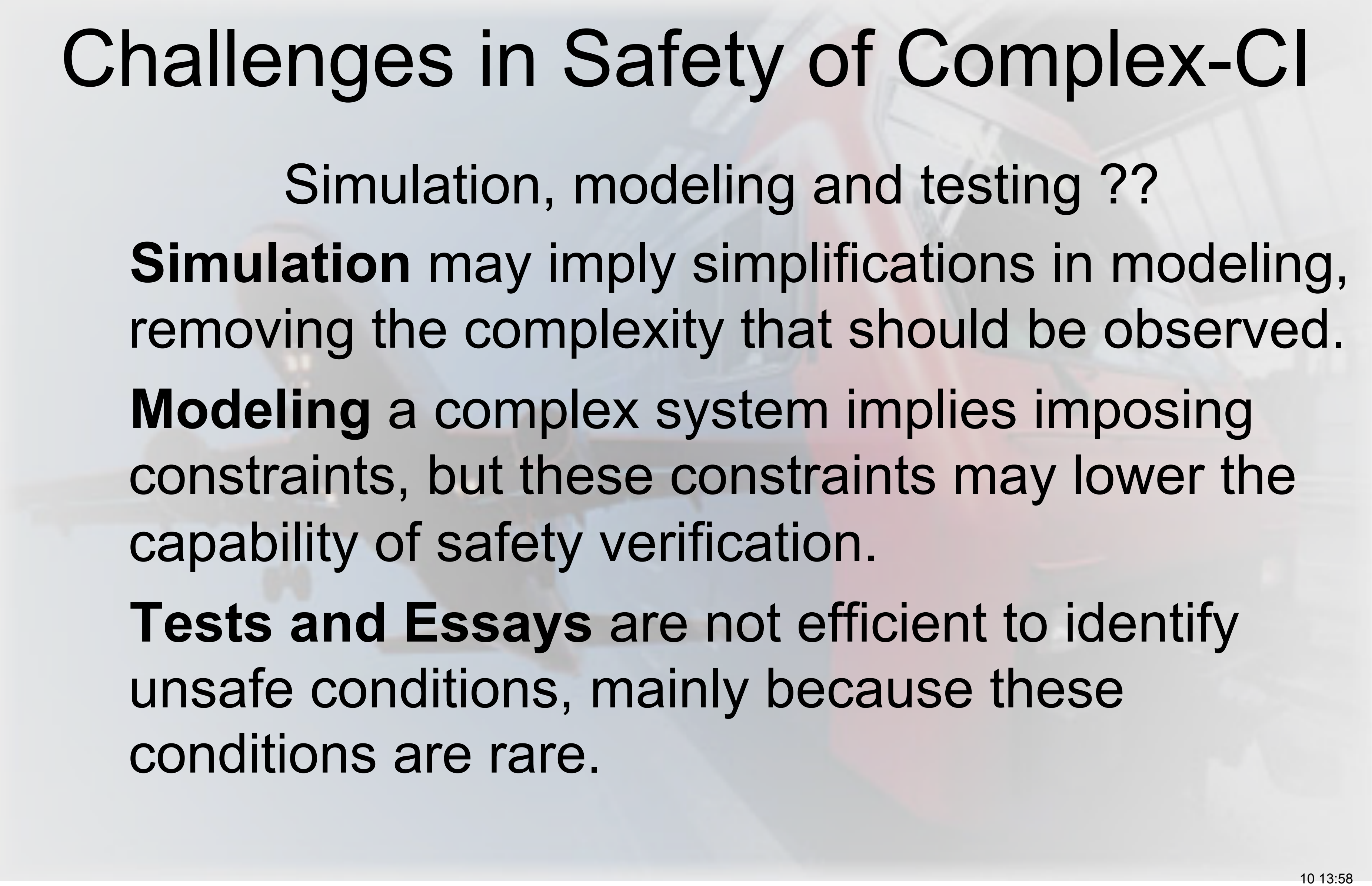


Challenges in Safety of Complex-CI

The traditional methods and techniques for safety assessment (and V&V) recommended by the current Normative Basis are based on **hierarchical functional decomposition**.

These techniques and methods are becoming not appropriate to evaluate the current CI, since these systems have strong ***System Complexity*** characteristics.(**emergent behaviors**)

Challenges in Safety of Complex-CI



Simulation, modeling and testing ??

Simulation may imply simplifications in modeling, removing the complexity that should be observed.

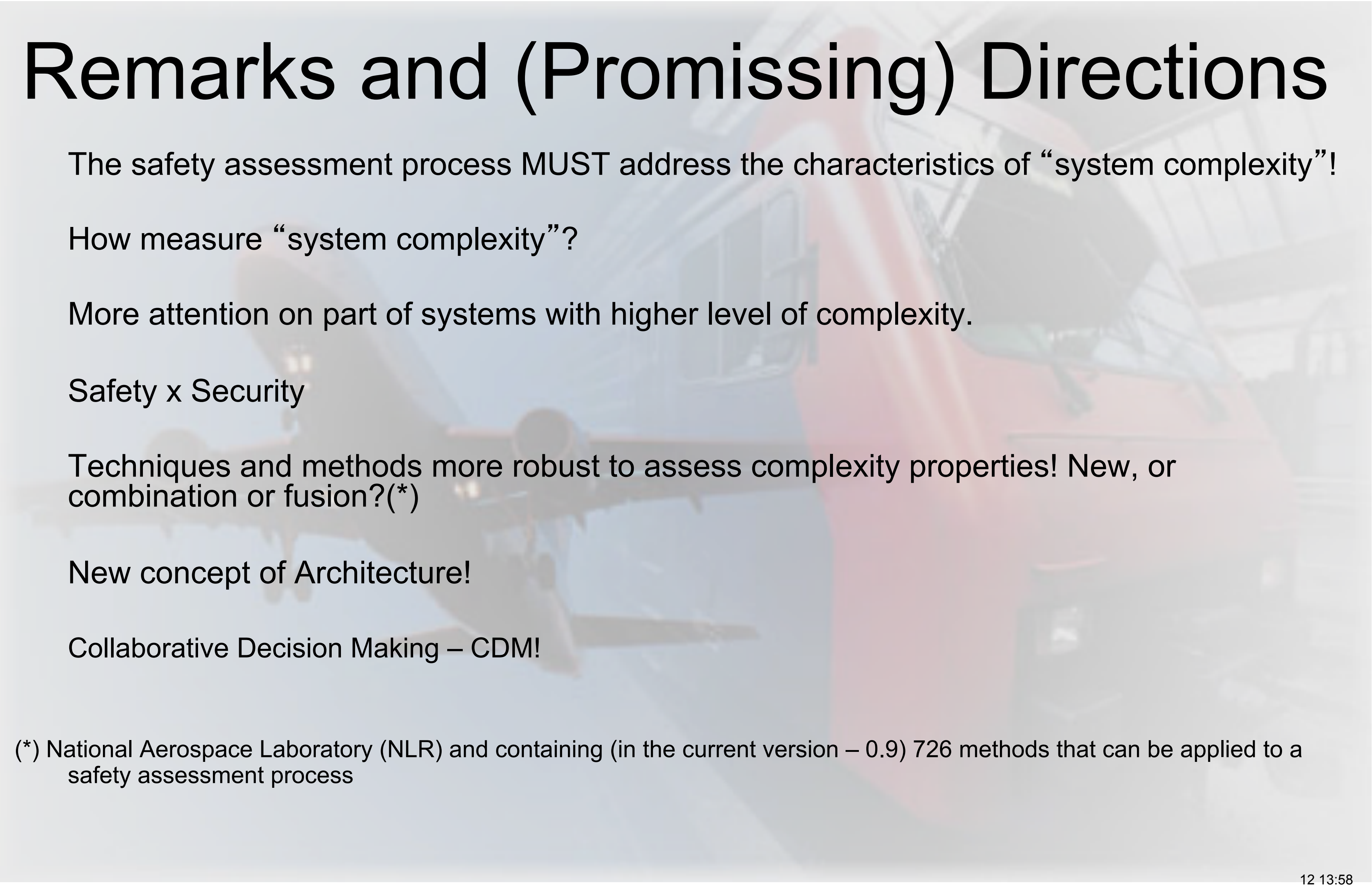
Modeling a complex system implies imposing constraints, but these constraints may lower the capability of safety verification.

Tests and Essays are not efficient to identify unsafe conditions, mainly because these conditions are rare.

Challenges in Safety of Complex-CI

The trend is that the techniques and methods for safety assessment recommended by the Normative Basis will more and more become **less effective** in identifying unsafe conditions in our "**increasing complex world**".

Remarks and (Promissing) Directions



The safety assessment process MUST address the characteristics of “system complexity”!

How measure “system complexity”?

More attention on part of systems with higher level of complexity.

Safety x Security

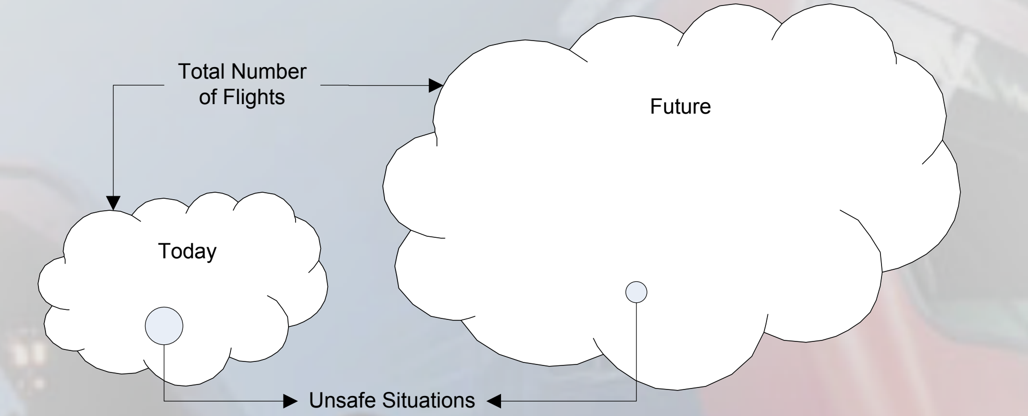
Techniques and methods more robust to assess complexity properties! New, or combination or fusion?(*)

New concept of Architecture!

Collaborative Decision Making – CDM!

(*) National Aerospace Laboratory (NLR) and containing (in the current version – 0.9) 726 methods that can be applied to a safety assessment process

Examples - Future Scenery



The ICAO (International Civil Aviation Organization) GLOBAL AVIATION SAFETY PLAN - GASP (2004)

The aims of the ICAO GASP are to:

a) reduce the number of accidents and fatalities worldwide <u>irrespective</u> of the volume of air traffic; and

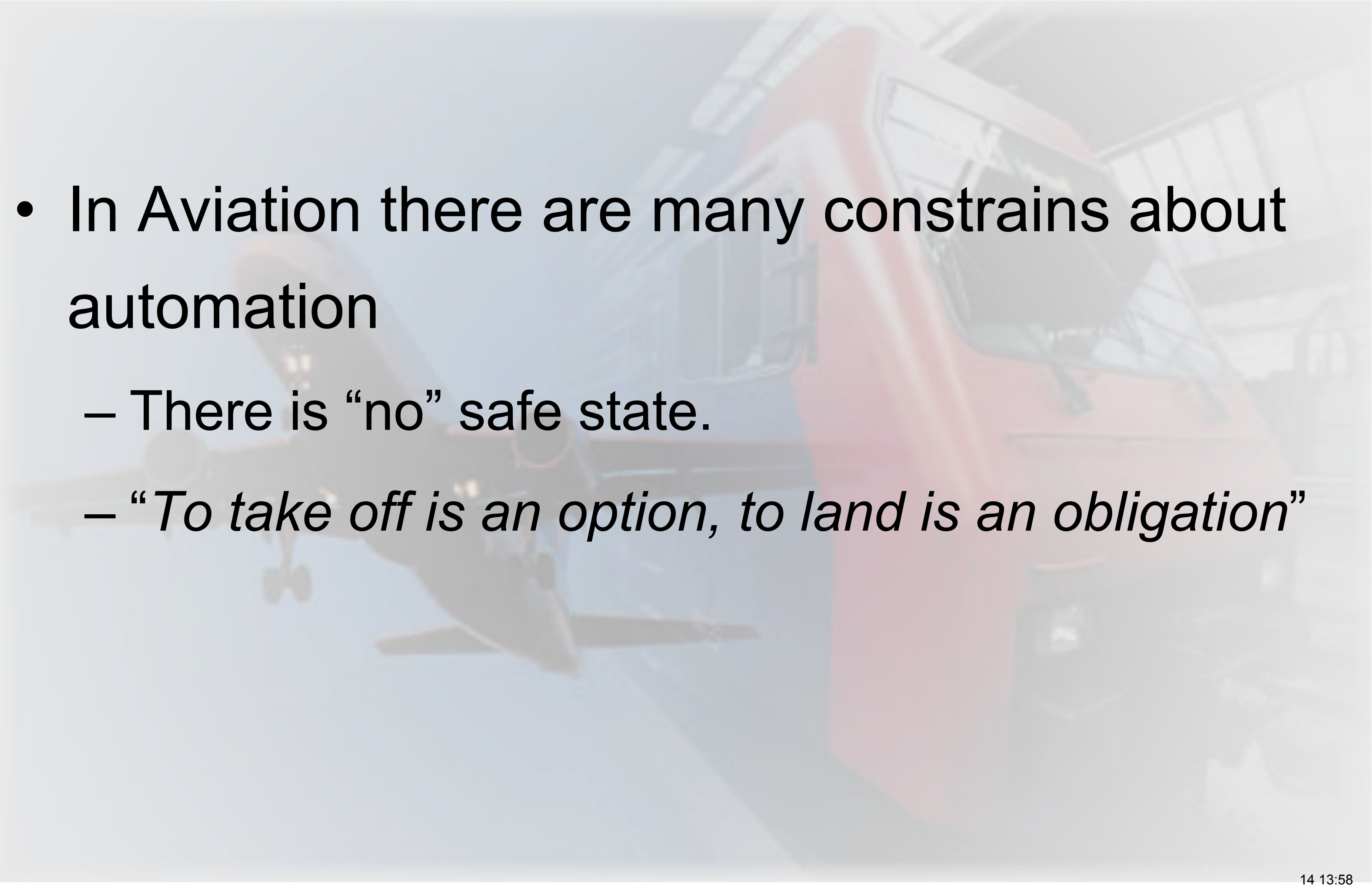
b) achieve a significant decrease in accident rates, particularly in regions where these remain high.

SESAR - *Single European Sky ATM Research Programme:*

By 2025, demand is expected to be 2.4 times higher than today

Diversity in the types of airspace users *(e.g., low-cost airlines, general & business aviation, unmanned aerial vehicles)* is expected to continue to grow

Goal for 2020: improve the safety performance by a factor of 10!!



- In Aviation there are many constrains about automation
  - There is “no” safe state.
  - “*To take off is an option, to land is an obligation*”