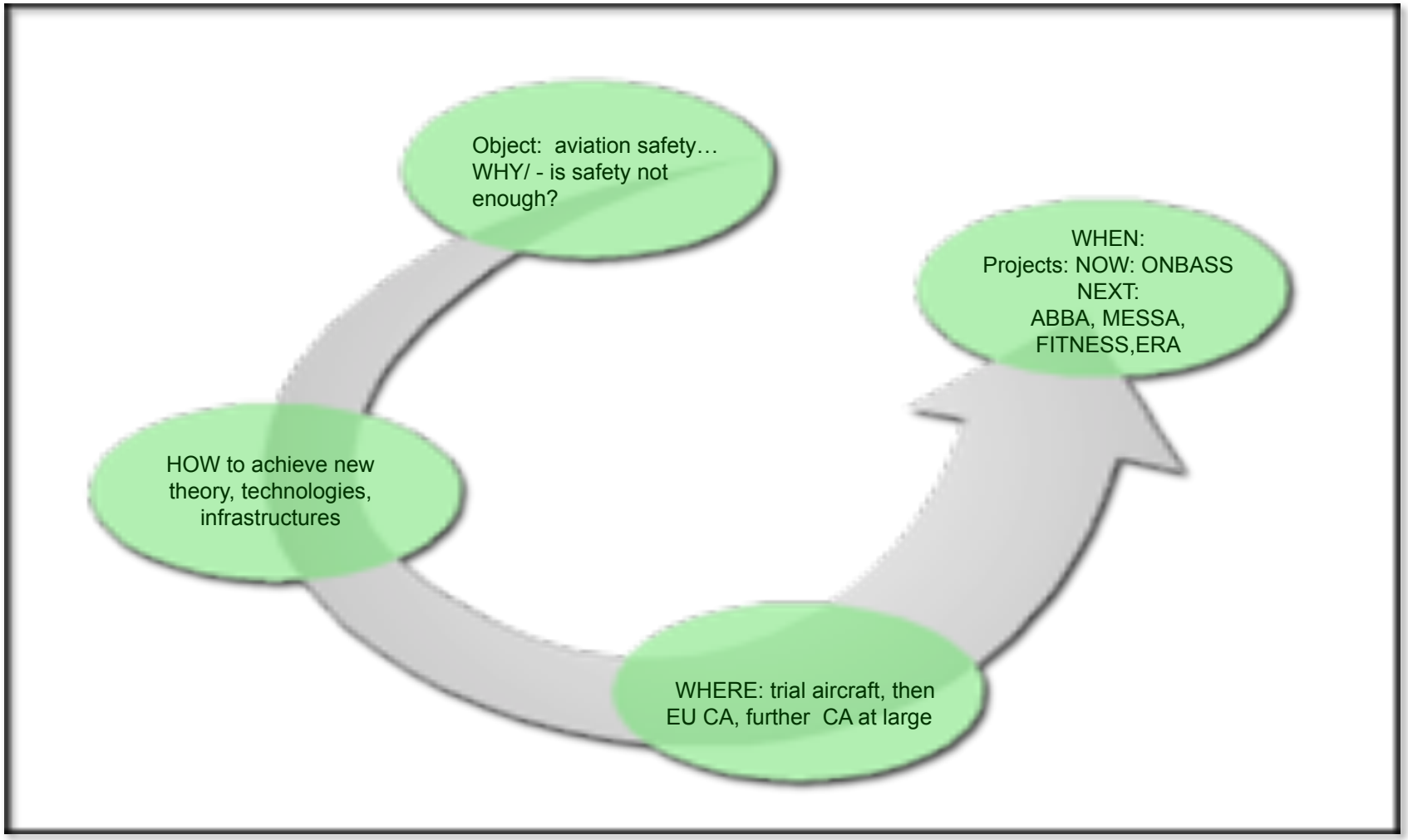
Principle of Active System Safety:

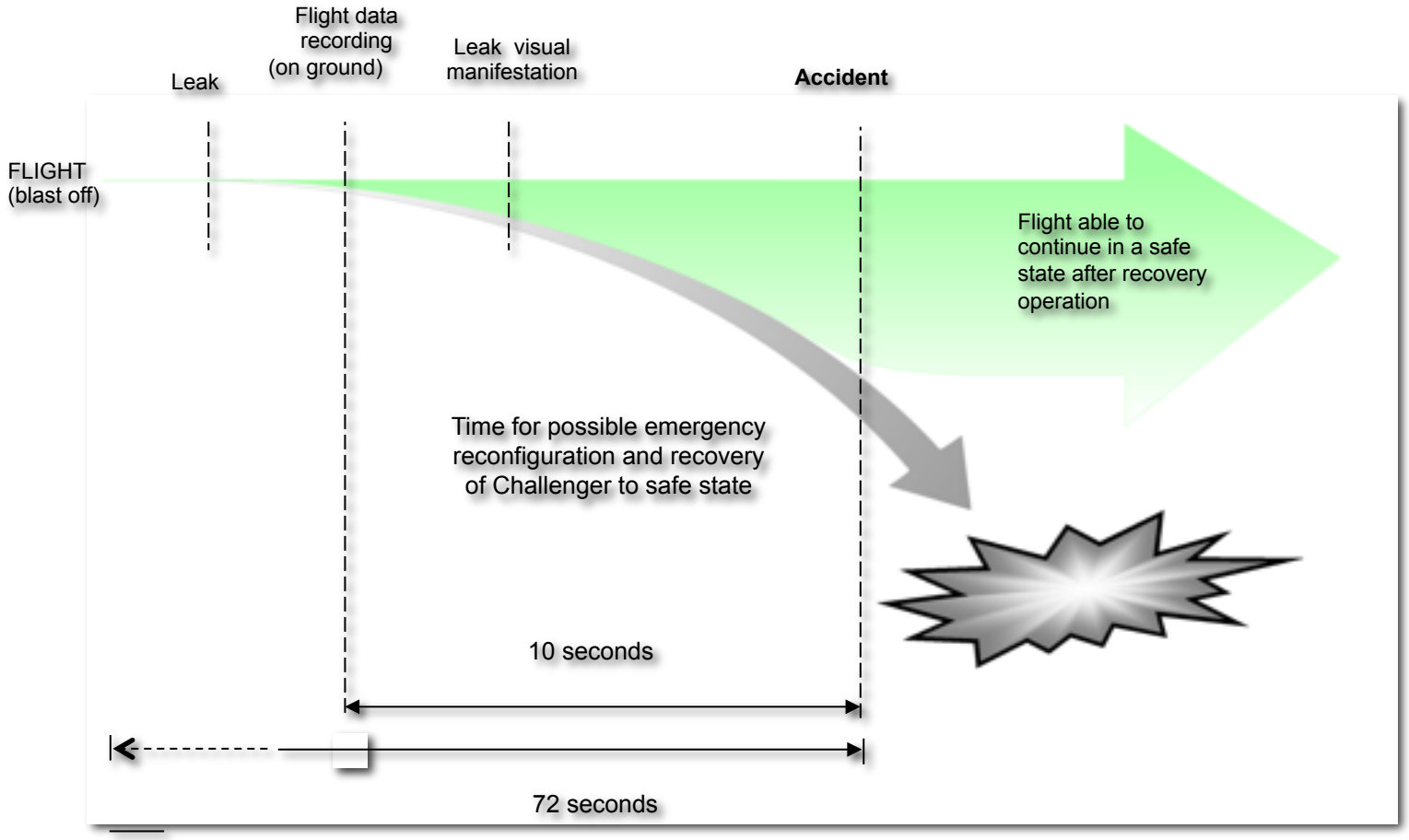
Challenges, Supportive Theory, Implementation, Application and Future

itacs ltd

active safety for aviation: plan



safety accident aspect



classification of aircraft vs. safety

…classification aiming a formation of technical portrait of a typical aircraft including design, technological and management features;
…they altogether have substantial impact on aircraft reliability, maintainability, and, therefore, safety.

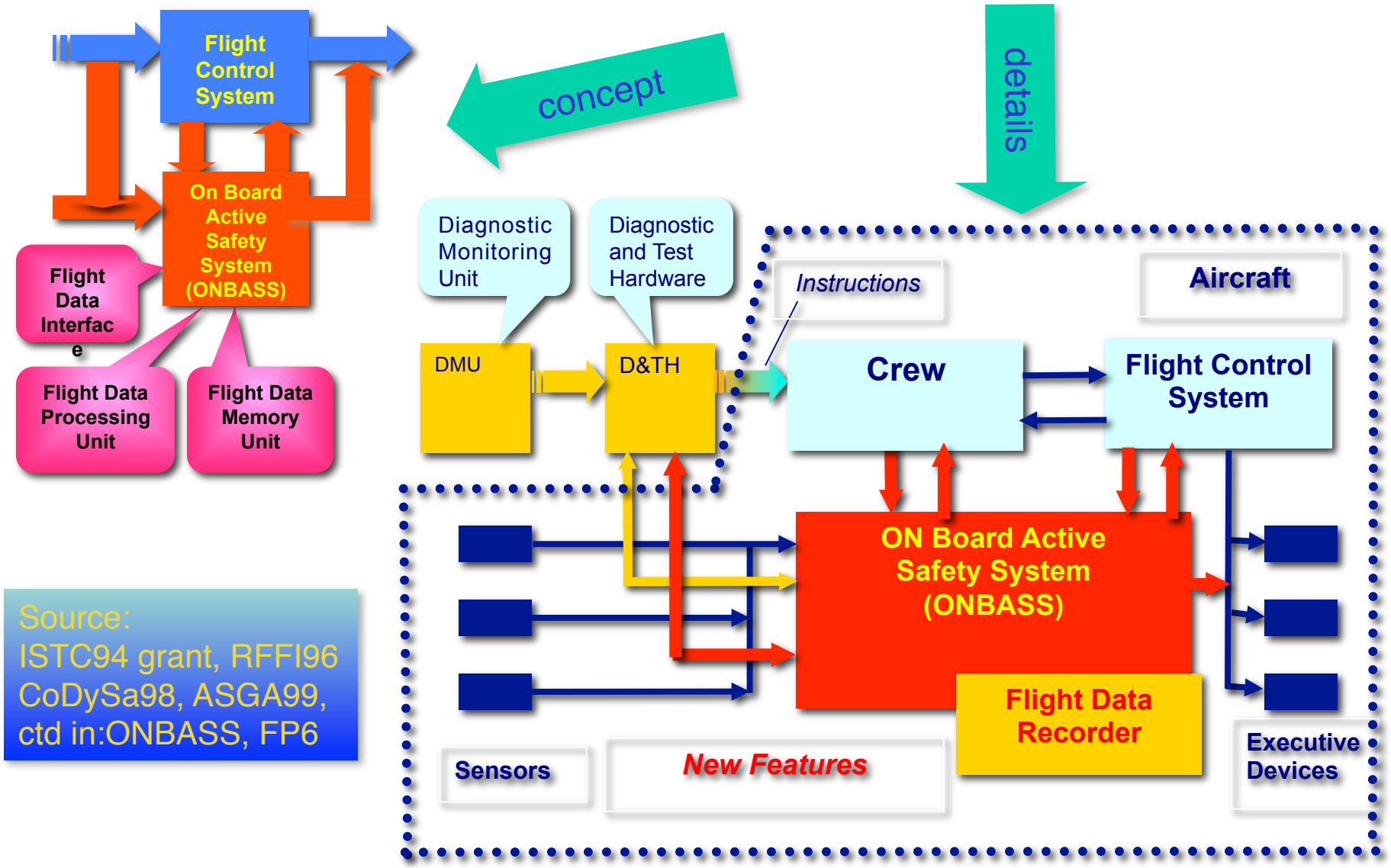
…Existing schemes of safety management in aviation are either conservative or oriented on strategic goals and after flight (accident) analysis (CA, military) or do not exist (GA).
…All these schemes are easily avoidable by aircraft owners and users, as they depend upon 'human' factor (*the weakest link in the chain can't be relied on to fix the chain*)…

PASS definition

PASS is an approach to continuously evaluate and process the state of an aircraft in real time of flight to define when necessary appropriate RT recovery action or the most efficient scheme of graceful degradation

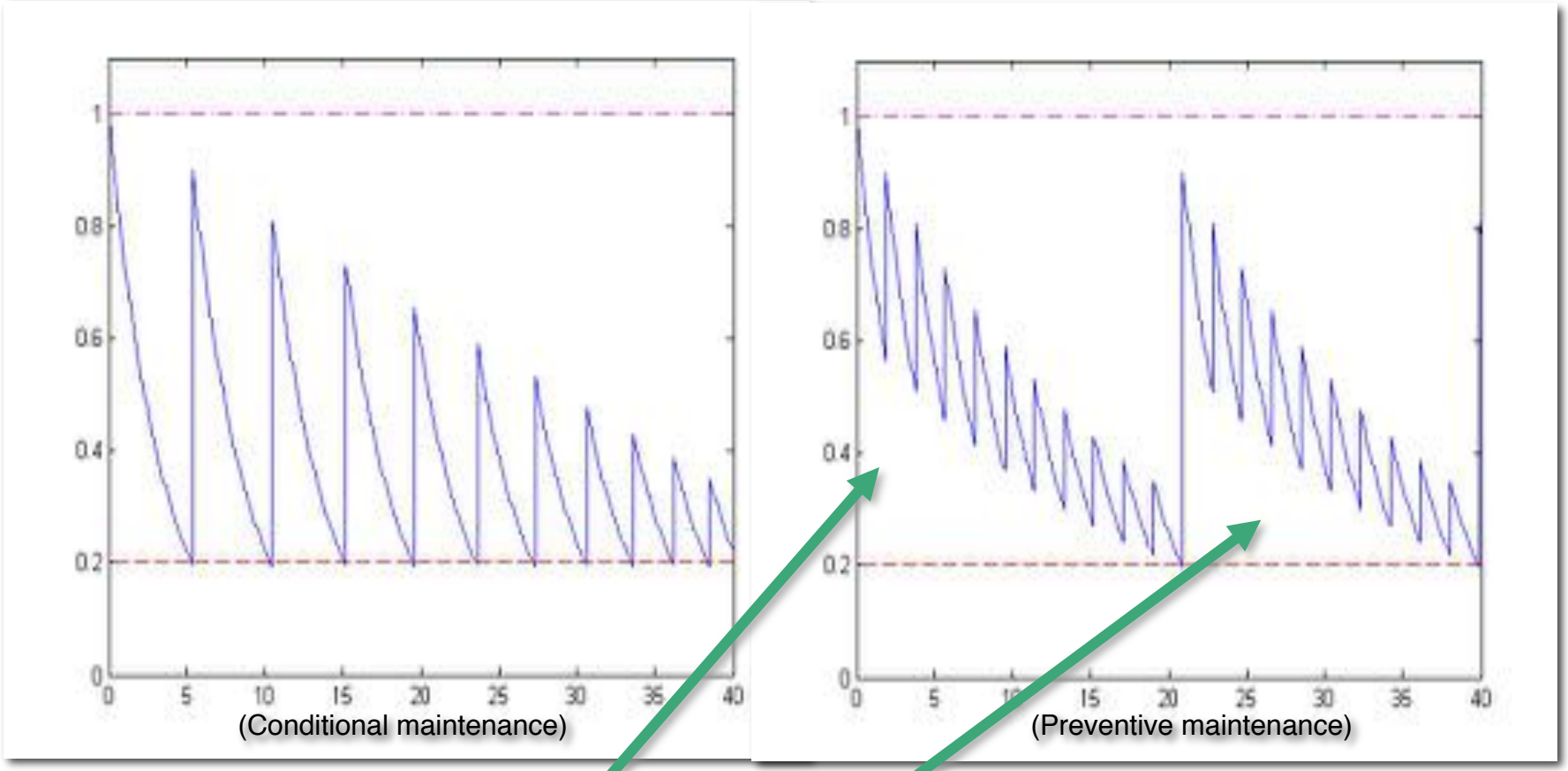
- Implementation of PASS for GA and further CAA
- Process-oriented Information model: object, elements, flight data and predicates
- Dependency and Recovery matrices (DM, RM)
- Method of active system safety and it's algorithms

PASS in the medium - schemes



Source:
ISTC94 grant, RFFI96 CoDySa98, ASGA99, ctd in:ONBASS, FP6

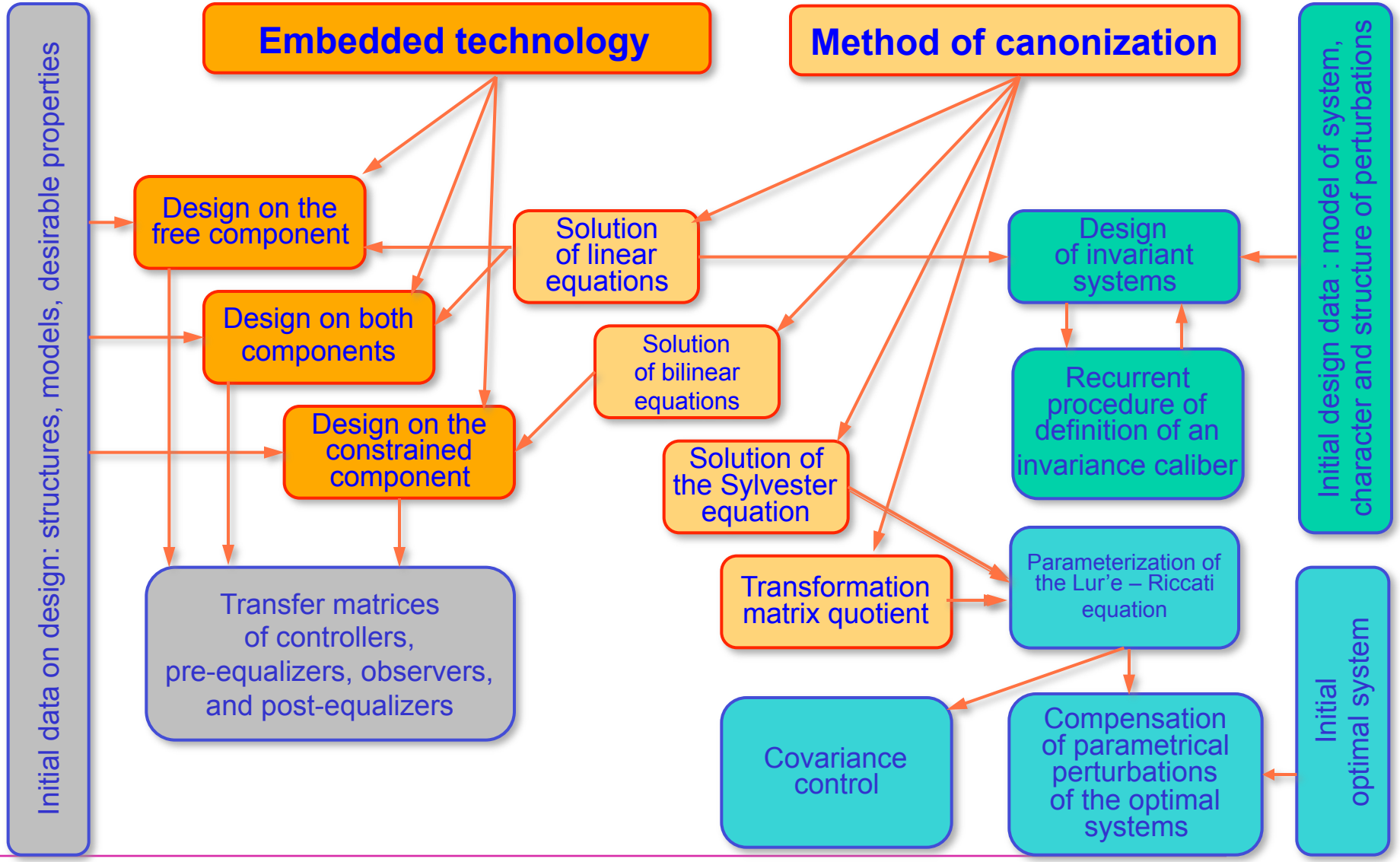
PASS vs.conditional and preventive maintenance



PASS "profit" is here and here…

besides, PASS is possible…

PASS when we do know models…



PASS when we don't know models

- Dependency matrix (topologic, functional,electric)
- elements, recovery matrix

Practice speak louder:

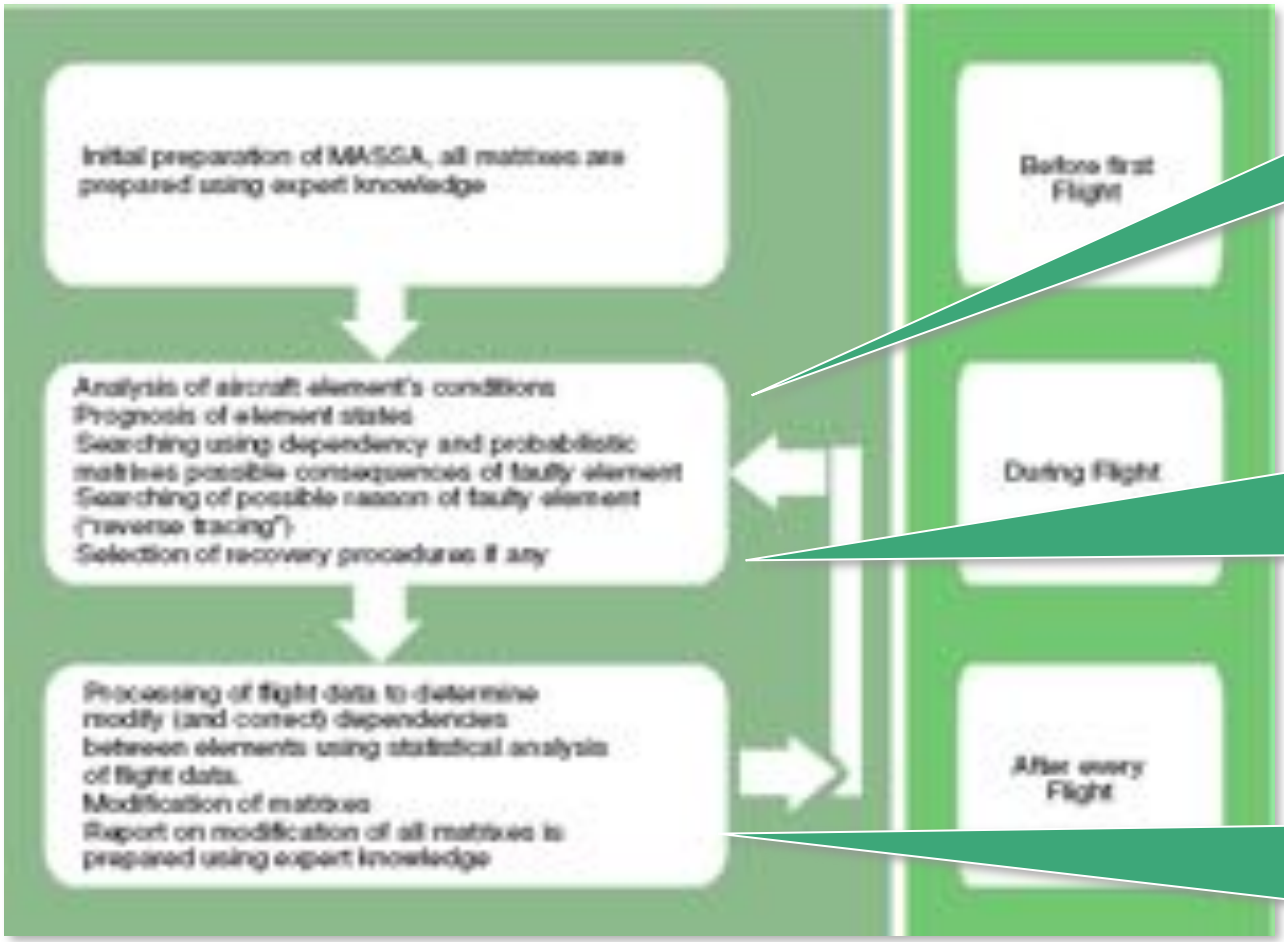
- When there are symptoms that system is faulty (with differences or deviations from scheduled scheme, behaviour or rules) it is required to determine "guilty" element(s)
- Known solutions for the localization problem are based on very strong assumptions about analyzed system (see analytic equations) and information about fault models
- Practice vote for multiple fault assumptions
- Probabilistic models using for *location* of faulty element for real time systems are not always adequate, recovery and(or) graceful degradation needs monitoring, thus…

New model of active system safety is required…

MASSA vs. FTA

	FAULT TREE ANALYSIS	COMMENT/REQUIREMENTS
1	The class of all faults is known before operation of the application	The class of faults changes during the life cycle of a system (of its objects) due to ageing, maintenance or external reasons.
2	Fault tree analysis is static, developed during design of the objects and sub-systems	Dependence between elements of the system is reflected in dynamic changes of structure and significance.
3	Fault trees are known from design time are applied after events/accidents to detect and understand the cause(s) using expert opinion	Structure of dependence is becoming variable and must be updated during life cycle using existing and updated information; otherwise the predictive power of prognosis is reduced.
4	Number of fault trees, and their interactions, is growing quickly with complexity of a system	The possibility to identify, keep and manage of all possible scenarios and fault trees for any system of objects of reasonable complexity is disputable in practice.
5	Markov Processes are used to analyze outcome of the flow of events	A realistic model of the system might not be Markovian: the rate of transitions is changing, as well as importance of consequences and the possibilities for recovery and or repair before harm is inflicted.
6	Mutual exclusion of possibilities are applied for event analysis	The consequences of many common events ARE NOT MUTUALLY EXCLUSIVE. Another more realistic model is required.
7	There is no possibility to use FTA in real time of system operation	A model for prognosis of the system behaviour MUST be used in real-time to take account the operational state of the system

Model of active system safety: MASSA



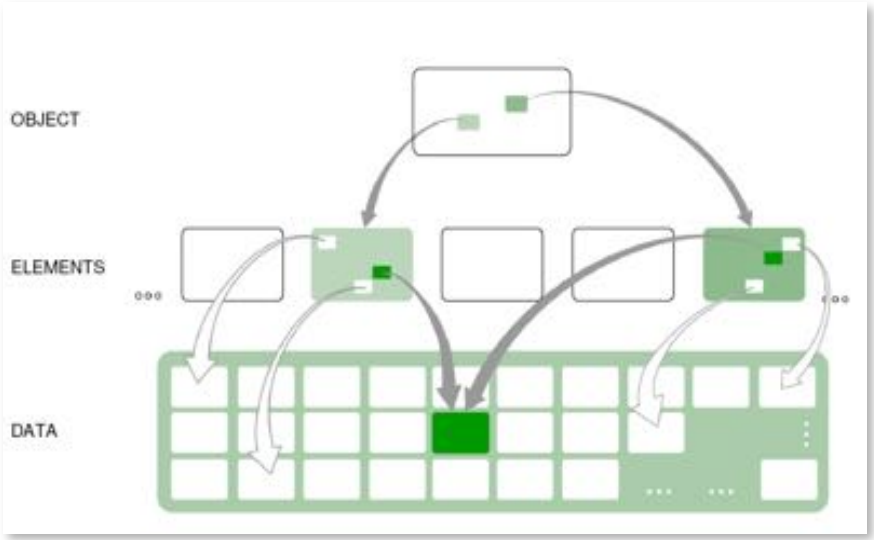
Models of elements are required

Performance of MASS should be evaluated (β estimation)

Effective statistical models of mutual dependence

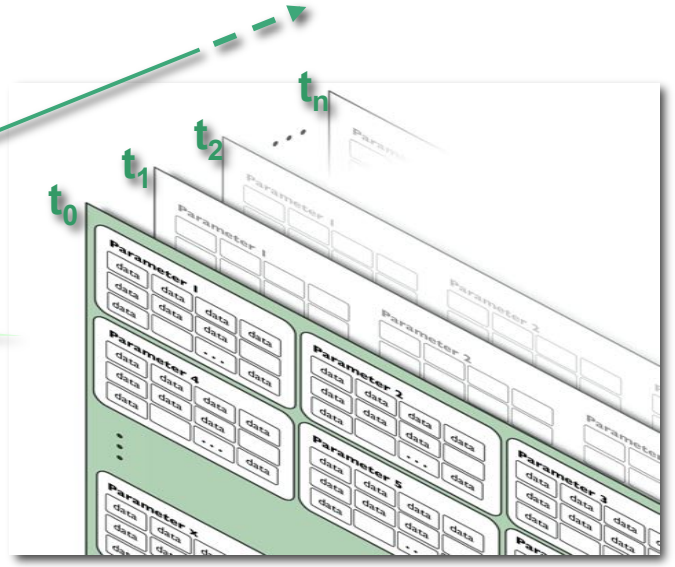
Source: © Deliverable 1.2, ONBASS 2006, FP6

PASS – Model and Flight Data



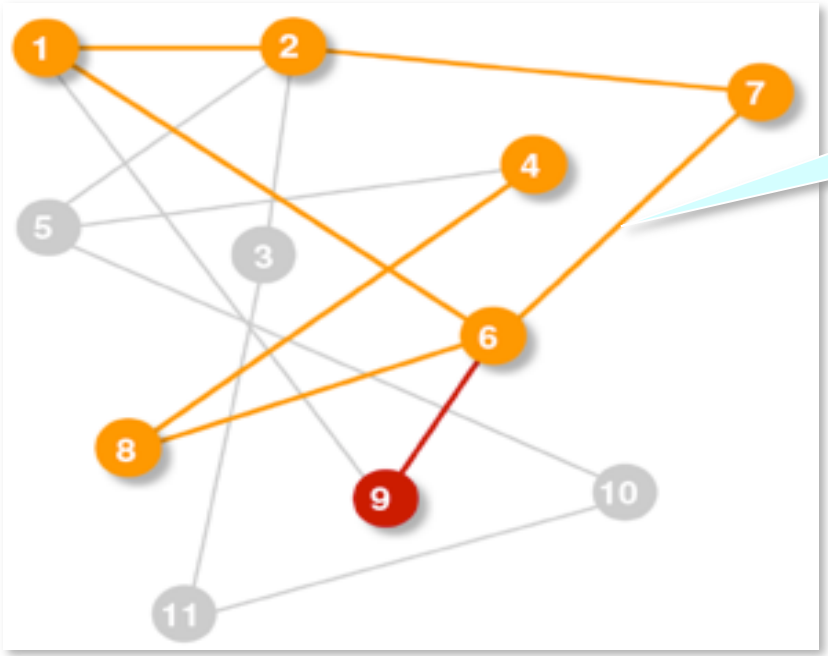
This is what we model…

This is what we record…



Source: © Deliverable 1.2, ONBASS 2006, FP6

PASS – In The Medium: Matrix

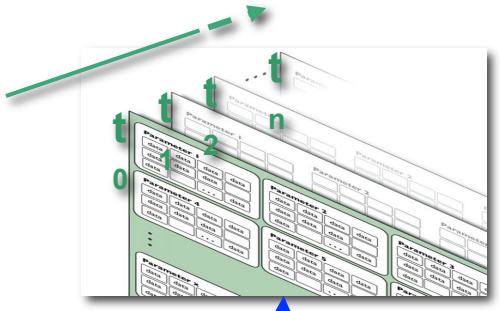


Probabilities of link activation, (dependency of elements)

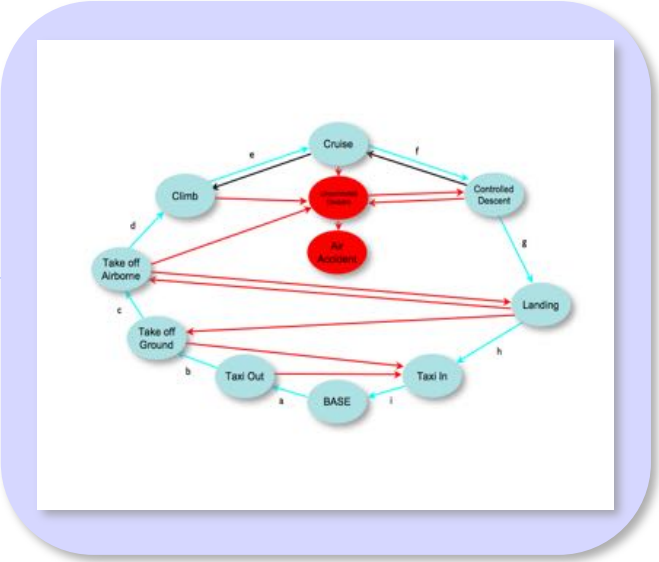
	1	2	3	4	5	6	7	8	9	10	11
1	P_{11}	P_{12}				P_{16}			P_{19}		
2	P_{21}		P_{23}		P_{25}		P_{27}				
3		P_{32}									$P_{3,11}$
4					P_{45}			P_{48}			
5		P_{52}		P_{54}						$P_{5,10}$	
6	P_{61}						P_{67}	P_{68}	P_{69}		
7		P_{72}				P_{76}					
8				P_{84}		P_{86}					
9	P_{91}					P_{96}					
10					$P_{10,5}$						$P_{10,11}$
11			$P_{11,3}$							$P_{11,10}$	

Source: © Deliverable 1.2,ONBASS 2006, FP6

PASS in the medium: dependency matrices



Flight data dependency matrix



Flight mode dependency matrix

aircraft devices, structural elements, Dependency matrix

	1	2	3	4	5	6	7	8	9	10	11
1	P_{11}	P_{12}				P_{16}			P_{19}		
2	P_{21}		P_{23}		P_{25}		P_{27}				
3		P_{32}									$P_{3,11}$
4					P_{45}			P_{48}			
5		P_{52}		P_{54}						$P_{5,10}$	
6	P_{61}						P_{67}	P_{68}	P_{69}		
7		P_{72}				P_{76}					
8				P_{84}		P_{86}					
9	P_{91}					P_{96}					
10					$P_{10,5}$						$P_{10,11}$
11			$P_{11,3}$							$P_{11,10}$	

Source: © Deliverable 1.2, 3.3 ONBASS 2006, FP6

PASS further steps: ABBA

- Principle of active system safety is established and tested using external (RF, BA) expertise
- Complexity of PASS implementation has linear growth (function of number of devices (elements))

NASA and China already fund projects:

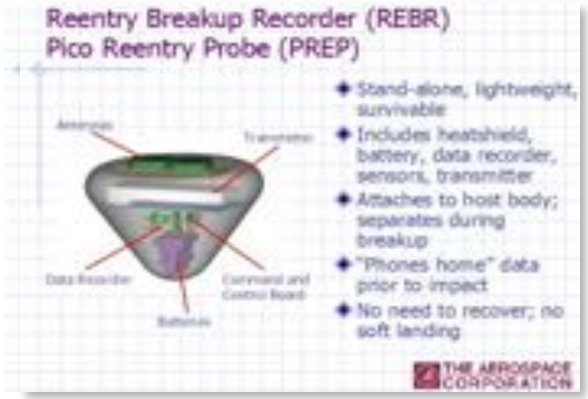
US: New US Program Healthy Aircraft (2002-now)

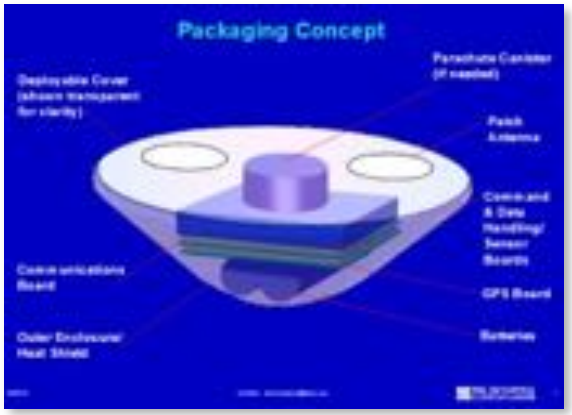
- Participants: NASA, ARINC, NTSB
- Total budget $180Mi + (tbc)
- New Program Safety for Aerospace, NASA, Boeing
- National Transport Safety Board – new program

ABBA - active Black Box for aviation

PASS further steps: ABBA

USA NASA…





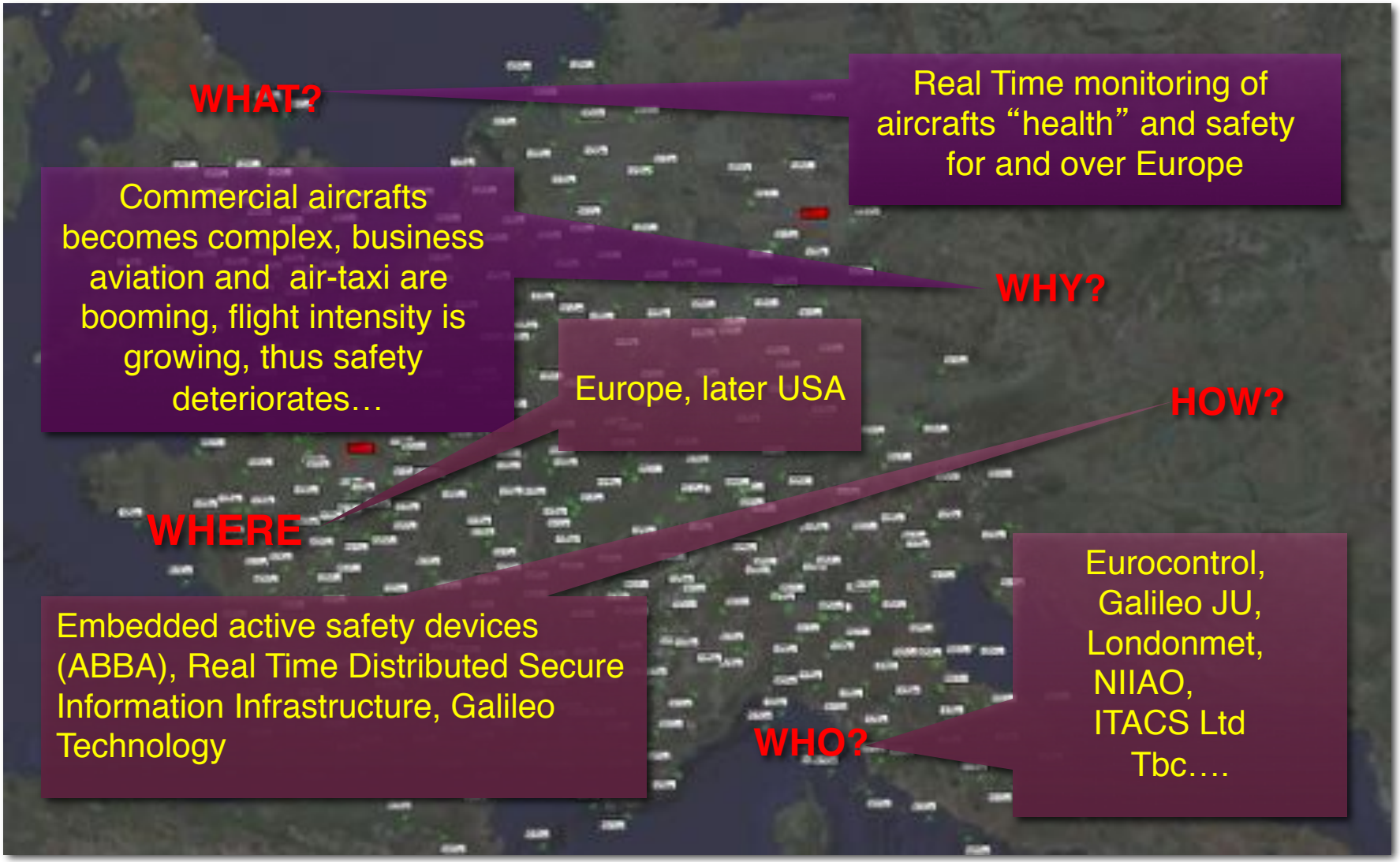
Columbia carried an experimental data recorder fed by more than 700 sensors, measuring parameters all over the craft…

Our response…

PASS in ABBA

- An innovative concept for the conservation of flight data during and after a catastrophic incident
- Involves study of the relationship between crash dynamics, mechanical resilience, shape of packaging, thermal endurance and material science, fault tolerance and reliability
- The basic concepts have already established by ONBASS, NIIAO, ITACS
- The invention is believed to be patentable
- A research proposal has been submitted (May) FP7 relevant call as ONBASS follow-up project.

PASS Further Steps: MESSA



PASS further - MESSA: things to do…

- seek wider partnership such as potential partners here are: Eurocontrol, EASA,EADS/Airbus, ESA, Galileo JU
- developing a new real time interfaces safety bus and channel for connection of and communication with the devices on the aircraft
- design of intuitive representations and data filters to extract relevant information from flight data and distribute it to ATC (Eurocontrol), EASA, flight operators and aircraft users
- design algorithms for flight data processing that will monitor safety in real time of flight (similar to ONBASS) and be transparent for on-ground and on-board application with ability to upgrade/ expand: scalable and dynamically bind.
- *managerial* and *regulatory* aspects need to be analysed to investigate how a proposed system safety level for European aviation can be delivered and administered.
- simulation might be used to envisage the effect of such legislation on the overall safety of flight in Europe, and hence the effectiveness of MESSA and benefits to the EC. Then analysis of decision making efficiency could be justified rigorously.

conclusions:

- ONBASS proved active system safety possibility for GA and CA
- Results have high IPR potential and, if implemented, will restore EU leadership in aerospace safety domain
- Further projects are: Active Black Box for Aviation (ABBA) and Monitor of European System Safety for Aviation (MESSA)
- Widening of cooperation/collaboration between research EU and RF leading centres, regulatory bodies (Eurocontrol, EASA,EADS/Airbus, ESA, Galileo JU, tbc.) is required
- Active safety for aviation might be used by all: flight operators, regulators and aircraft users
- Coordination of this research is required at EC level

contact: info@it-acs.co.uk