SESAR WPE
LONG TERM AND INNOVATIVE RESEARCH

System Performance under Automation Degradation

(SPAD WP-E project)

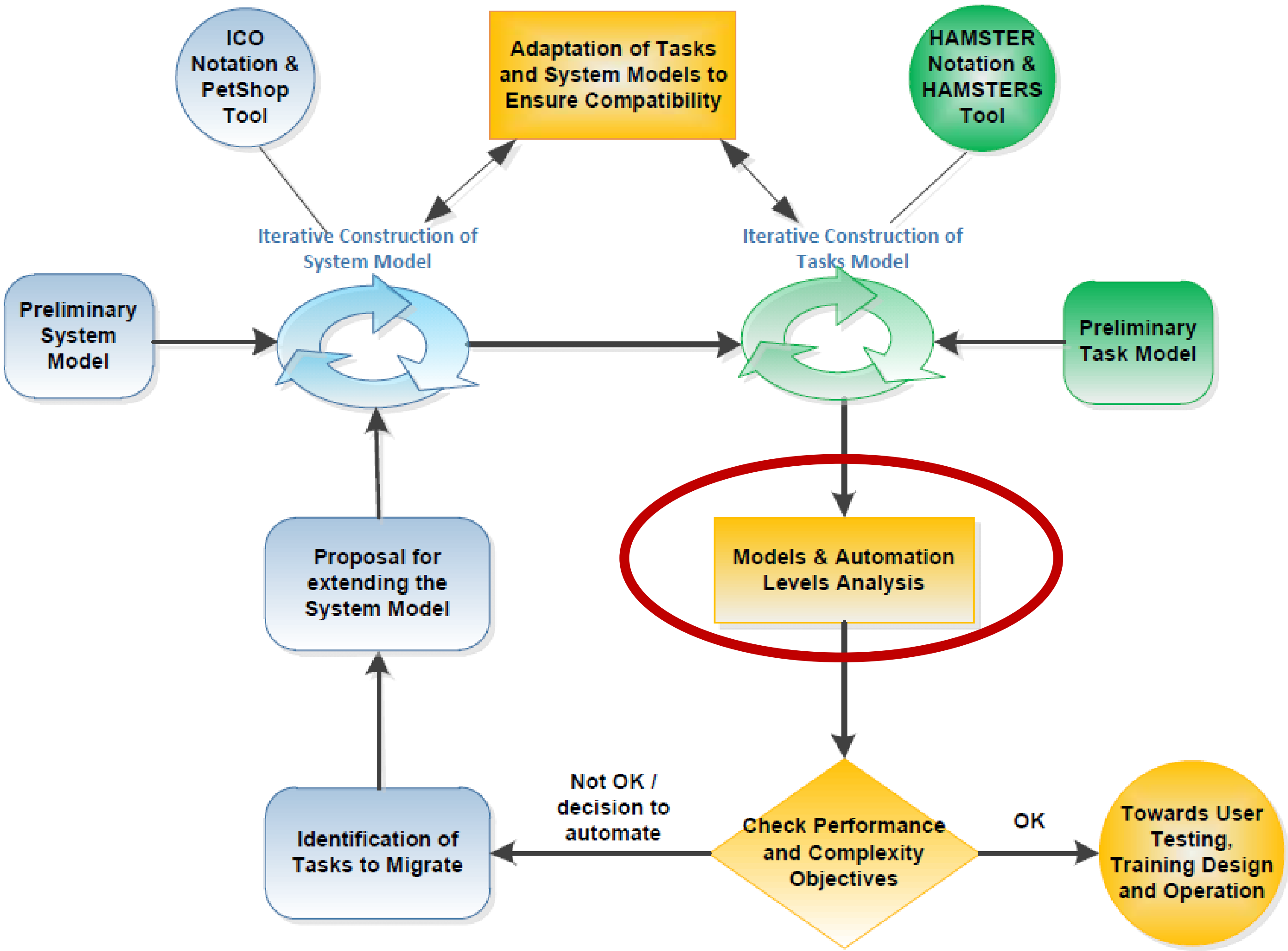
E. Hollnagel, C. Martinie, Philippe Palanque, A. Pasquini, M. Ragosta, E. Rigaud, Sara Silvagni

sara.silvagni@dblue.it - palanque@irit.fr

SESAR WPE
LONG TERM AND INNOVATIVE RESEARCH

DEEPBLUE iCS ARMINES

Iterative Process with Automation

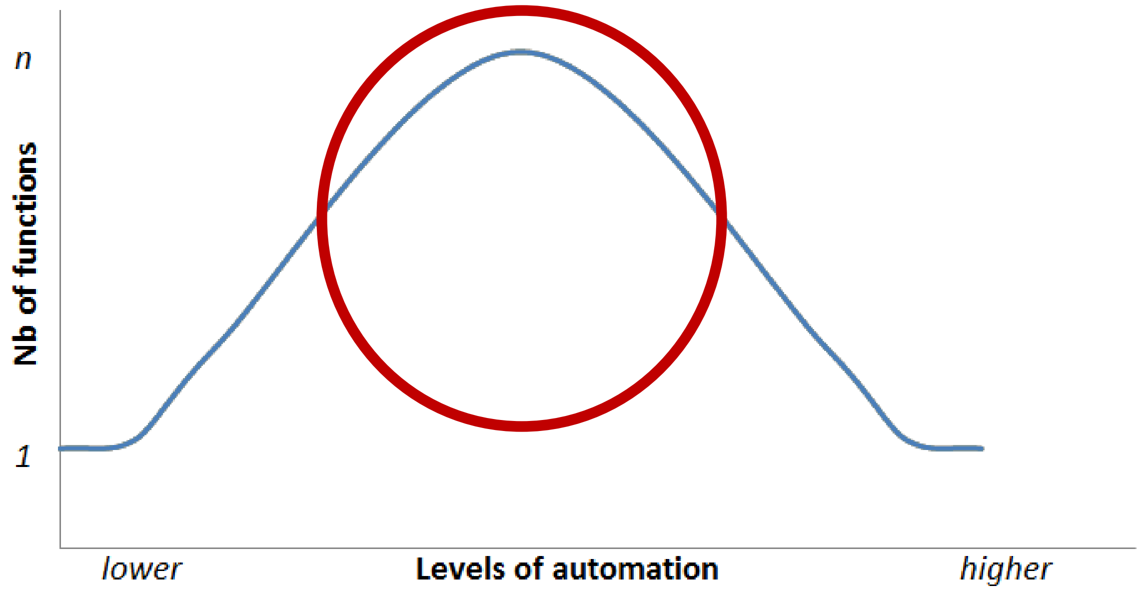


C.Martinie et al. **Formal Tasks and Systems Models as a Tool for Specifying and Assessing Automation Designs.** (ATACCS 2011) Barcelona, Spain, May 2011, ACM DL

Problem

- How to balance automation and interactivity (function allocation)?
- How to precisely and exhaustively describe automation and interaction in Command and Control Systems?
- How to assess design options including automation?

Manual



Autonomous

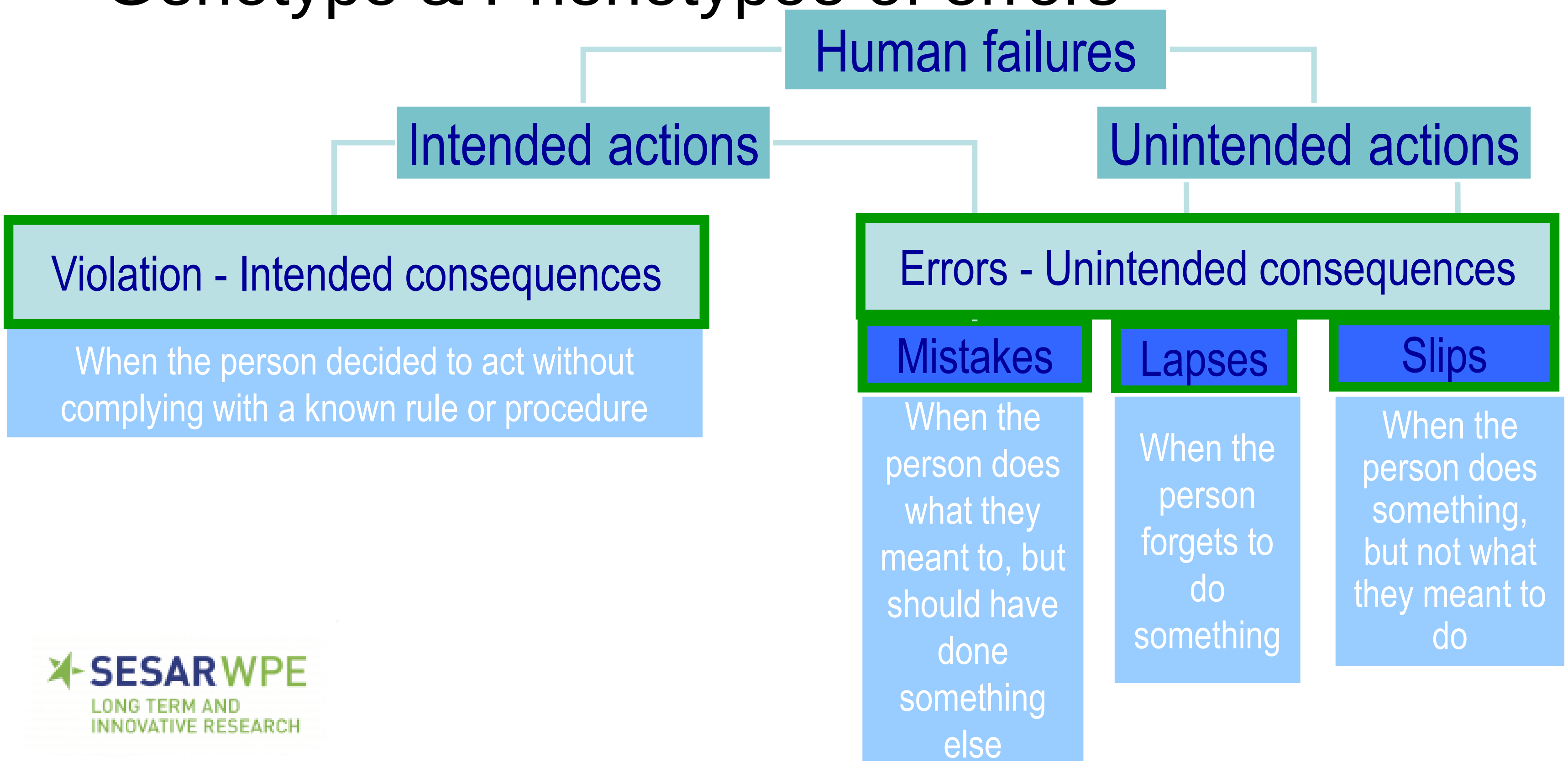
SESAR WPE
LONG TERM AND
INNOVATIVE RESEARCH

Human Do Errors

- Human Error
  - To err is human
  - Slips, lapses and mistakes
  - Genotype & Phenotypoe of errors

James Reason 1990, Human error

Erik Hollnagel 1998 Cognitive Reliability and Error Analysis Method. Elsevier Science, Oxford.



SESARWPE LONG TERM AND INNOVATIVE RESEARCH

Human Do Errors

- Human Error
  - To err is human *(Cicero, I century BC)*
  - "…to understand the reasons why humans err is science" (Hollnagel, 1993)
- Mitigate human error
  - Notice (detection)
  - Reduce number of occurrence (prevention)
    - Designing adequate training
    - Designing interfaces for affordance
    - Designing usable system
  - Reduce the impact of an error (protection)
    - Include barriers in the design
    - Duplicate operators – differentiate their training
    - Separate roles/responsibility

Human Do Errors – the proof

One Solution: "Get Rid of the User"

- Automation is an option
- Reduces costs
- Improves System Performance
- Enhances Human Abilities
- The "Cool" Factor
- Reduces Human Error (by definition)

Automation Levels

Sheridan, T. B., & Verplank, W. (1978)

HIGH	10. The computer decides everything, acts autonomously, ignoring the human.
	9. informs the human only if it, the computer, decides to
	8. informs the human only if asked, or
	7. executes automatically, then necessarily informs the human, and
	6. allows the human a restricted time to veto before automatic execution, or
	5. executes that suggestion if the human approves, or
	4. suggests one alternative
	3. narrows the selection down to a few, or
	2. The computer offers a complete set of decision/action alternatives, or
LOW	1. The computer offers no assistance: human must take all decisions and actions.

System Dependability

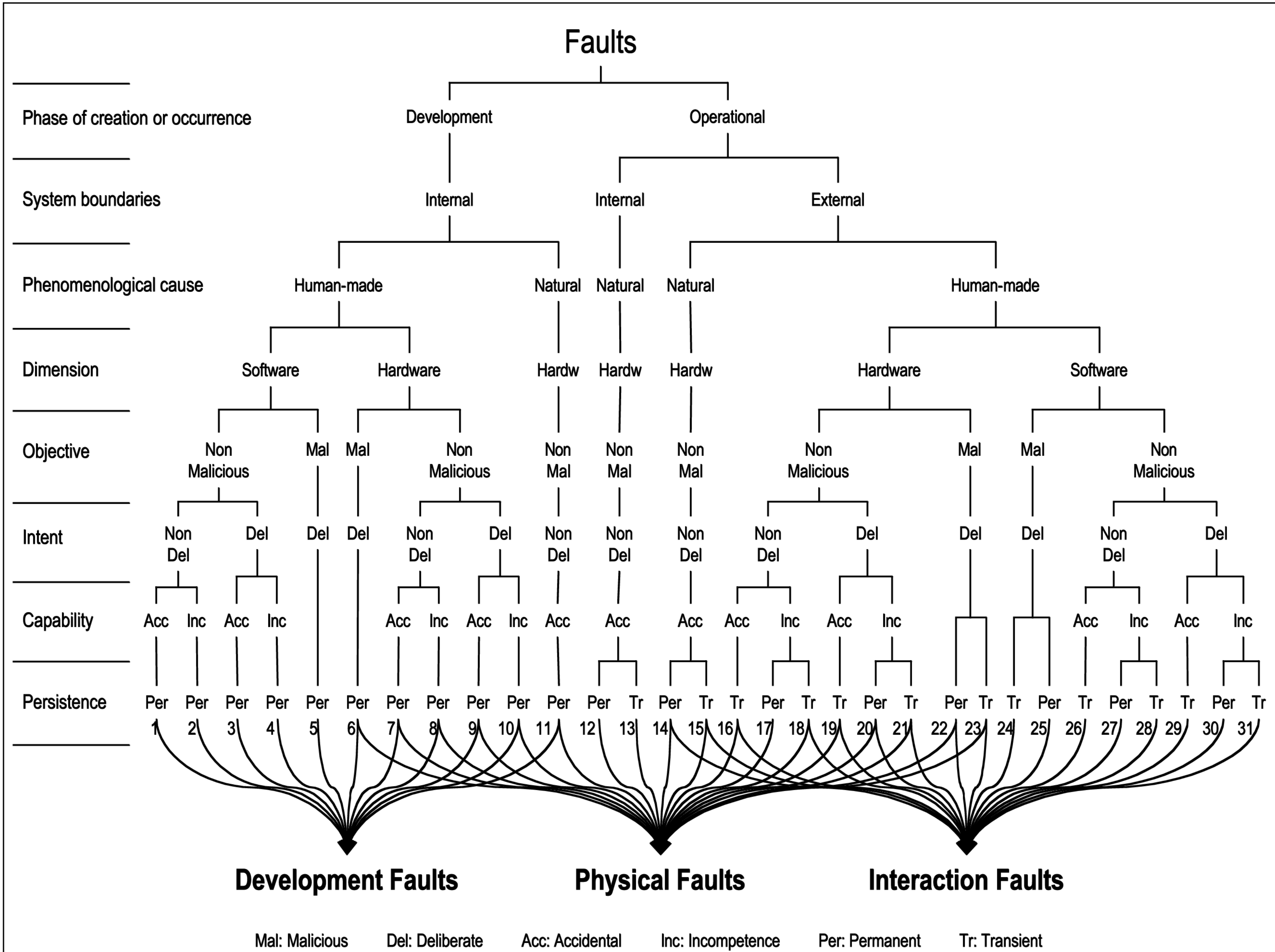
- "The dependability of a system is the ability to avoid service failures that are more frequent and more severe than is acceptable" Avizienis A., Laprie J-C., Randell B., Landwehr C: Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE (2004)

- Failure Condition Severity and Probabillity Objectives

Failure Condition Severity	**Probability Objective**	**Probability descriptive**
Catastrophic	$<10^{-9}$ + **Fail-Safe**	Extremely Improbable
Hazardous	$<10^{-7}$	(very) Improbable
Major	$<10^{-5}$	Improbable
Minor	$<10^{-3}$	Reasonably probable

SESAR WPE
LONG TERM AND INNOVATIVE RESEARCH

Redundancy is required to provide fail-safe design protection from catastrophic failure conditions (ARP 4761)

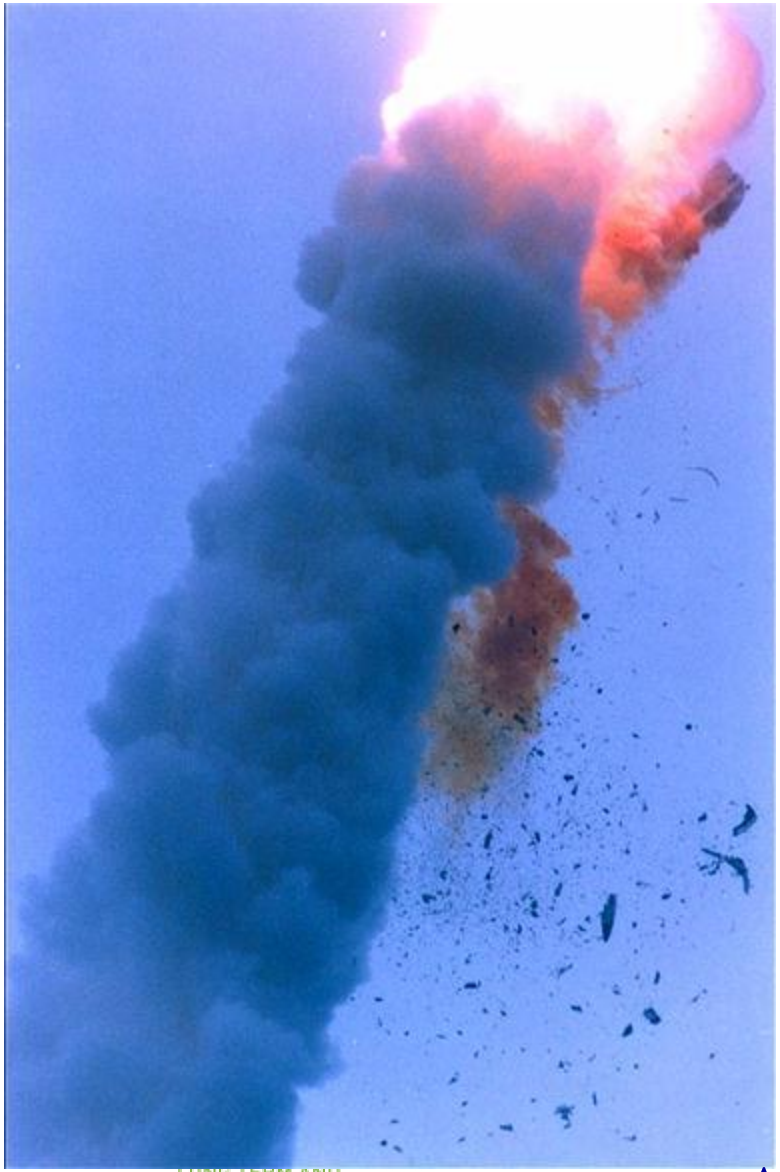


Faults
Phase of creation or occurrence
System boundaries
Phenomenological cause
Dimension
Objective
Intent
Capability
Persistence
Development
Operational
Internal
Internal
External
Human-made
Natural
Natural
Natural
Human-made
Software
Hardware
Hardw
Hardw
Hardw
Hardware
Software
Non Malicious
Mal
Mal
Non Malicious
Non Mal
Non Mal
Non Mal
Non Malicious
Mal
Mal
Non Malicious
Non Del
Del
Del
Del
Non Del
Del
Non Del
Non Del
Non Del
Non Del
Del
Del
Del
Non Del
Del
Acc
Inc
Acc
Inc
Acc
Inc
Acc
Inc
Acc
Acc
Acc
Acc
Inc
Acc
Inc
Acc
Inc
Acc
Inc
Per
Per
Per
Per
Per
Per
Per
Per
Per
Per
Per
Per
Tr
Per
Tr
Tr
Per
Tr
Tr
Per
Tr
Per
Tr
Tr
Per
Tr
Per
Tr
Tr
Per
Tr
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
Development Faults
Physical Faults
Interaction Faults
Mal: Malicious
Del: Deliberate
Acc: Accidental
Inc: Incompetence
Per: Permanent
Tr: Transient

System Dependability

- Fault removal or mitigation
- Fault forecasting
- Fault tolerance (core principles)
  - **Redundancy**: hardware components are physically duplicated
  - **Diversity**: different Software/Hardware implementation
  - **Segregation**: isolation and separation of redundant elements in the system architecture

Systems make mistakes, lapses …



LONG TERM AND
INNOVATIVE RESEARCH

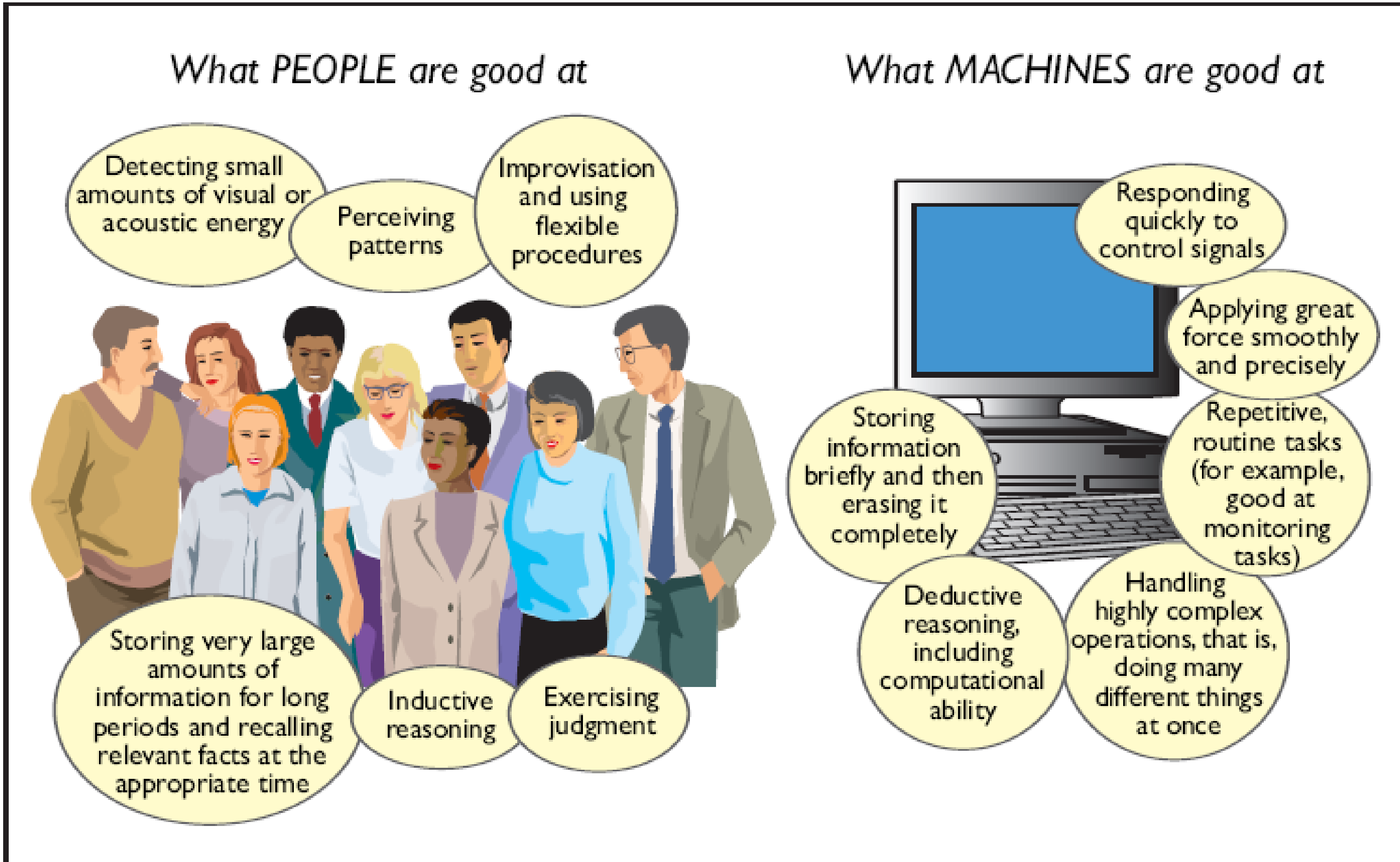
Ariane V501

iPhone v4


:03
October 19
r Needed
t make or receive
calls.
e.com/support
de to unlock

Furthermore …

Carver Turoff March 2007/Vol. 50, No. 3 comm. of the acm (from Fitts 51)



So… there is a int. system to build

- Fully Automated Systems are not an option
- Partly-automated Systems can be foreseen
- Design issues
  - How operators can foresee what the automation will do ?
  - How to avoid mode confusions?
  - How to interfere with automation behaviour?
  - How to modify autonomous behaviour?
  - …
  - Uberligen accident (TCAS versus ATC)
  - A320 and B737 autopilots behaviour

Interaction Dependability

- Hardware/software integration at the core
  - Input devices
  - Output devices
- Interaction techniques dependability
  - Connection to input/output devices (drivers)
  - Performance
  - Resilience
- Interactive Systems dependability

Dependability of the entire Int. Syst. is the one of its weakest point

SESAR WPE
LONG TERM AND INNOVATIVE RESEARCH

Interaction Error Prone Designs


COMMON SENSE
Just because you can, doesn't mean you should.

Problem Statement

- **How to forecast the impact of Automation Degradation on System Performance**
- **How to balance automation and interactivity (function allocation)?**
- **How to precisely and exhaustively describe automation and interaction in CCS?**
- **How to assess design options including automation?**

SESAR WPE
LONG TERM AND INNOVATIVE RESEARCH

Philosophy of SPAD

- Use models as a way of supporting
  - Representation of Systems
  - Representation of Actors
  - Representation …
- Deal with adequate level of abstraction
- Provide a way to analyze Systems' evolutions
- Focusing on relevant information (and to abstract away from the other ones)

Towards a federation of models

- One type of model is not enough
  - Different types of information
  - Different level of details
  - Different kinds of components (human, software and interaction)
- Performance evaluation is a target
  - Quantitative aspects
  - Time, throughput, … (KPI)
  - Propagation - resonance
- Behavioral analysis
  - Qualitative aspects
  - Properties of each model and over modelS

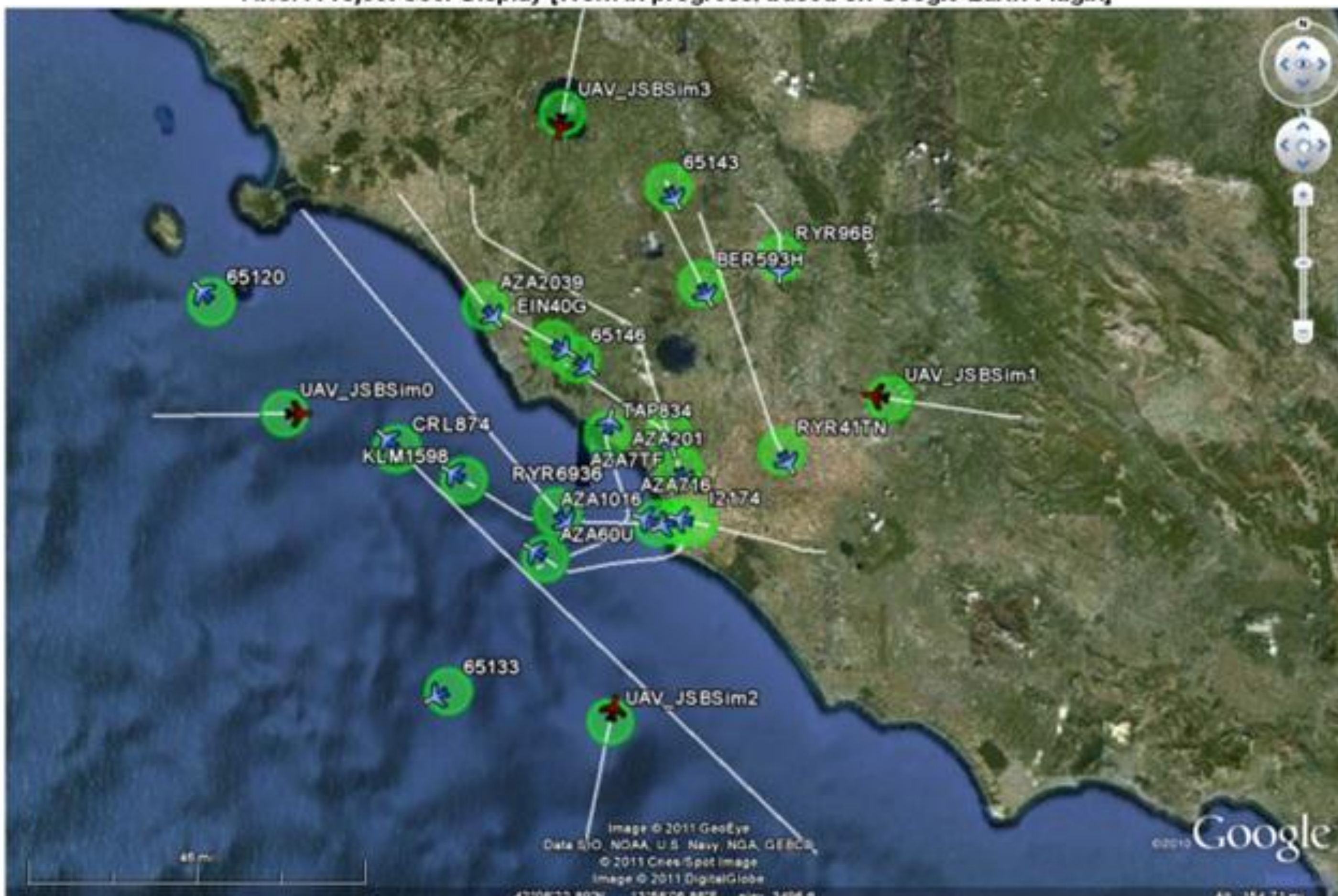
CASE STUDIES - basic ideas

- Two different case studies
  - UAV (see SPAD deliverable under review)
  - AMAN
- Define a general context
  - Infrastructure (mainly hardware)
  - Agents / operators
  - Software / system agents
- Define scenarios
  - Nominal scenario (as a baseline)
  - 3 degradation scenarios (confined, average, extended)

Unmanned Aerial Vehicles

System for automated self-separation

ARCA Project User Display [Work in progress, based on Google Earth Plugin]



SESAR WPE
LONG TERM AND
INNOVATIVE RESEARCH

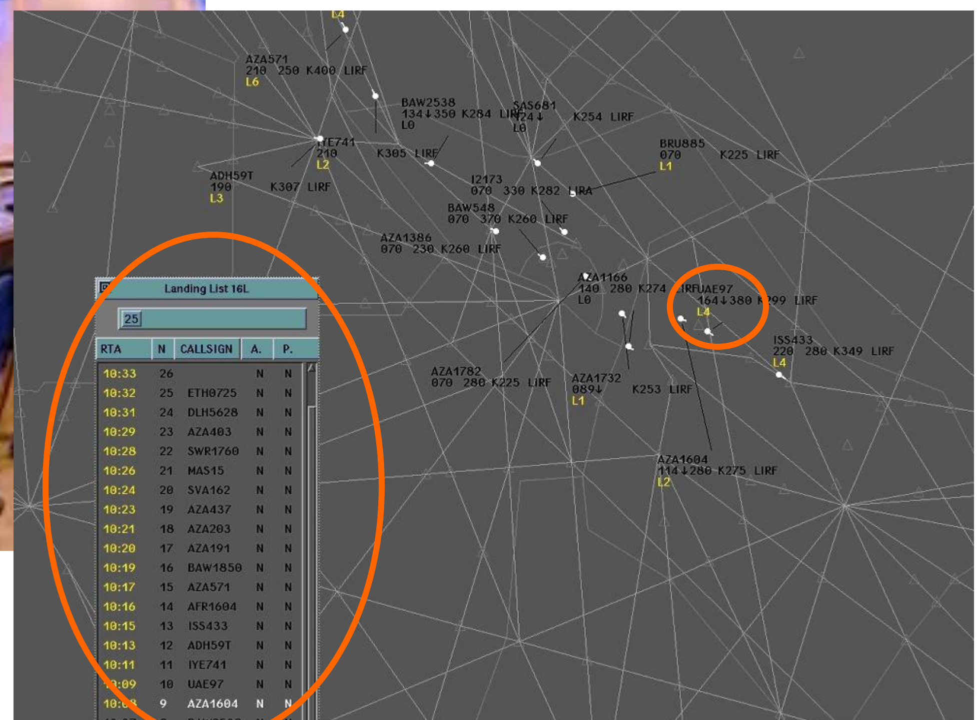
CASE STUDIES – UAV

High in the Sheridan's automation levels

- Level 7-8
- "Execute automatically then necessarily inform the human"
- "Informs the human only if asked"

Arrival Manager

Optimal arrival sequence times



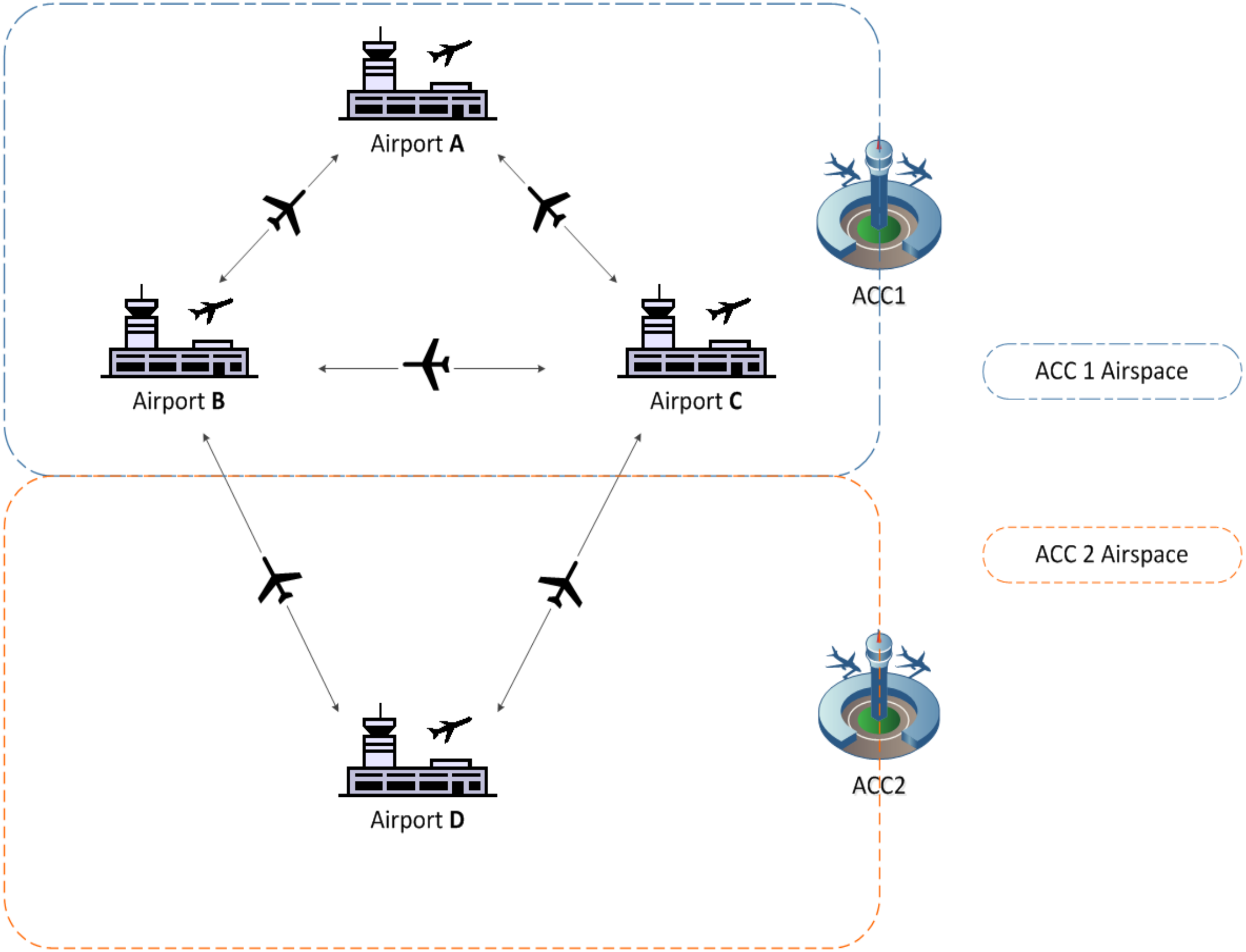
SESAR WPE
LONG TERM AND INNOVATIVE RESEARCH

CASE STUDIES – AMAN

Rather low in the Sheridan's automation levels

- **Level 3-4**
- **"Narrows the selection down to a few"**
- **"Suggests one alternative"**

AMAN - Infrastructure

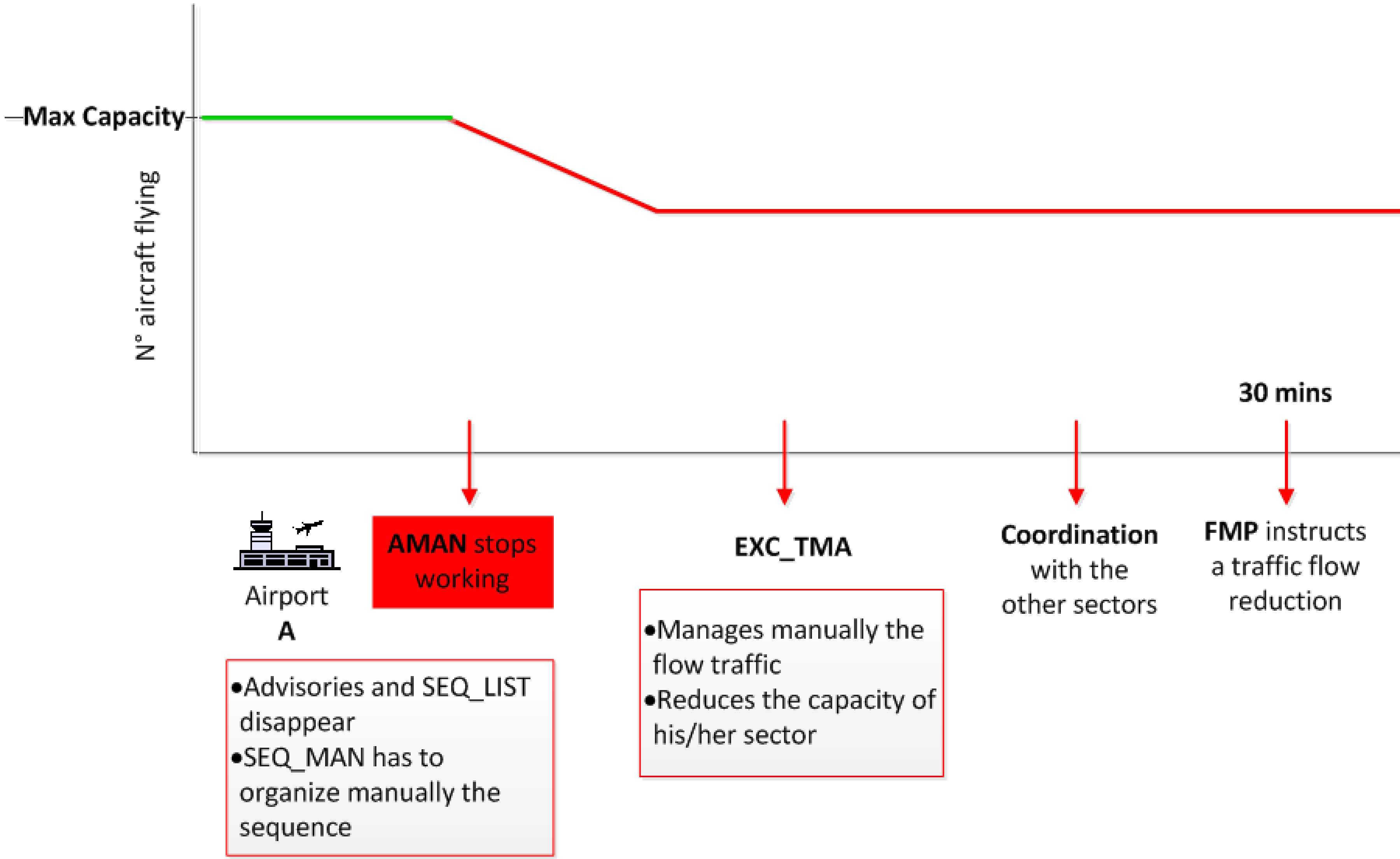


Arrival Manager - Scenarios

- Nominal Scenario
- AMAN temporary failure
- AMAN permanent failure
- AMAN providing misleading information

SESAR WPE
LONG TERM AND INNOVATIVE RESEARCH

Temporary failure

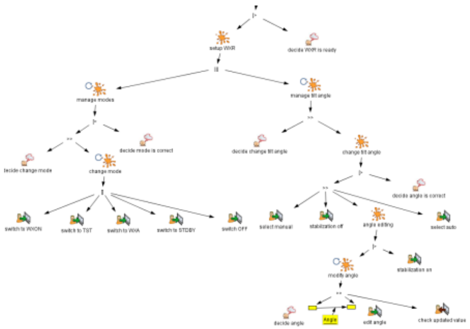


Next Steps

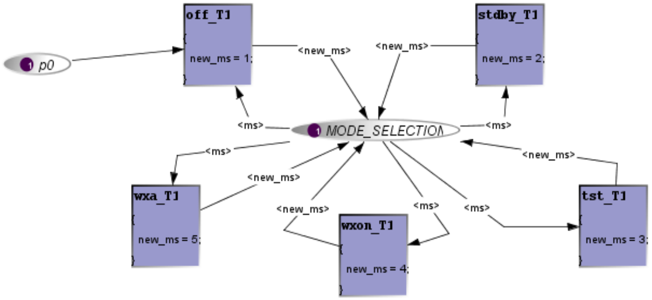
- Federation of Models
  - Identify candidates
  - Assess them individually
  - Assess their complementarity
- Degradation Lifecycle Analysis
  - Start of degradation
  - Work under degradation
  - End of degradation

Studied Notations and Tools

- **Task models: HAMSTER(S)**



- **Interactive system models: ICO (PetShop)**

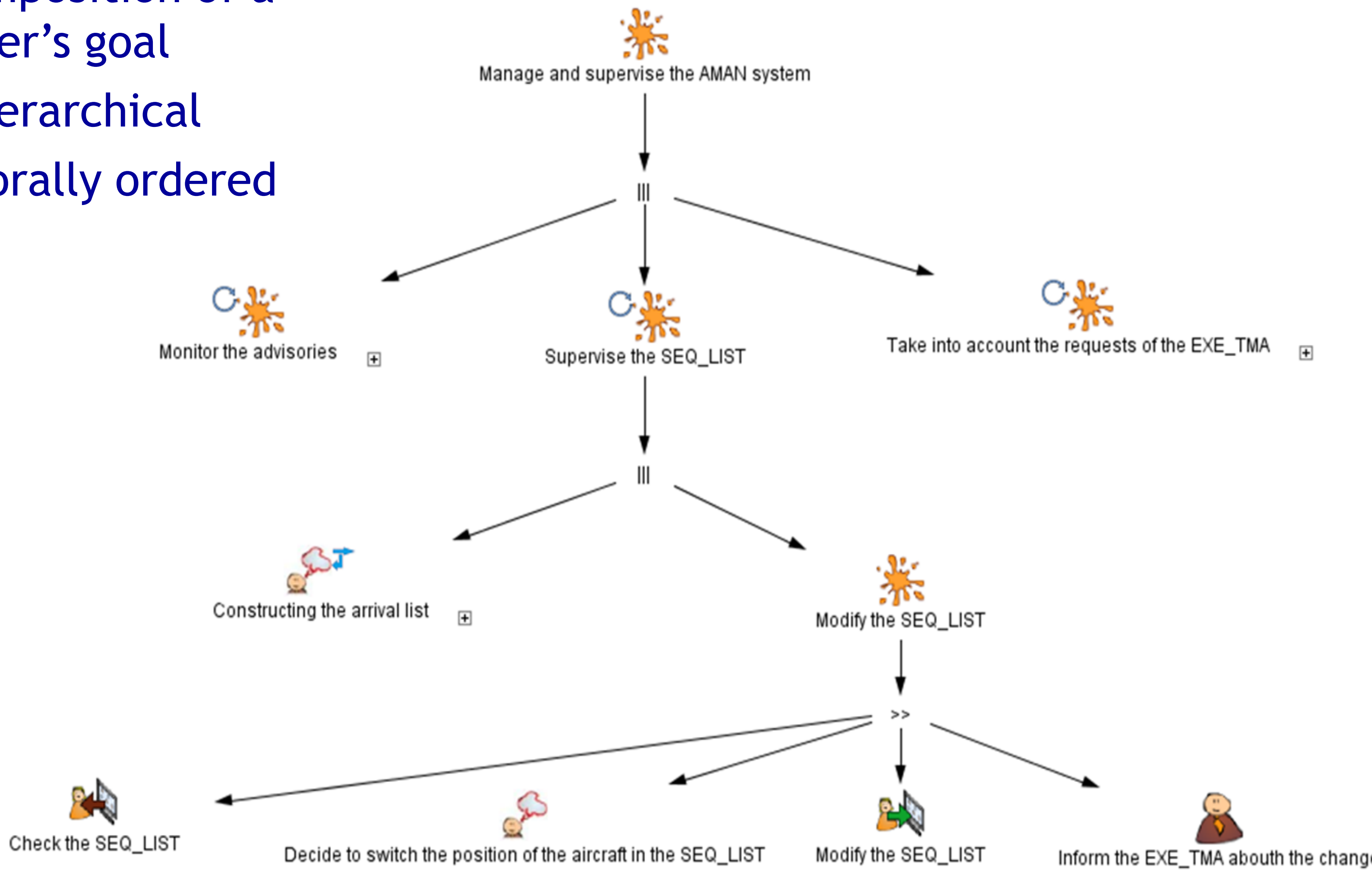


Two complementary views of the interaction between the user and the system

SESAR WPE LONG TERM AND INNOVATIVE RESEARCH

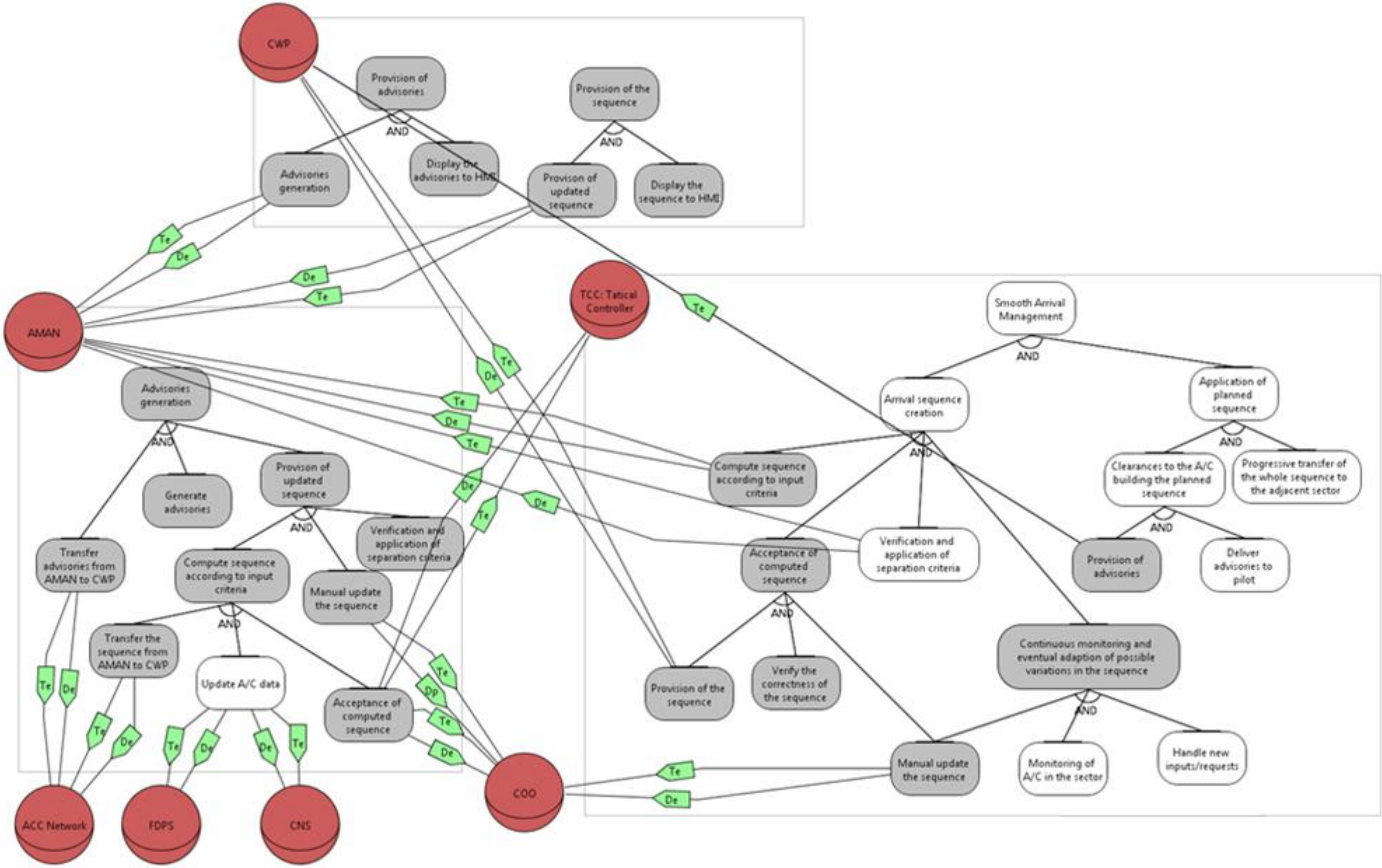
Task models: HAMSTER(S)

- Decomposition of a user's goal
- Hierarchical
- Temporally ordered

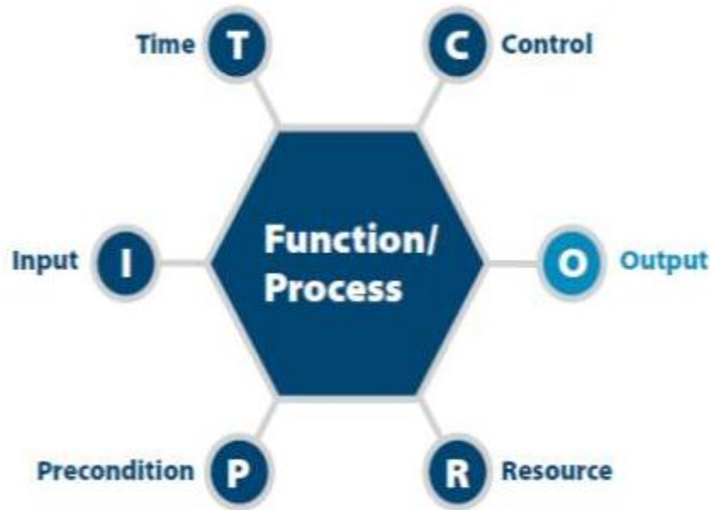


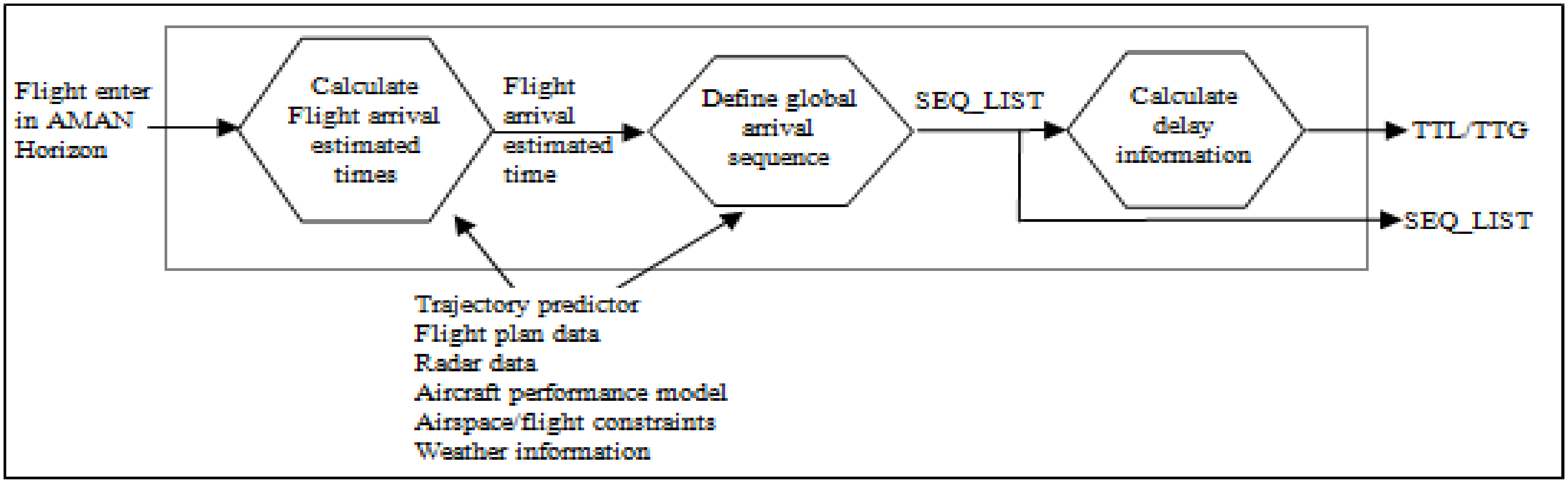
SESAR WPE
LONG TERM AND INNOVATIVE RESEARCH

Other Models - Tropos



Other Models - FRAM

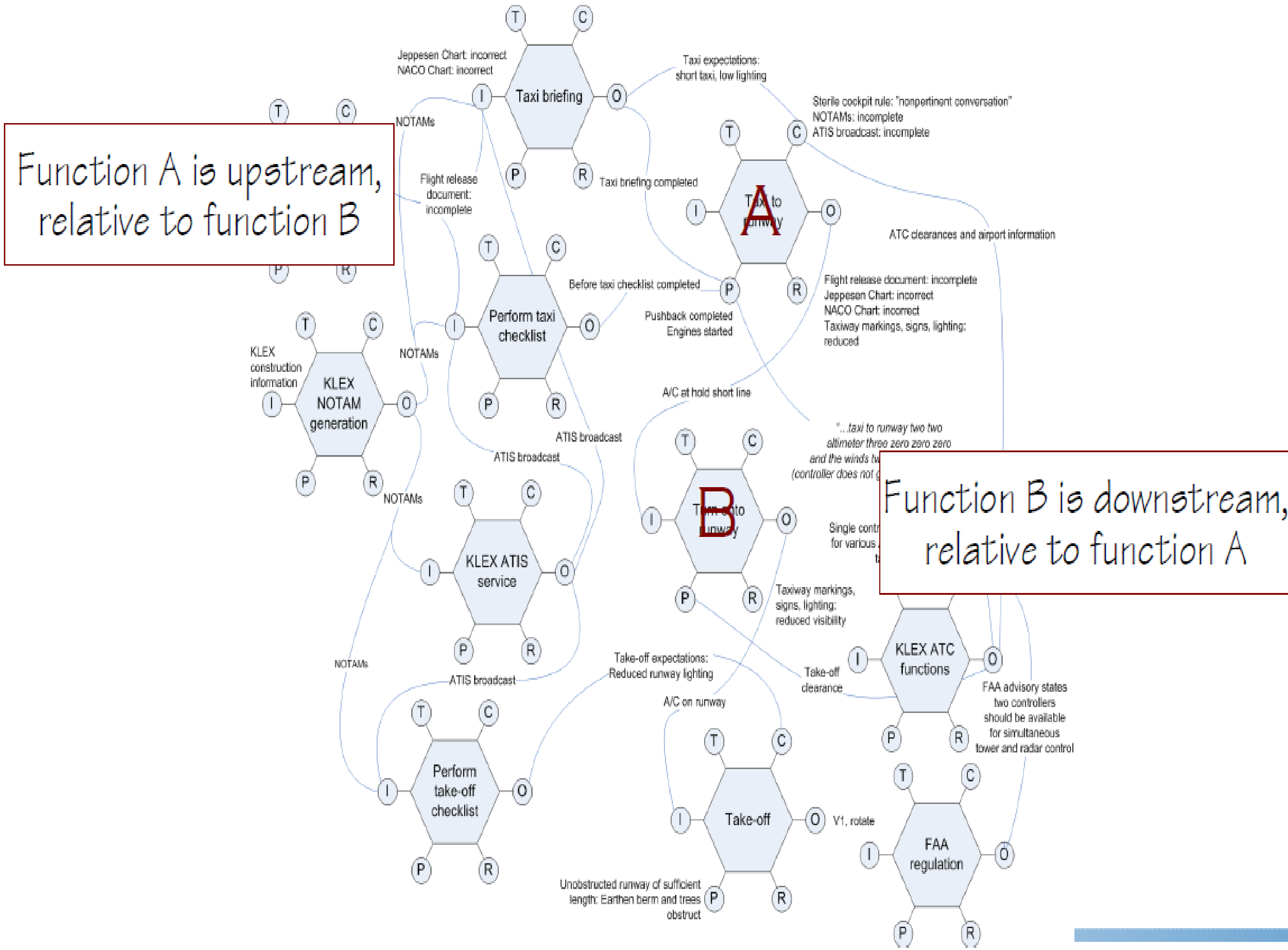




SESAR WPE
LONG TERM AND INNOVATIVE RESEARCH

Function A is upstream, relative to function B

Function B is downstream, relative to function A



Conclusions

- **Use models as a way of supporting**
  - **Representation of Systems**
  - **Representation of Actors**
  - **Representation of Interactions**
- **Providing a way to analyze System evolutions**
- **Providing ways of assessing impact of degradations**
- **Finding ways of mitigating their impact on performance**

System
Performances under
Automation
Degradation

THANKS FOR YOUR ATTENTION

http://www.irit.fr/recherches/ICS/projects/spad

SESAR WPE
LONG TERM AND
INNOVATIVE RESEARCH

DEEPBLUE

iCS

ARMINES

1st International Conference on

Application and Theory Automation in Co[…] and Control Sy[…]

Related work- quick overview

- Parasuraman, R.; Sheridan, T.B.; Wickens, C.D.; "A model for types and levels of human interaction with automation" Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Trans. on, vol.30, no.3, pp.286-297, May 2000.
- Proud, R. W., Hart, J. J., & Mrozinski, R. B. (2003). "Methods for Determining the Level of Autonomy to Design into a Human Spaceflight Vehicle: A Function Specific Approach," Proc. Performance Metrics for Intelligent Systems (PerMIS '03), September 2003.
- Cummings M.L., Bruni S., Collaborative Human-Automation Decision Making, Springer Handbook of Automation, pp. 437-447, 2009.
- Johansson B., Fasth A., Stahre J., Heilala J., Leong S., Tina Lee Y., Riddick F., Enabling Flexible Manufacturing Systems by using level of automation as design parameter, Proc. of the 2009 Winter Simulation Conference, 13-16 dec 2009

Types and levels

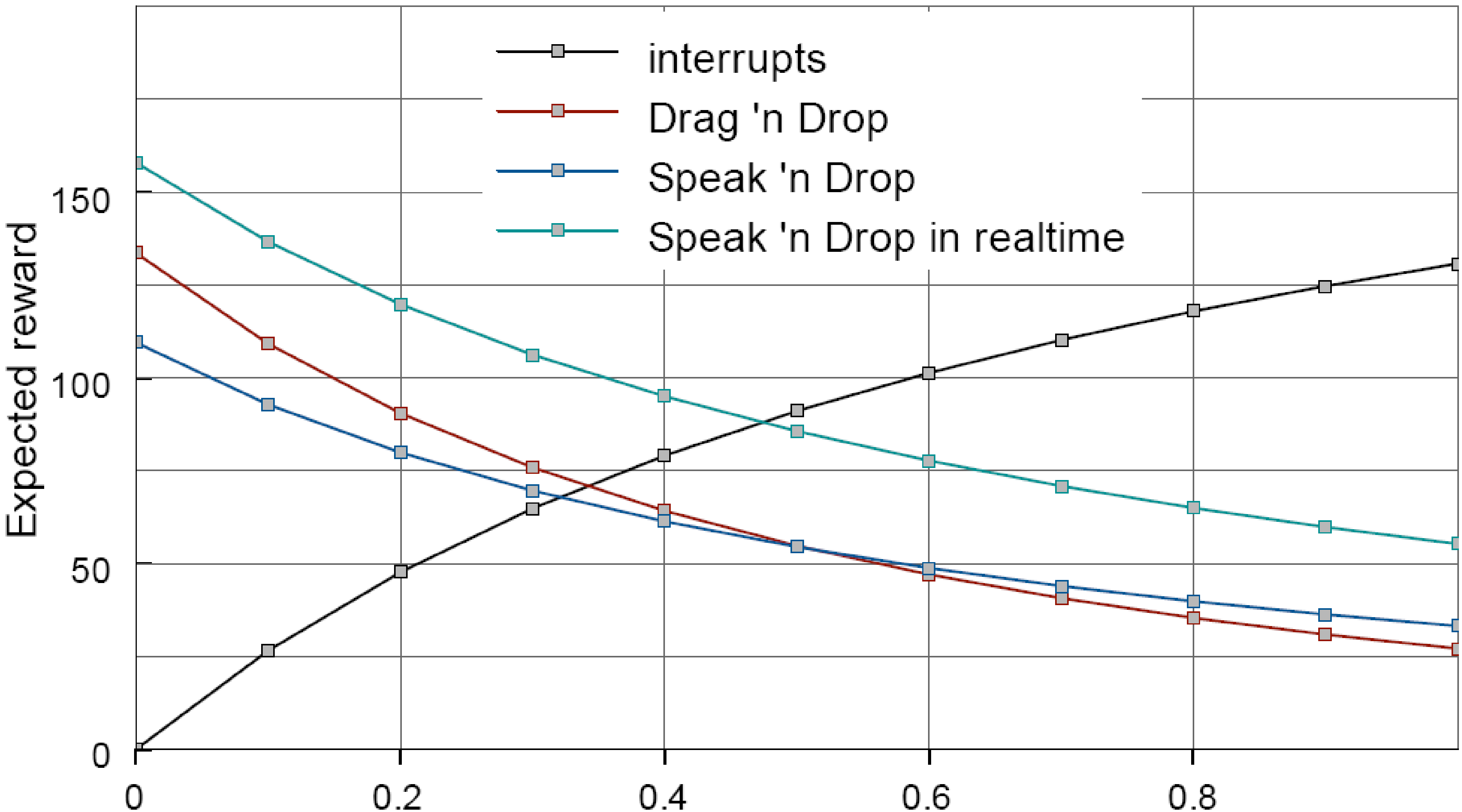
Analytic assessment scale and tool

Decision making step

Simulation tool

SESAR WPE
LONG TERM AND INNOVATIVE RESEARCH

Issue of context



LONG TERM AND
INNOVATIVE RESEARCH

The road to hell is paved with good intentions

Regina Bernhaupt, Guy A. Boy, Michael Feary, Philippe A. Palanque: Engineering automation in interactive critical systems. CHI Extended Abstracts 2011: 69-72

SESAR WPE
LONG TERM AND INNOVATIVE RESEARCH