Ground System Architectures Workshop
GSAW
2009

An operator-centered, model-based framework for ground segment design, supporting training and operations

Sandra STEERE[†], Erwann POUPART[†] & Philippe PALANQUE[††]

† Ground Segment Systems Office (DCT/PS/SGE), CNES, Toulouse, France
sandra.steere@cnes.fr, erwann.poupart@cnes.fr

†† Interacting Humans with Computing Systems IRIT, University Paul Sabatier, Toulouse, France
palanque@irit.fr   http://ihcs.irit.fr/palanque/

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

R&T project called TORTUGA (2008 – 2011)

- R&T TORTUGA "Tasks, Operations, Reliability & Training for Users of Ground Applications"

- Collaboration with IRIT, University Toulouse III
  - Head of project IRIT: Philippe PALANQUE (team IHCS a l'IRIT)
  - Head of project CNES: Erwann POUPART (DCT/PS/SGE)

- Participation with the "DCT/OP" (operations) service at CNES
  - Mission correspondent DCT/OP: Eliane CUBERO-CASTAN

- Objectives: improve the operability (reliability, usability, evolvability, error-tolerance) of command/control applications by using model-based approaches and user centred design (UCD)
  - Impacted design processes: UI design, operational procedure design, design of operator tasks, design of training materials

- Adaptation of methods and technologies already proven in other domains (aeronautics, nuclear etc) to the space domain

- Technologies and methodologies used in academia (ex ICO, CTT)

http://ihcs.irit.fr/tortuga

Introduction

- **Long term target**
  - **Study to improve current development practice at CNES**
  - **Improve reliability, training and operations while reducing costs**

- **Two connected problems**
  - **Consideration of operators too little and too late within the development process**
    - Impact of limited involvement has been considered harmful for many years in the field of HCI [Lim & Long, 1994]. Still requires attention in the field of ground segment development
  - **Design and implementation of procedures and material for ground segment operator training**
    - The focus in the space domain is mainly on improving the design of the satellite itself and not operations [Eickhoff J et al, 2007]

- **Aim**
  - **Apply an operator-centred model-based approach for the design of interactive ground segment applications**

Presentation outline

- Case study
  - Automated Transfer Vehicle
- Current practice at CNES (w.r.t to case study)
  - System design practice
  - Training practice
- Proposals / line of research for changing practice
  - TORTUGA framework

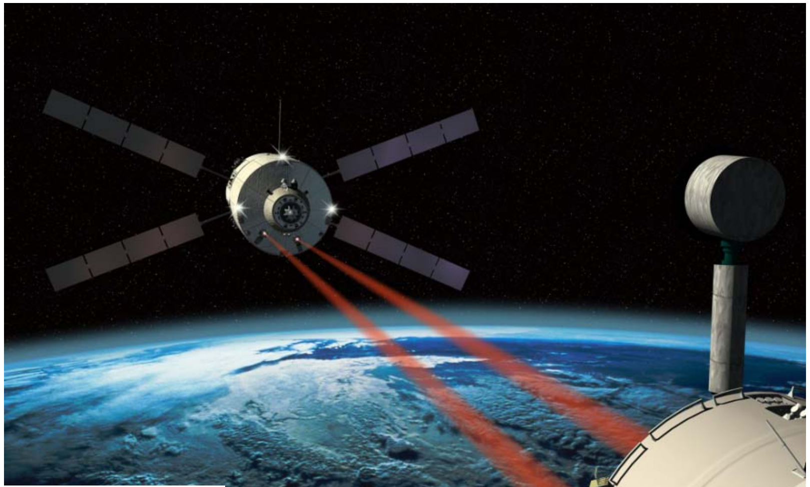
cnes

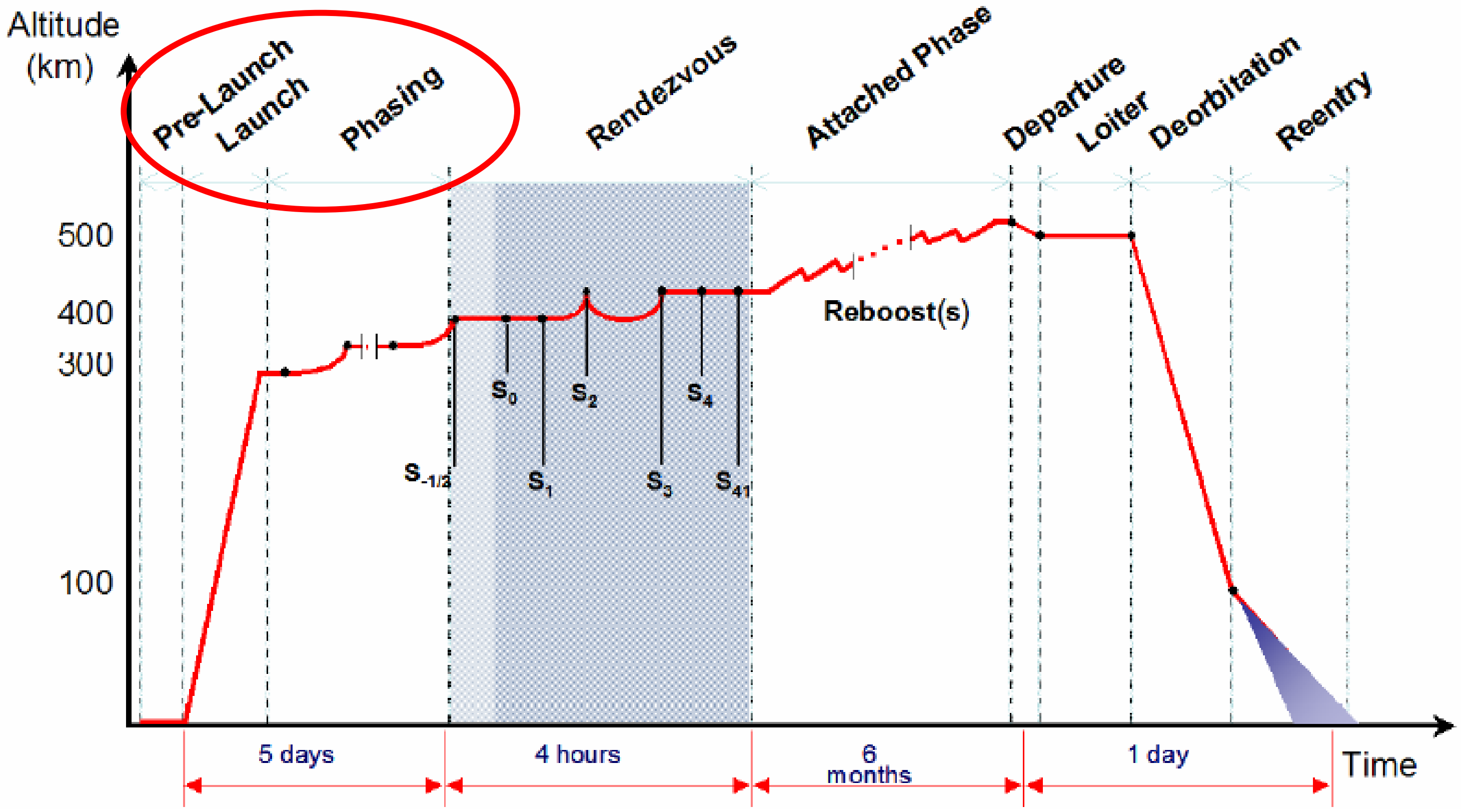
CENTRE NATIONAL D'ÉTUDES SPATIALES

Case study (1/3)

The CNES ESA ATV-1 (and soon ATV-2) project

- European contribution to the ISS
- Automated space vehicle
- Docking to the Russian part of ISS

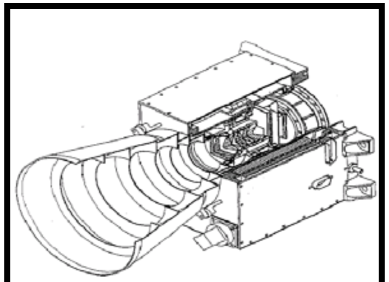




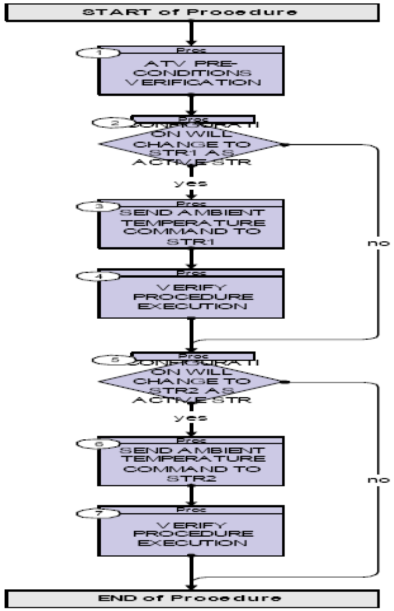
- Dry and wet cargo delivery and disposal
- Support ISS on-orbit control through its re-boost capability
- Destructive re-entry

Case study (2/3)

- In this study, we focus on sub-systems

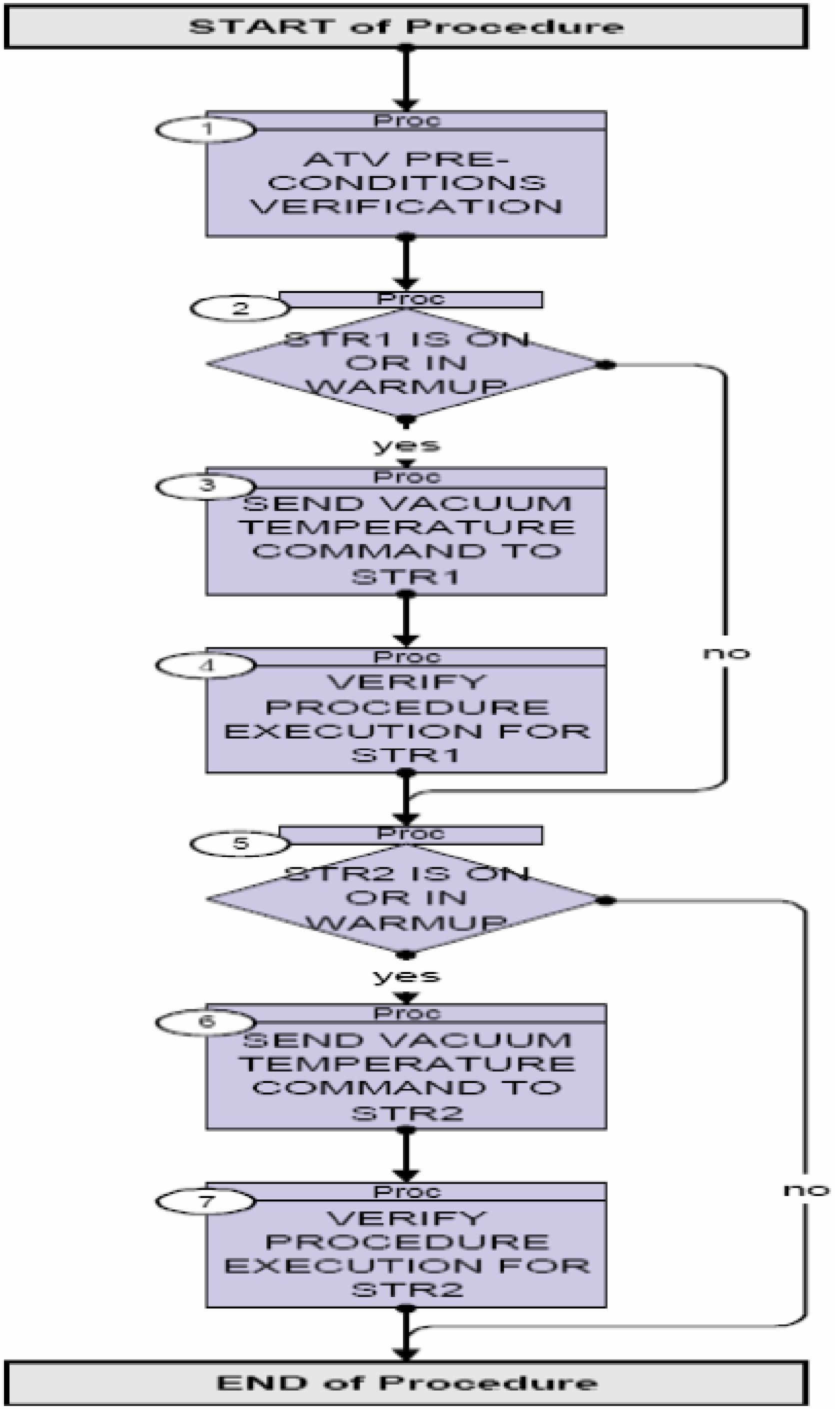


Star tracker of the ATV space vehicle

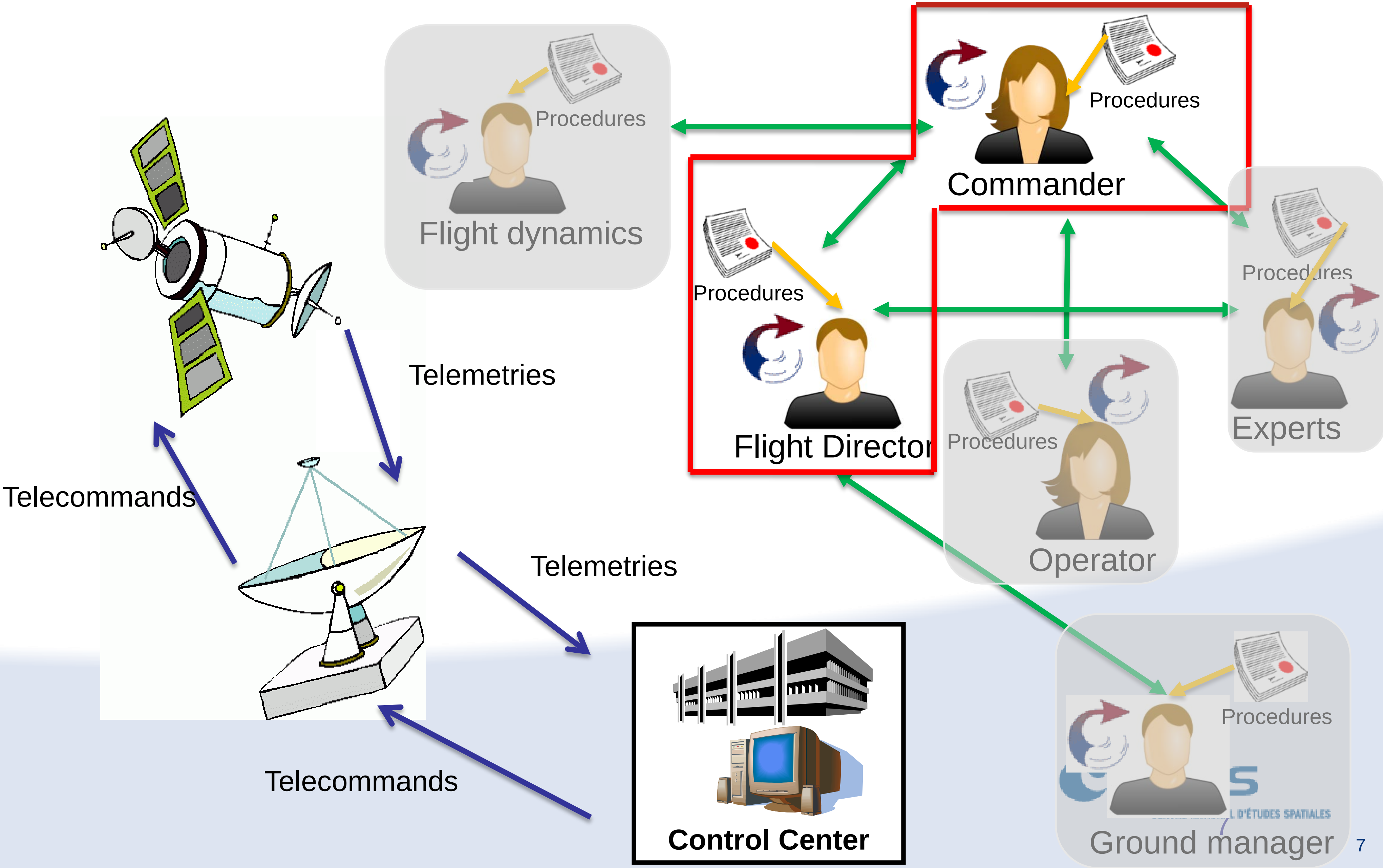

START of Procedure
1
Proc
ATV PRE-CONDITIONS VERIFICATION
2
Proc
CONFIGURATION WILL CHANGE TO STR1 AS ACTIVE STR
yes
no
3
Proc
SEND AMBIENT TEMPERATURE COMMAND TO STR1
4
Proc
VERIFY PROCEDURE EXECUTION
5
Proc
CONFIGURATION WILL CHANGE TO STR2 AS ACTIVE STR
yes
no
6
Proc
SEND AMBIENT TEMPERATURE COMMAND TO STR2
7
Proc
VERIFY PROCEDURE EXECUTION
END of Procedure

A star tracker procedure

Command and c
ground segment


START of Procedure
1
Proc
ATV PRE-CONDITIONS VERIFICATION
2
Proc
STR1 IS ON OR IN WARMUP
yes
no
3
Proc
SEND VACUUM TEMPERATURE COMMAND TO STR1
4
Proc
VERIFY PROCEDURE EXECUTION FOR STR1
5
Proc
STR2 IS ON OR IN WARMUP
yes
no
6
Proc
SEND VACUUM TEMPERATURE COMMAND TO STR2
7
Proc
VERIFY PROCEDURE EXECUTION FOR STR2
END of Procedure

Case study (3/3) : Control room interactions

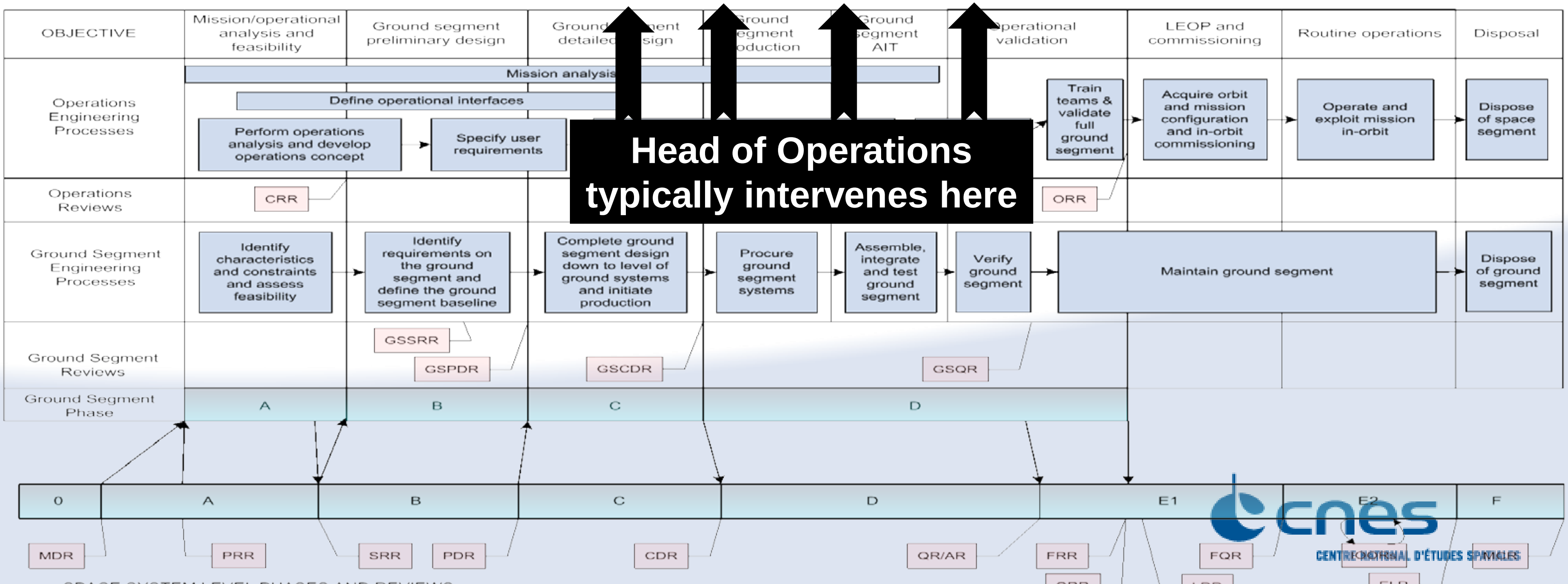


Presentation outline

- Case study
  - Automated Transfer Vehicle
- Current practice at CNES (w.r.t to case study)
  - System design practice
  - Training practice
- Proposals / line of research for changing practice
  - TORTUGA framework

Current system design practice (1/2)

- Development process for operational procedures and ground segment systems at CNES is based on the European Cooperation for Space Standardisation ECSS E-70B


OBJECTIVE
Mission/operational analysis and feasibility
Ground segment preliminary design
Ground ment detailed sign
round egment oduction
Ground segment AIT
perational validation
LEOP and commissioning
Routine operations
Disposal
Operations Engineering Processes
Mission analysis
Define operational interfaces
Perform operations analysis and develop operations concept
Specify user requirements
Train teams & validate full ground segment
Acquire orbit and mission configuration and in-orbit commissioning
Operate and exploit mission in-orbit
Dispose of space segment
Operations Reviews
CRR
ORR
Ground Segment Engineering Processes
Identify characteristics and constraints and assess feasibility
Identify requirements on the ground segment and define the ground segment baseline
Complete ground segment design down to level of ground systems and initiate production
Procure ground segment systems
Assemble, integrate and test ground segment
Verify ground segment
Maintain ground segment
Dispose of ground segment
Ground Segment Reviews
GSSRR
GSPDR
GSCDR
GSQR
Ground Segment Phase
A
B
C
D
0
A
B
C
D
E1
E2
F
MDR
PRR
SRR
PDR
CDR
QR/AR
FRR
ORR
FQR
LRR
ELR

Head of Operations typically intervenes here

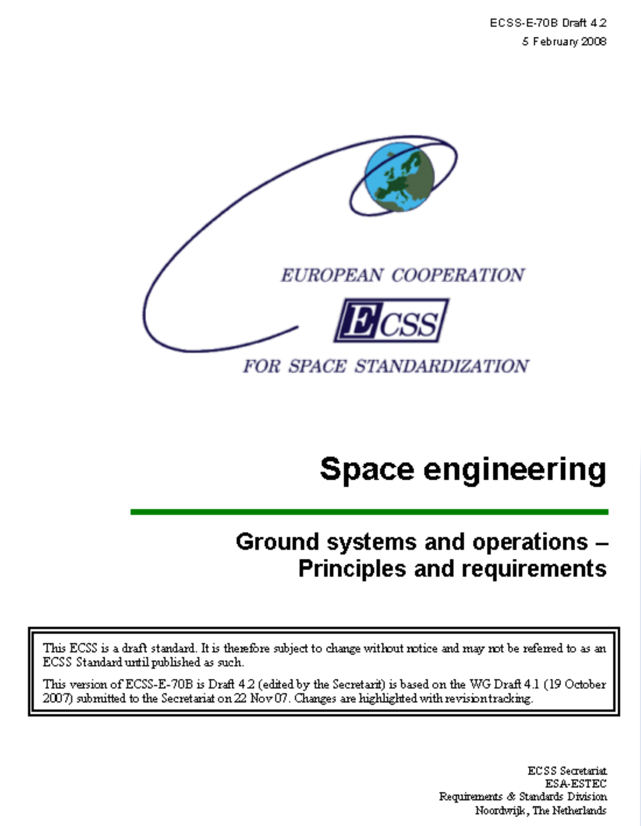
SPACE SYSTEM LEVEL PHASES AND REVIEWS

Current system design practice (2/2)

- A specificity of ground segments with respect to standard interactive systems is that operator teams are neither in place at the start of a project nor in the early phases of development
- Thus necessary to involve future operators to “test” the application during the last step of phase D, Operational Qualification (OQ) after the Ground Segment AIT and Technical Qualification steps
- However, more recently operator intervention during design is increasingly encouraged
- Though it is argued that operational testing should be a period of confirmation and not a period of discovery, in ground segments this is difficult to achieve

Ground segment and operations phases

- ECSS E70-B Draft 4.2
  - No explicit involvement of end users
  - No dedicated activity for User Interface design or development of training material
  - No dedicated activity for User Interface evaluation
  - No dedicated means for integrating knowledge of previously known control room incidents which is the only means to prevent previous incidents/accidents from reoccurring



ECSS-E-70B Draft 4.2
5 February 2008

EUROPEAN COOPERATION
ECSS
FOR SPACE STANDARDIZATION

Space engineering

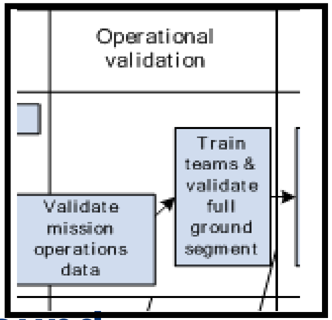
Ground systems and operations –
Principles and requirements

This ECSS is a draft standard. It is therefore subject to change without notice and may not be referred to as an ECSS Standard until published as such.

This version of ECSS-E-70B is Draft 4.2 (edited by the Secretarit) is based on the WG Draft 4.1 (19 October 2007) submitted to the Secretariat on 22 Nov 07. Changes are highlighted with revision tracking.

ECSS Secretariat
ESA-ESTEC
Requirements & Standards Division
Noordwijk, The Netherlands

Current training practice


Operational validation
Validate mission operations data
Train teams & validate full ground segment

- "Operational Validation" objective, "Train teams and validate full ground segment"
- For new applications, industrial partner provides training
- For existing applications, operators rely on shared knowledge between colleagues
  - Diverges from a formal structured planned activity (industrial presentation) to an informal "storytelling"-based activity
  - Information transfer relies more on emotional factors such as near misses and incidents rather than on task-based, routine operations
- Compensates non-systematic way of reporting known incidents
  - but time consuming and provides a limited coverage of the ground segment functionalities and operational procedures
  - storytelling is not a substitute for incident-reporting systems as operators emphasize attention, vigilance, personal responsibility and carefulness as the major means to maintain safe practice, but pay too little attention to the wider context of accident causation

Presentation outline

- Case study
  - Automated Transfer Vehicle
- Current practice at CNES (w.r.t to case study)
  - System design practice
  - Training practice
- **Proposals / line of research for changing practice**
  - **TORTUGA framework**

TORTUGA project approach

- Model-based design (as opposed to current document based design)
- Formal description techniques for modelling & construction of system
  - Support reliability of the system
  - Support usability of the system
  - Can provide help during operations (contextual help)
  - Support specification and construction of training material
  - Support evolvability of the system
  - Support non re-occurrence of incident/accident
- Integration of Human Factors, UCD (User Centred Design) techniques and Incident analysis
  - Tasks/goal descriptions
  - Procedures
- Training materials
  - User manuals
  - User training sessions
  - Verification of SRK acquisition (Skills, Knowledge, Rules)

CENTRE NATIONAL D'ÉTUDES SPATIALES

HCI & formal description techniques

Human Computer Interaction

- HCI concerned with the design, evaluation & implementation of interactive computing systems for human use and with the study of major phenomena surrounding them
- User Centred Design (UCD) (Norman,1986)
- Non-formal HCI methods
  - Storyboarding, Card sorting, Usability evaluations
- Formal HCI methods
  - Task analysis, State diagrams…

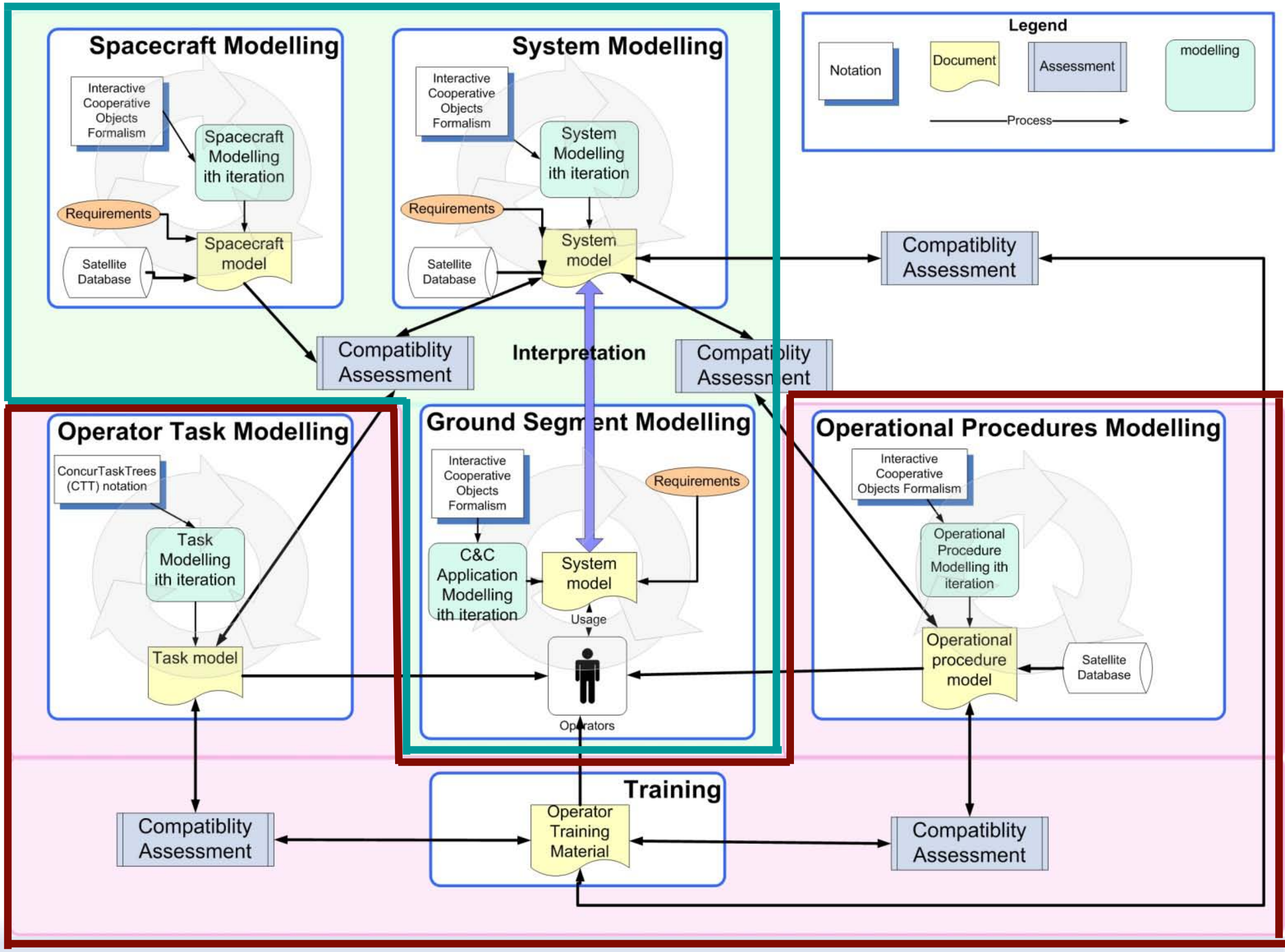
Formal Description Techniques

- Model-based design approach for accentuating potential reliability gaps
- Formal description techniques for the specification and the construction of the system
  - Support reliability of the system
  - Support the usability of the system
    - Can provide help during operations (contextual help)
    - Support specification and construction of training material
  - Support the evolvability
  - Support non re-occurrence of incident/accident
- Formal modelling technique for the description of user behaviour & system makes it possible to compare, analyse and integrate them
- Prove accounting of HCI requirements e.g
  - ATV commands (REQ325) The operator initiated commands for collision avoidance manoeuvre (Red Button CAM) shall be single step commands
  - ATV commands (REQ330) With the exception of the Red Button CAM command, all operator initiated commands involving safety critical functions shall be two step operations with feedback from the function initiator

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

TORTUGA framework

- System side (green part)
  - spacecraft modelling
  - (sub)-system modelling
  - ground segment C&C model
- Human side (red part)
  - operator task modelling
  - training
  - operational procedure modelling
- Compatibility assessment phases made explicit



Spacecraft Modelling
Interactive Cooperative Objects Formalism
Spacecraft Modelling ith iteration
Requirements
Spacecraft model
Satellite Database
System Modelling
Interactive Cooperative Objects Formalism
System Modelling ith iteration
Requirements
System model
Satellite Database
Compatiblity Assessment
Interpretation
Compatiblity Assessment
Compatiblity Assessment
Legend
Notation
Document
Assessment
modelling
Process
Operator Task Modelling
ConcurTaskTrees (CTT) notation
Task Modelling ith iteration
Task model
Ground Segment Modelling
Interactive Cooperative Objects Formalism
Requirements
C&C Application Modelling ith iteration
System model
Usage
Operators
Operational Procedures Modelling
Interactive Cooperative Objects Formalism
Operational Procedure Modelling ith iteration
Operational procedure model
Satellite Database
Training
Operator Training Material
Compatiblity Assessment
Compatiblity Assessment

- Goals
  - Reduce the occurrence of erroneous events in safety-critical interactive systems/ground segment control rooms
  - Increase usability, safety and reliability

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES

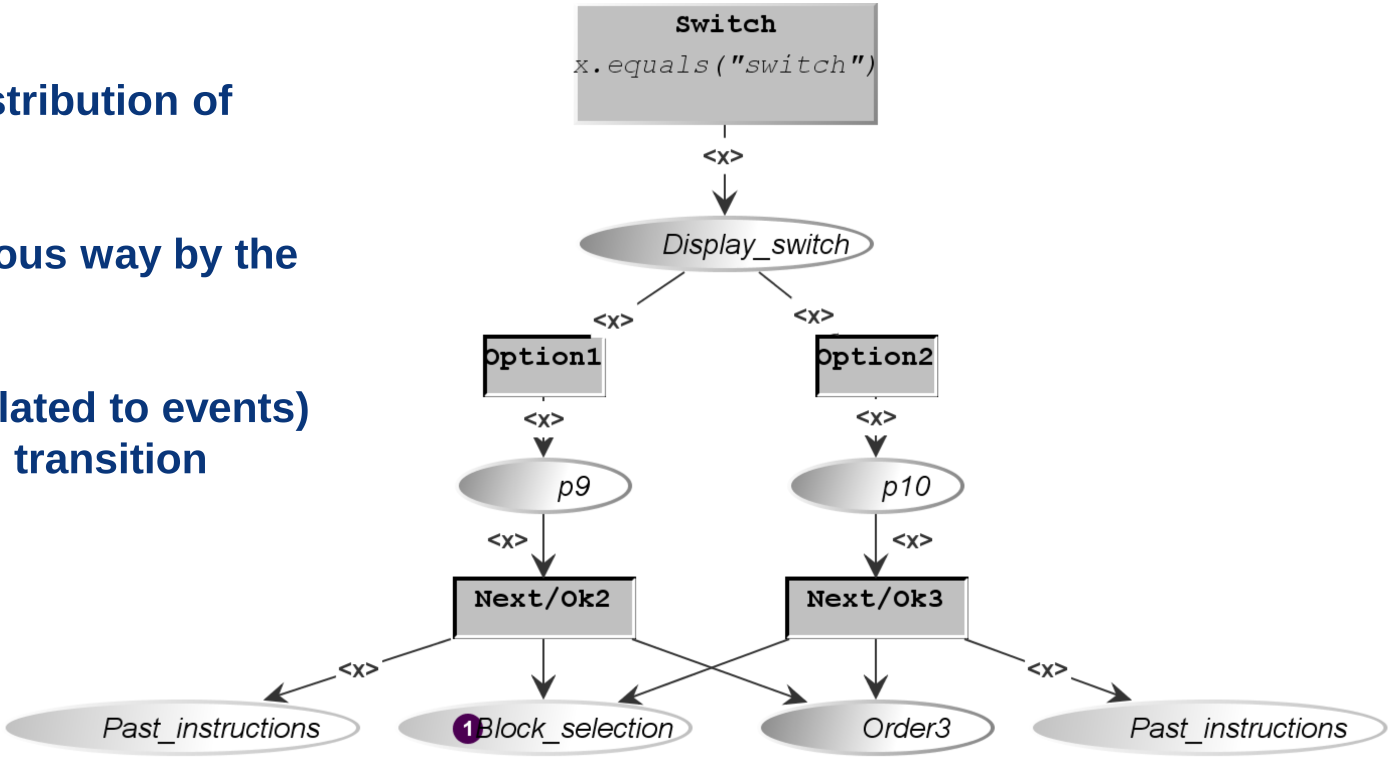
Overview of Interactive Cooperative Objects (ICO): a formal description technique

- ICOs, an object-oriented, Petri net-based formalism dedicated to the modelling and construction of highly interactive distributed systems

States are represented by the distribution of tokens into places

Actions triggered in an autonomous way by the system are called transitions

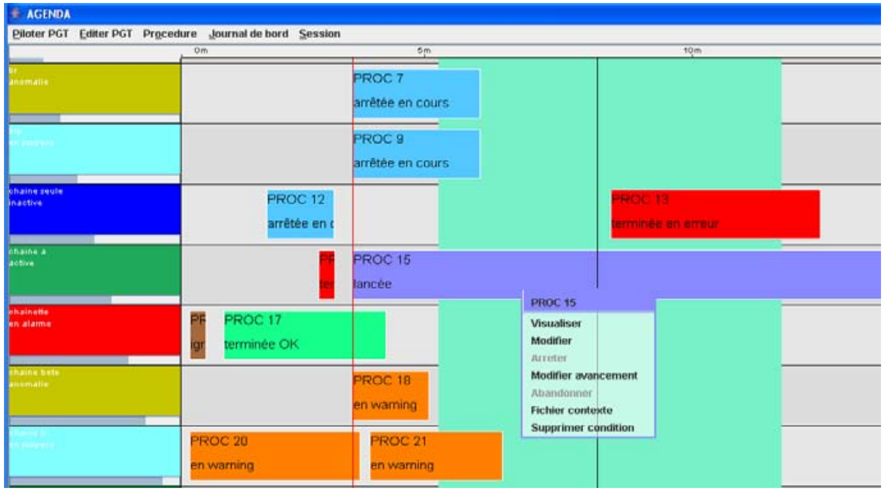
Actions triggered by users (or related to events) are represented by half bordered transition



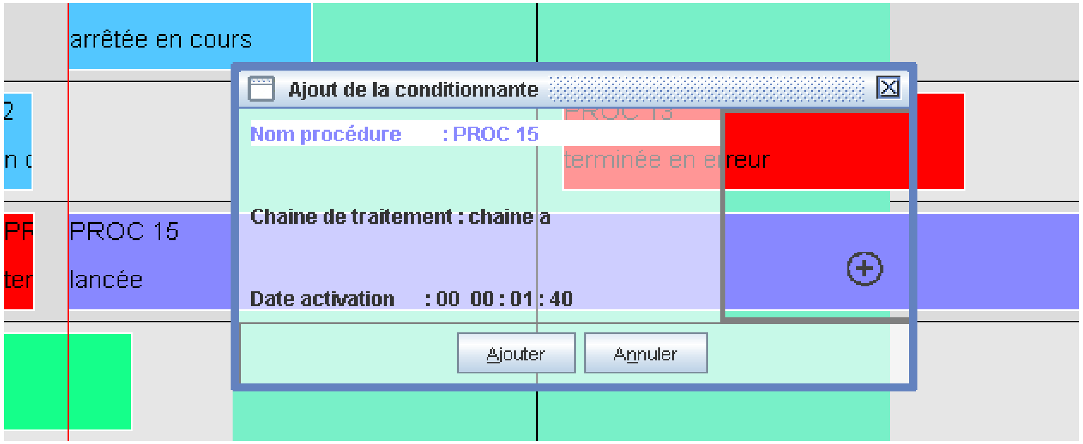
- ICOs has been applied to Civil & military cockpits, Command & control stations for drones and air traffic control

ICO tool: Petshop http://ihcs.irit.fr/petshop

Semi transparent menus



Click-through & multi-mouse

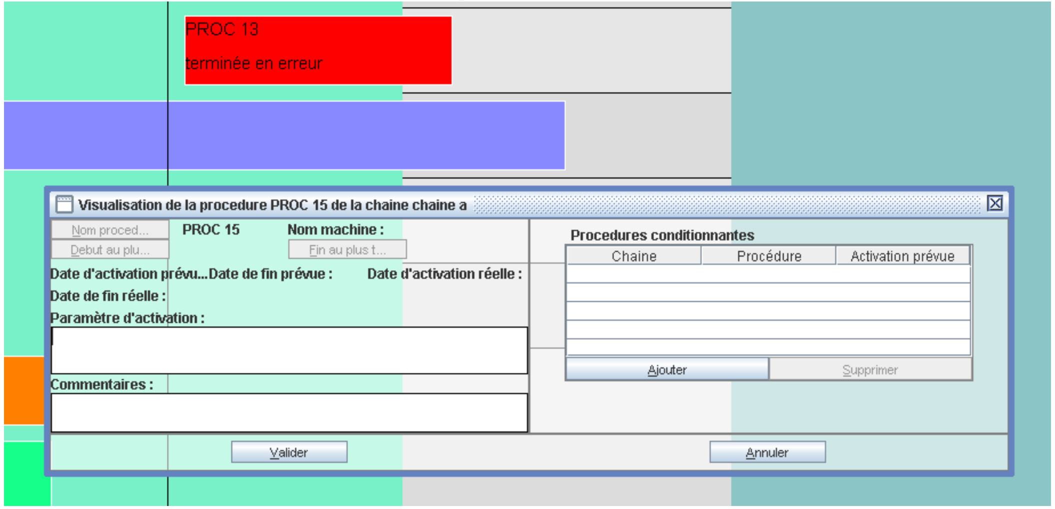


Nom procédure : PROC 15

Chaine de traitement : chaine a

Date activation : 00 00 : 01 : 40

Semi transparent windows



PROC 15 Nom machine :

Date d'activation prévu...Date de fin prévue : Date d'activation réelle :

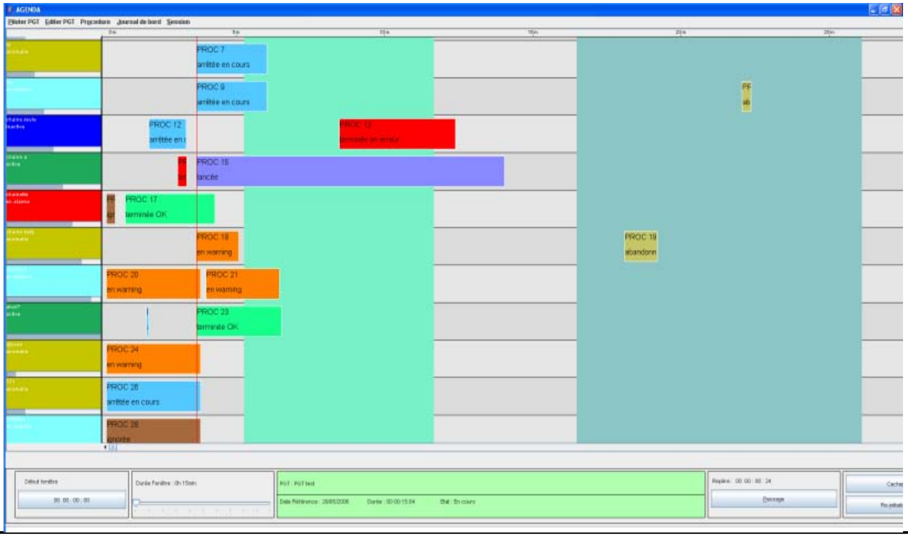
Date de fin réelle :

Paramètre d'activation :

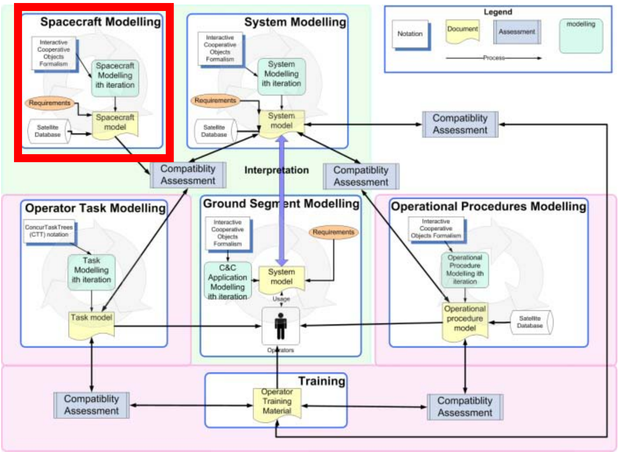
Commentaires :

Chaine	Procédure	Activation prévue

Continuos zoom



Spacecraft modelling


Spacecraft Modelling
Interactive Cooperative Objects Formalism
Spacecraft Modelling ith iteration
Requirements
Spacecraft model
Satellite Database
System Modelling
Interactive Cooperative Objects Formalism
System Modelling ith iteration
Requirements
System model
Satellite Database
Legend
Notation
Document
Assessment
modelling
Process
Compatiblity Assessment
Compatiblity Assessment
Interpretation
Compatiblity Assessment
Operator Task Modelling
ConcurTaskTrees (CTT) notation
Task Modelling ith iteration
Task model
Ground Segment Modelling
Interactive Cooperative Objects Formalism
Requirements
C&C Application Modelling ith iteration
System model
Usage
Operators
Operational Procedures Modelling
Interactive Cooperative Objects Formalism
Operational Procedure Modelling ith iteration
Operational procedure model
Satellite Database
Training
Operator Training Material
Compatiblity Assessment
Compatiblity Assessment

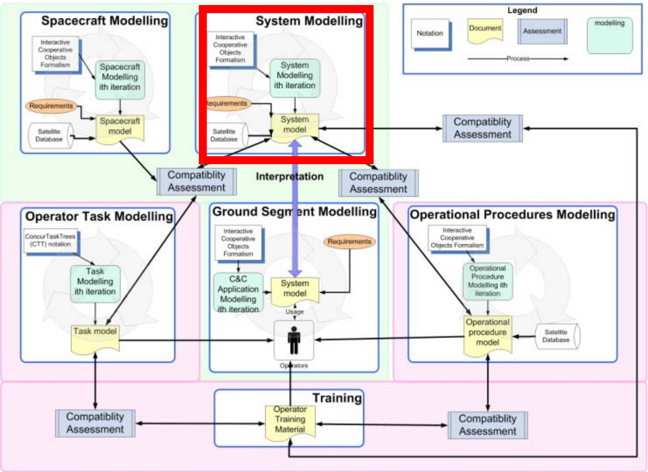
- Represents the entire Spacecraft (ATV)
- The selected sub-system for the case study is the Star Tracker

ATV simulation facility

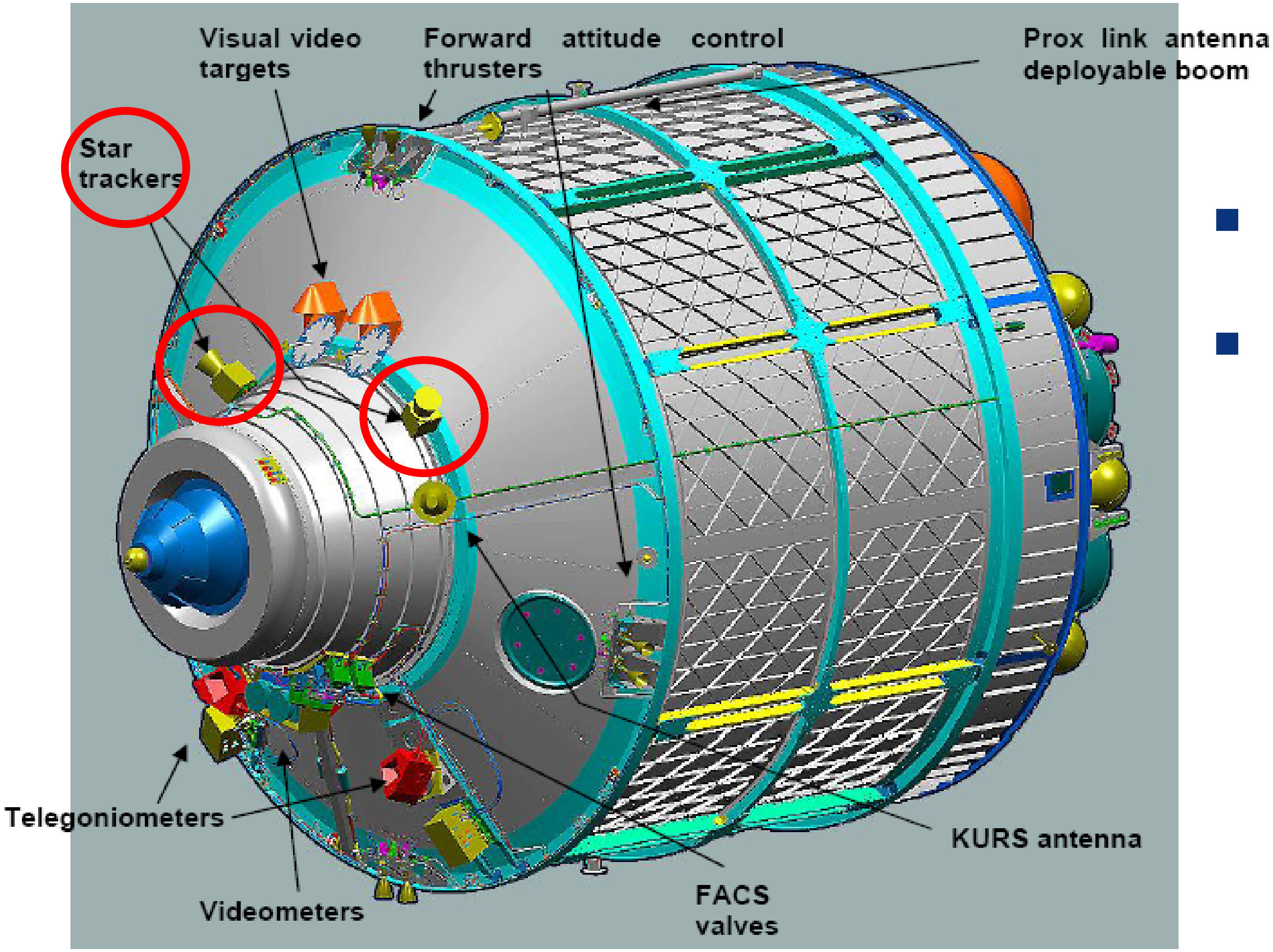
© ESA / EADS - S.Corvaja 2008

- Only useful for simulation purposes, for providing feedback
- Would be replaced by real platform and system when in operations

Sub-system modelling (1/2)


Spacecraft Modelling
Interactive Cooperative Objects Formalism
Spacecraft Modelling ith iteration
Requirements
Spacecraft model
Satellite Database
System Modelling
Interactive Cooperative Objects Formalism
System Modelling ith iteration
Requirements
System model
Satellite Database
Legend
Notation
Document
Assessment
modelling
Process
Compatiblity Assessment
Compatiblity Assessment
Interpretation
Compatiblity Assessment
Operator Task Modelling
ConcurTaskTrees (CTT) notation
Task Modelling ith iteration
Task model
Ground Segment Modelling
Interactive Cooperative Objects Formalism
Requirements
C&C Application Modelling ith iteration
System model
Usage
Operators
Operational Procedures Modelling
Interactive Cooperative Objects Formalism
Operational Procedure Modelling ith iteration
Operational procedure model
Satellite Database
Training
Operator Training Material
Compatiblity Assessment
Compatiblity Assessment

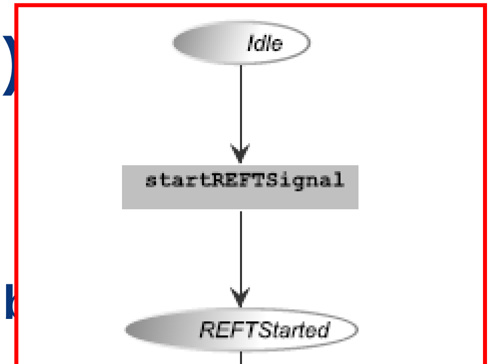
- Use ICO formalism to represent the dynamic behaviour of the Star Tracker

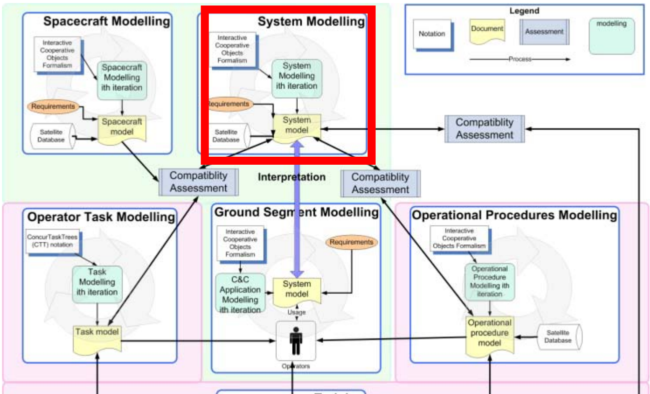


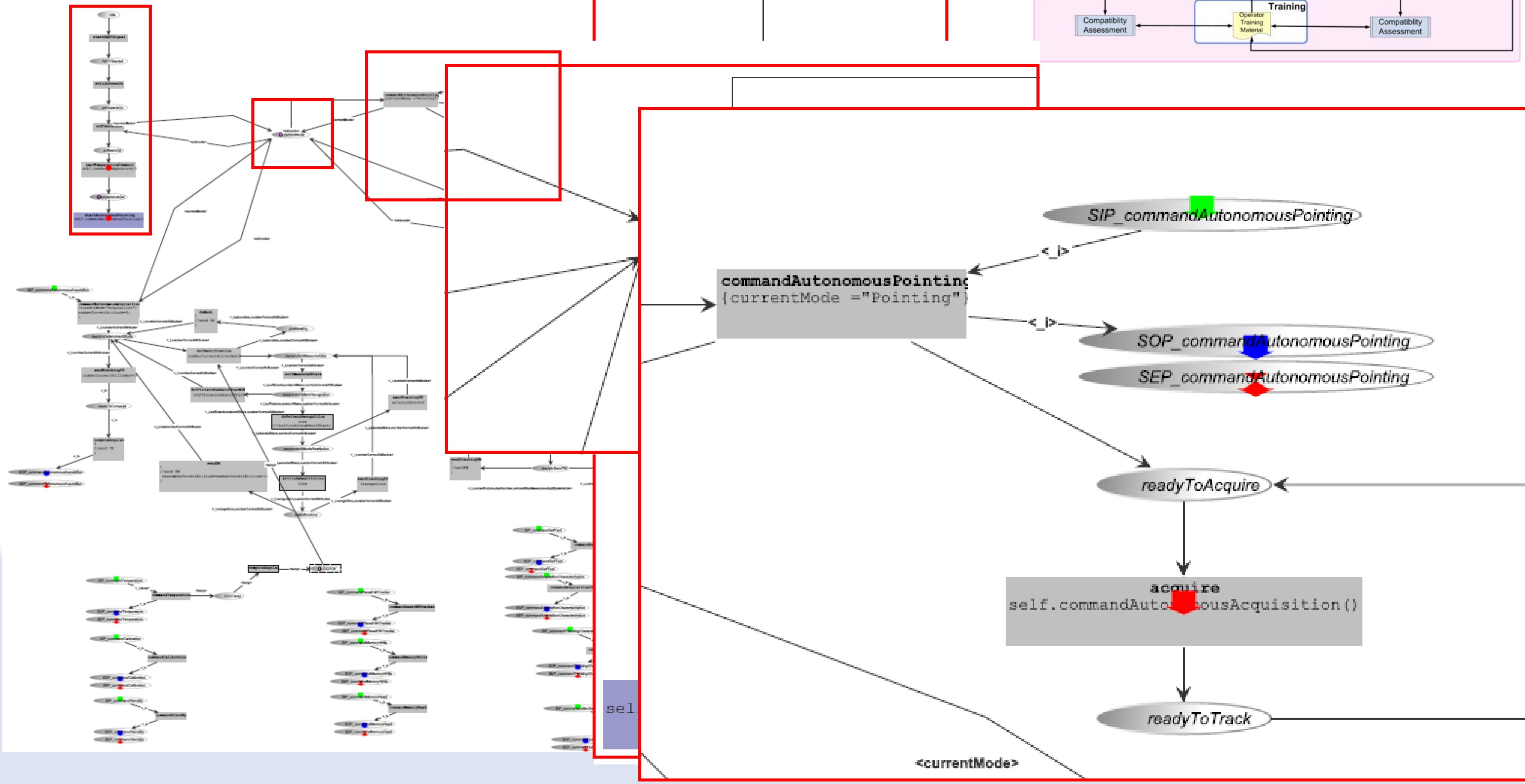
- Based on ATV User Manual documentation
- Included some statecharts with definitions of transitions

Sub-system modelling (2/2)

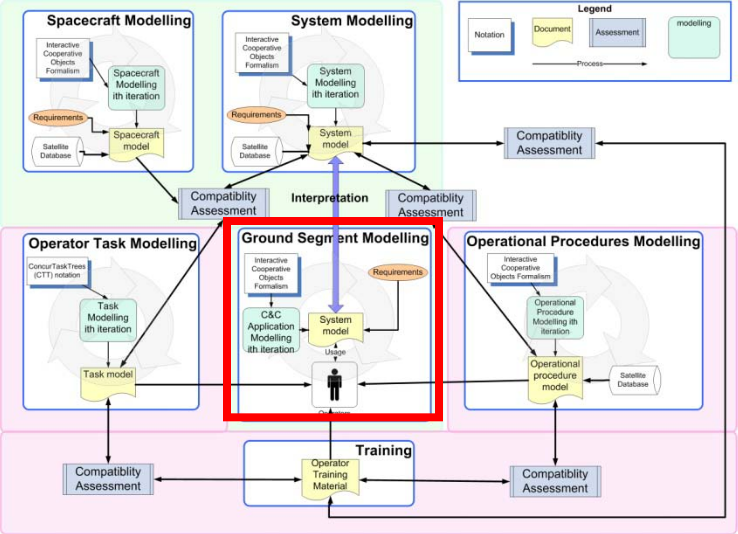
- Represents the Star Tracker b



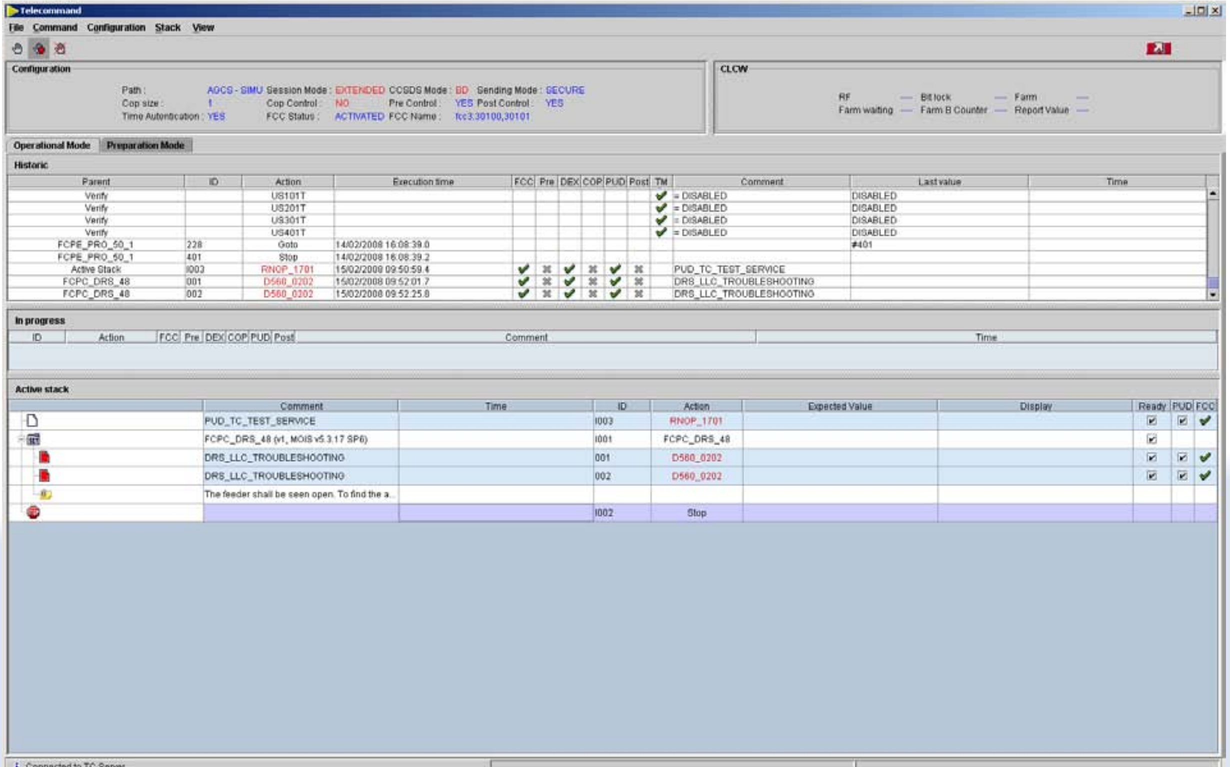

Spacecraft Modelling
Interactive Cooperative Objects Formalism
Spacecraft Modelling ith iteration
Requirements
Satellite Database
Spacecraft model
System Modelling
Interactive Cooperative Objects Formalism
System Modelling ith iteration
Requirements
Satellite Database
System model
Legend
Notation
Document
Assessment
modelling
Process
Compatibility Assessment
Compatibility Assessment
Interpretation
Compatibility Assessment
Operator Task Modelling
ConcurTaskTrees (CTT) notation
Task Modelling ith iteration
Task model
Ground Segment Modelling
Interactive Cooperative Objects Formalism
Requirements
C&C Application Modelling ith iteration
System model
Usage
Operators
Operational Procedures Modelling
Interactive Cooperative Objects Formalism
Operational Procedure Modelling ith iteration
Operational procedure model
Satellite Database
Training
Operator Training Material
Compatibility Assessment
Compatibility Assessment


SIP_commandAutonomousPointing
<_i>
commandAutonomousPointing
{currentMode ="Pointing"}
<_i>
SOP_commandAutonomousPointing
SEP_commandAutonomousPointing
readyToAcquire
acquire
self.commandAutonomousAcquisition()
readyToTrack
<currentMode>
sel

Ground segment (1/2)


Spacecraft Modelling
Interactive Cooperative Objects Formalism
Spacecraft Modelling ith iteration
Requirements
Spacecraft model
Satellite Database
System Modelling
Interactive Cooperative Objects Formalism
System Modelling ith iteration
Requirements
System model
Satellite Database
Legend
Notation
Document
Assessment
modelling
Process
Compatiblity Assessment
Compatiblity Assessment
Interpretation
Compatiblity Assessment
Operator Task Modelling
ConcurTaskTrees (CTT) notation
Task Modelling ith iteration
Task model
Ground Segment Modelling
Interactive Cooperative Objects Formalism
Requirements
C&C Application Modelling ith iteration
System model
Usage
Operators
Operational Procedures Modelling
Interactive Cooperative Objects Formalism
Operational Procedure Modelling ith iteration
Operational procedure model
Satellite Database
Training
Operator Training Material
Compatiblity Assessment
Compatiblity Assessment

- Command & Control application
- It’s only modelled component within the framework that has a UI



Configuration

Path : AOCS - SIMU Session Mode : EXTENDED CCSDS Mode : BD Sending Mode : SECURE
Cop size : 1 Cop Control : NO Pre Control : YES Post Control : YES
Time Autentication : YES FCC Status : ACTIVATED FCC Name : fcc3.30100,30101

CLCW

RF — Bit lock — Farm —
Farm waiting — Farm B Counter — Report Value —

Historic

Parent	ID	Action	Execution time	FCC	Pre	DEX	COP	PUD	Post	TM	Comment	Last value	Time
Verify		US101T								✓	= DISABLED	DISABLED	
Verify		US201T								✓	= DISABLED	DISABLED	
Verify		US301T								✓	= DISABLED	DISABLED	
Verify		US401T								✓	= DISABLED	DISABLED	
FCPE_PRO_50_1	228	Goto	14/02/2008 16:08:39.0									#401	
FCPE_PRO_50_1	401	Stop	14/02/2008 16:08:39.2										
Active Stack	I003	RNOP_1701	15/02/2008 09:50:59.4	✓	✗	✓	✗	✓	✗		PUD_TC_TEST_SERVICE		
FCPC_DRS_48	001	D560_0202	15/02/2008 09:52:01.7	✓	✗	✓	✗	✓	✗		DRS_LLC_TROUBLESHOOTING		
FCPC_DRS_48	002	D560_0202	15/02/2008 09:52:25.8	✓	✗	✓	✗	✓	✗		DRS_LLC_TROUBLESHOOTING		

In progress

ID	Action	FCC	Pre	DEX	COP	PUD	Post	Comment	Time

Active stack

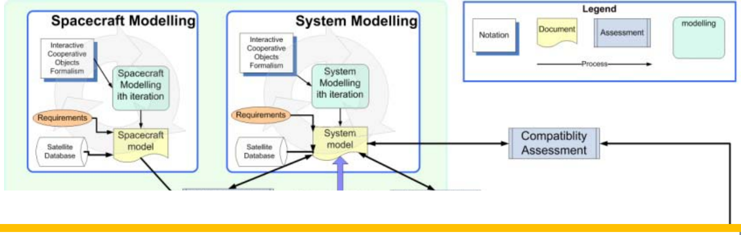
	Comment	Time	ID	Action	Expected Value	Display	Ready	PUD	FCC
	PUD_TC_TEST_SERVICE		I003	RNOP_1701			☑	☑	✓
	FCPC_DRS_48 (v1, MOIS v5.3.17 SP6)		I001	FCPC_DRS_48			☑		
	DRS_LLC_TROUBLESHOOTING		001	D560_0202			☑	☑	✓
	DRS_LLC_TROUBLESHOOTING		002	D560_0202			☑	☑	✓
	The feeder shall be seen open. To find the a...								
			I002	Stop					

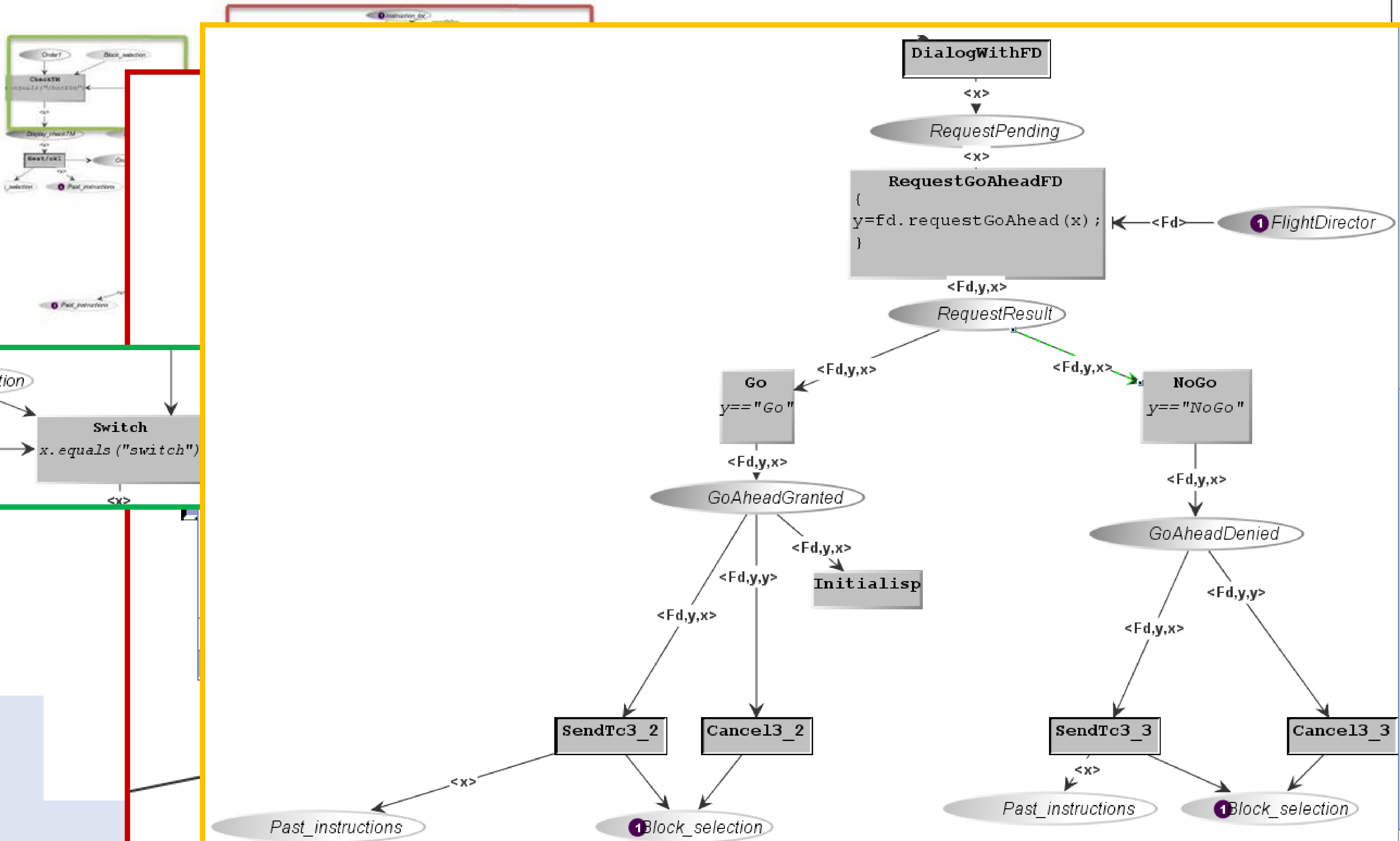
Connected to TC Server

ATV monitoring & control application

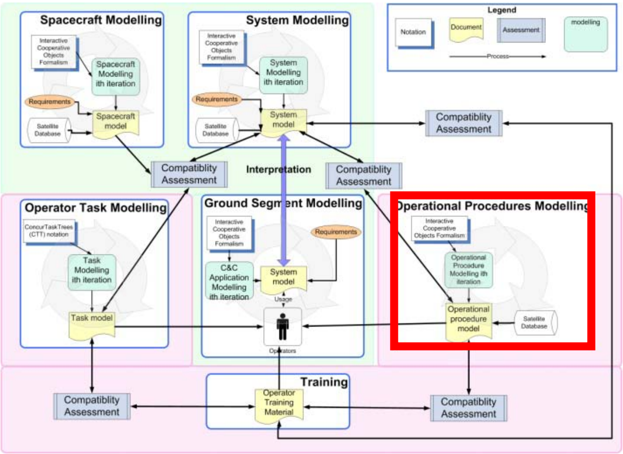
- Need description techniques able to cope with UIs
- Modelled an abstraction of full behaviour (generic behaviour for manipulating a procedure)

Ground segment (2/2)





STR operational procedure modelling (1/3)

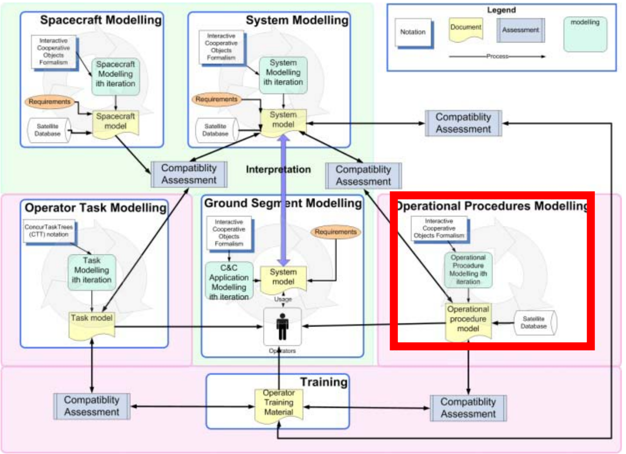

Spacecraft Modelling
Interactive Cooperative Objects Formalism
Spacecraft Modelling ith iteration
Requirements
Spacecraft model
Satellite Database
System Modelling
Interactive Cooperative Objects Formalism
System Modelling ith iteration
Requirements
System model
Satellite Database
Legend
Notation
Document
Assessment
modelling
Process
Compatiblity Assessment
Compatiblity Assessment
Interpretation
Compatiblity Assessment
Operator Task Modelling
ConcurTaskTrees (CTT) notation
Task Modelling ith iteration
Task model
Ground Segment Modelling
Interactive Cooperative Objects Formalism
Requirements
C&C Application Modelling ith iteration
System model
Usage
Operators
Operational Procedures Modelling
Interactive Cooperative Objects Formalism
Operational Procedure Modelling ith iteration
Operational procedure model
Satellite Database
Training
Operator Training Material
Compatiblity Assessment
Compatiblity Assessment

- **A Star Tracker operational procedure**
- **Procedures do not take into account UI behaviour**
  - **Procedures and C&C application developed in parallel**
- **Requirements related to UI impact the procedures**

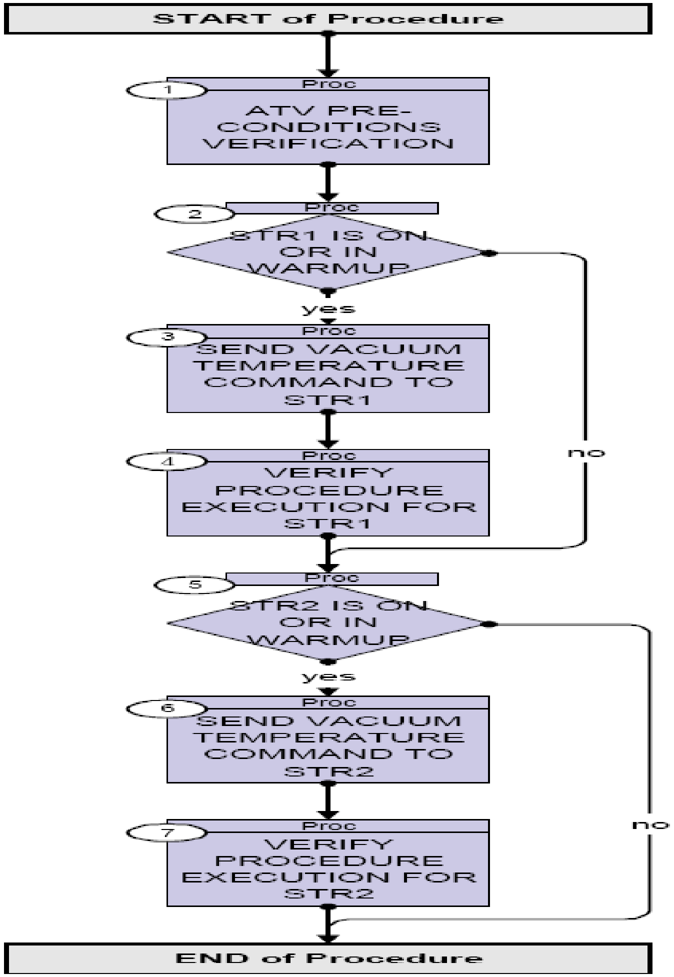
> “*With the exception of the Red Button CAM command, all operator initiated commands involving functions that could lead to catastrophic consequences shall be three step operations with feedback from the function initiator after each step prior to the acceptance of the command*”

- **Requirements & UI behaviour accounted for when running the procedure**

STR operational procedure modelling (2/3)

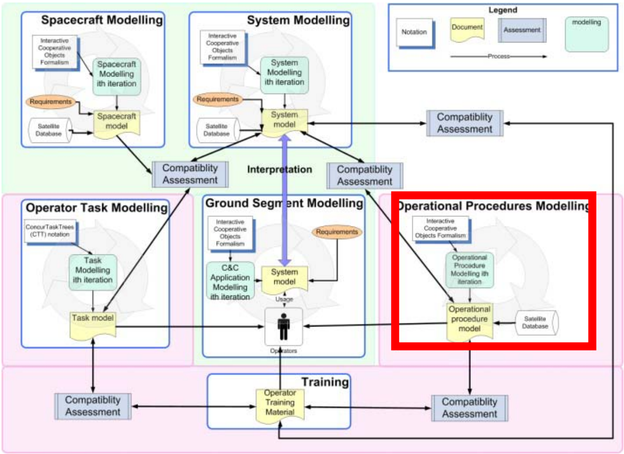

Spacecraft Modelling
Interactive Cooperative Objects Formalism
Spacecraft Modelling ith iteration
Requirements
Spacecraft model
Satellite Database
System Modelling
Interactive Cooperative Objects Formalism
System Modelling ith iteration
Requirements
System model
Satellite Database
Legend
Notation
Document
Assessment
modelling
Process
Compatiblity Assessment
Compatiblity Assessment
Interpretation
Compatiblity Assessment
Operator Task Modelling
ConcurTaskTrees (CTT) notation
Task Modelling ith iteration
Task model
Ground Segment Modelling
Interactive Cooperative Objects Formalism
Requirements
C&C Application Modelling ith iteration
System model
Usage
Operators
Operational Procedures Modelling
Interactive Cooperative Objects Formalism
Operational Procedure Modelling ith iteration
Operational procedure model
Satellite Database
Training
Operator Training Material
Compatiblity Assessment
Compatiblity Assessment

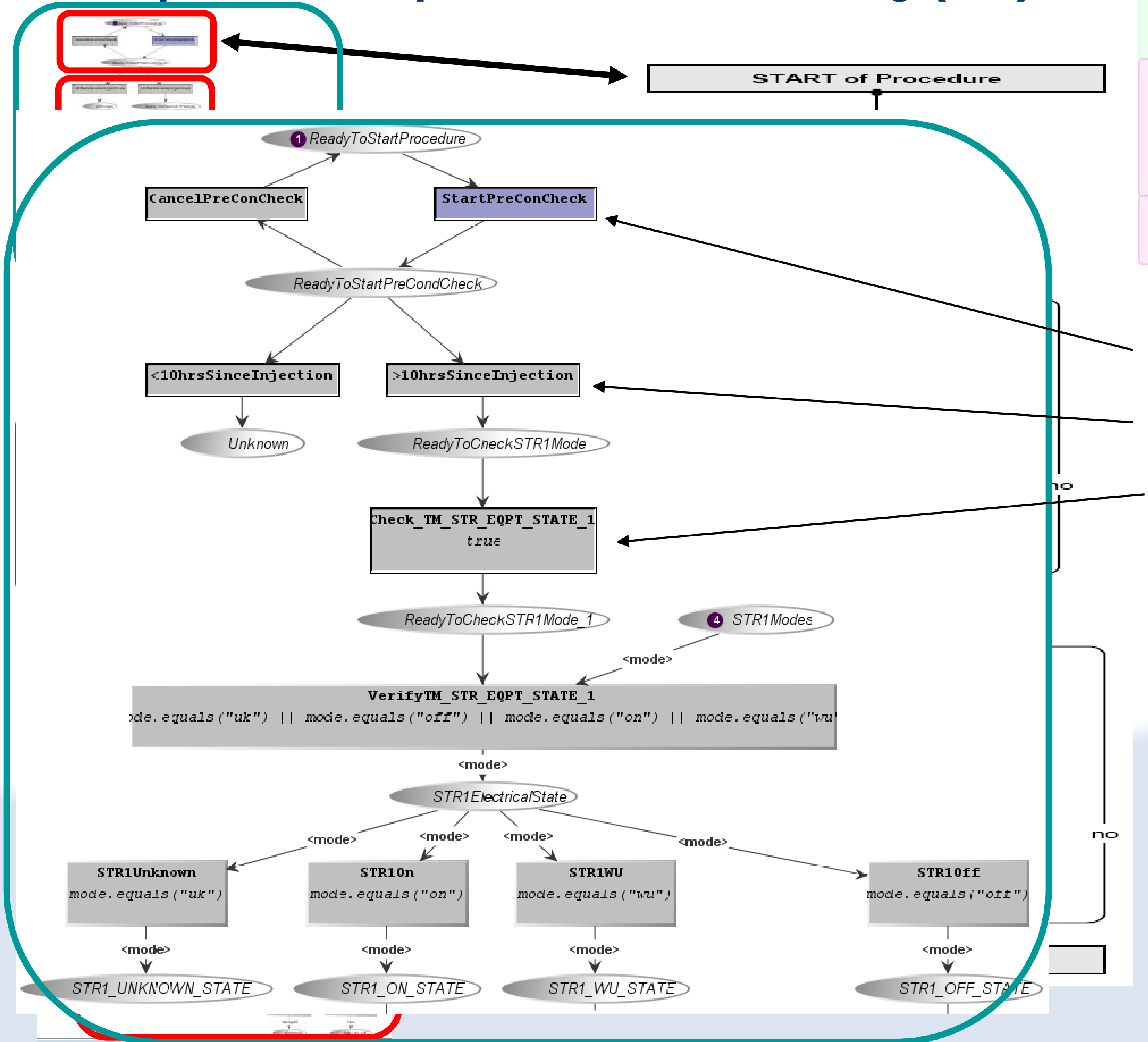
- Cooling down star tracker CCD sensor
- Once powered on, STR initialises and starts measurement acquisitions 10 minutes after


START of Procedure
1
Proc
ATV PRE-CONDITIONS VERIFICATION
2
Proc
STR1 IS ON OR IN WARMUP
yes
no
3
Proc
SEND VACUUM TEMPERATURE COMMAND TO STR1
4
Proc
VERIFY PROCEDURE EXECUTION FOR STR1
5
Proc
STR2 IS ON OR IN WARMUP
yes
no
6
Proc
SEND VACUUM TEMPERATURE COMMAND TO STR2
7
Proc
VERIFY PROCEDURE EXECUTION FOR STR2
END of Procedure

- Goal
  - This procedure includes a command to set the temperature of the STRs, which are on or in warm-up
  - To obtain the best performance of the STR, it is necessary to cool down the CCD sensor to -10°C (vacuum temperature) for 10 minutes after reception by the STR of the vacuum temperature command, which is sent by ATV-CC
- Ex. potential risk
  - Procedure must not be executed within the first 10 hours after Ariane 5 separation
  - A cooling temperature TC reduces the temperature of the CCD to -10°C
  - In the atmosphere, because of humidity, condensation appears on the CCD and pollutes it
  - The TC is therefore not allowed when the ATV is in the atmosphere
- Hazardous TC
  - STR_EC_TEMP “To command the order of the STRi peltier temperature regulation”

STR operational procedure modelling (3/3)


Spacecraft Modelling
Interactive Cooperative Objects Formalism
Spacecraft Modelling ith iteration
Requirements
Satellite Database
Spacecraft model
System Modelling
Interactive Cooperative Objects Formalism
System Modelling ith iteration
Requirements
Satellite Database
System model
Legend
Notation
Document
Assessment
modelling
Process
Compatiblity Assessment
Compatiblity Assessment
Interpretation
Compatiblity Assessment
Operator Task Modelling
ConcurTaskTrees (CTT) notation
Task Modelling ith iteration
Task model
Ground Segment Modelling
Interactive Cooperative Objects Formalism
Requirements
C&C Application Modelling ith iteration
System model
Usage
Operators
Operational Procedures Modelling
Interactive Cooperative Objects Formalism
Operational Procedure Modelling ith iteration
Operational procedure model
Satellite Database
Training
Compatiblity Assessment
Operator Training Material
Compatiblity Assessment



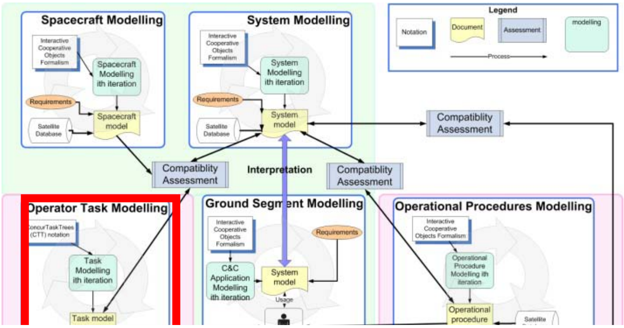
Start preconditions check

+/- 10hrs since injection

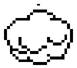
Check STR state

CENTRE NATIONAL D'ÉTUDES SPATIALES

Operator task modelling (1/3)


Spacecraft Modelling
Interactive Cooperative Objects Formalism
Spacecraft Modelling ith iteration
Requirements
Spacecraft model
Satellite Database
System Modelling
Interactive Cooperative Objects Formalism
System Modelling ith iteration
Requirements
System model
Satellite Database
Legend
Notation
Document
Assessment
modelling
Process
Compatiblity Assessment
Compatiblity Assessment
Interpretation
Compatiblity Assessment
Operator Task Modelling
ConcurTaskTrees (CTT) notation
Task Modelling ith iteration
Task model
Ground Segment Modelling
Interactive Cooperative Objects Formalism
Requirements
C&C Application Modelling ith iteration
System model
Usage
Operational Procedures Modelling
Interactive Cooperative Objects Formalism
Operational Procedure Modelling ith iteration
Operational procedure
Satellite

CTT Task Types

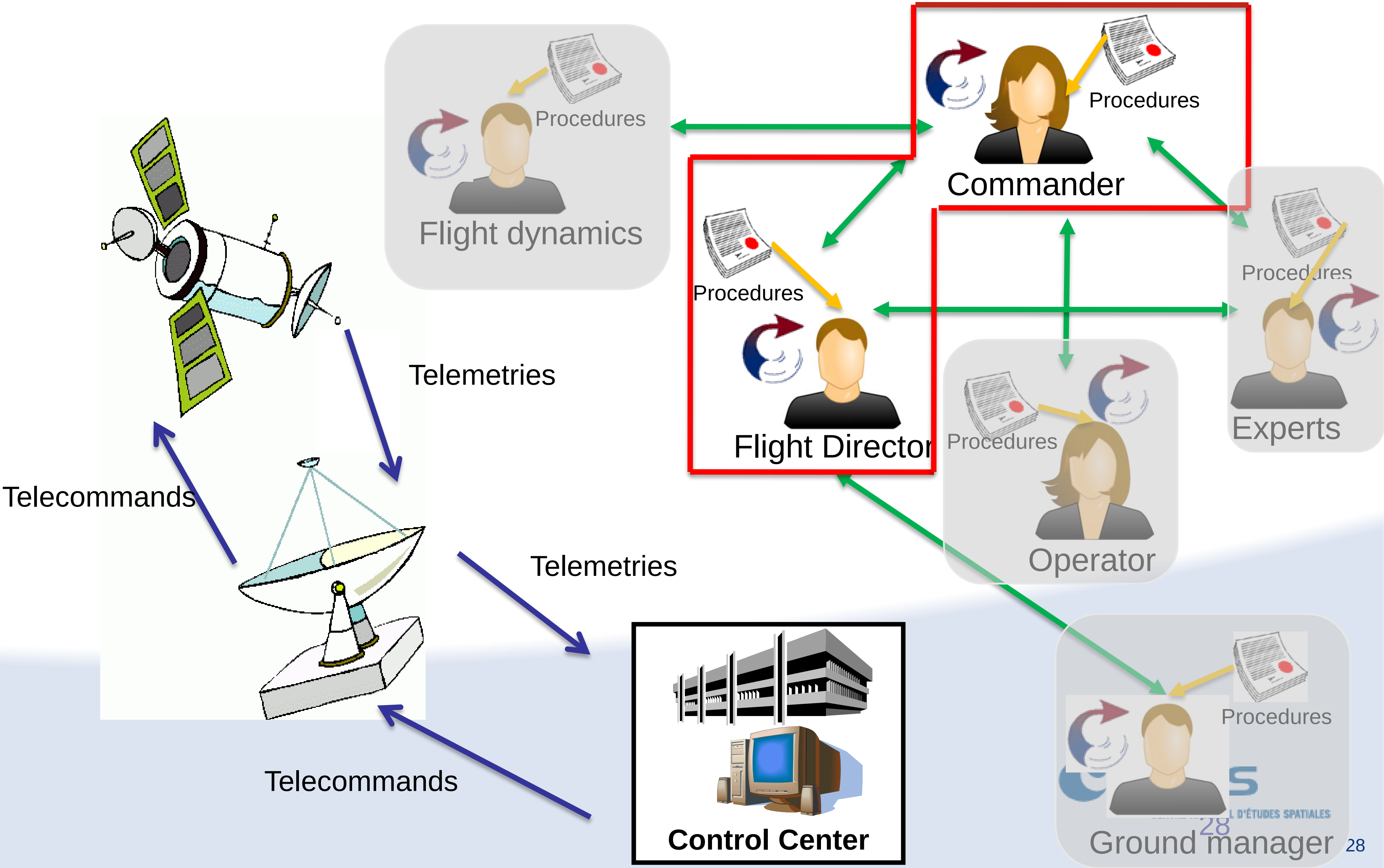
Graphical Symbols	Description
	Abstract Tasks: Tasks that which require complex activities whose performance cannot be univocally allocated
	User Tasks: Usually they are important cognitive activities
	Application Tasks: Can supply information to the user
	Interaction Tasks: Between the user and the system

CTT Temporal Operators

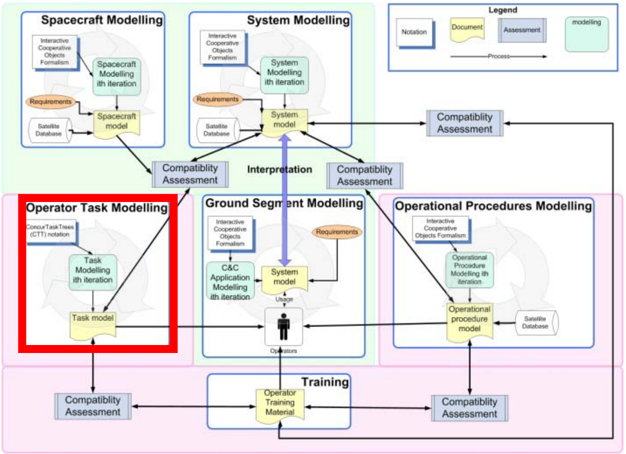
Notation	Description
T1 >>T2	Enabling
T1 [ ]>>T2	Enabling with information processing
T1 [>T2	Deactivation
T1 [] T2	Choice
T1 *	Iteration
T1 [I] T2	Concurrency with information exchange
T1 |>T2	Suspend resume
T1 | | | T2	Independent concurrency
T1 (n)	Finite iteration
[T1]	Optional task

Operator task modelling (2/3) : Control room interactions

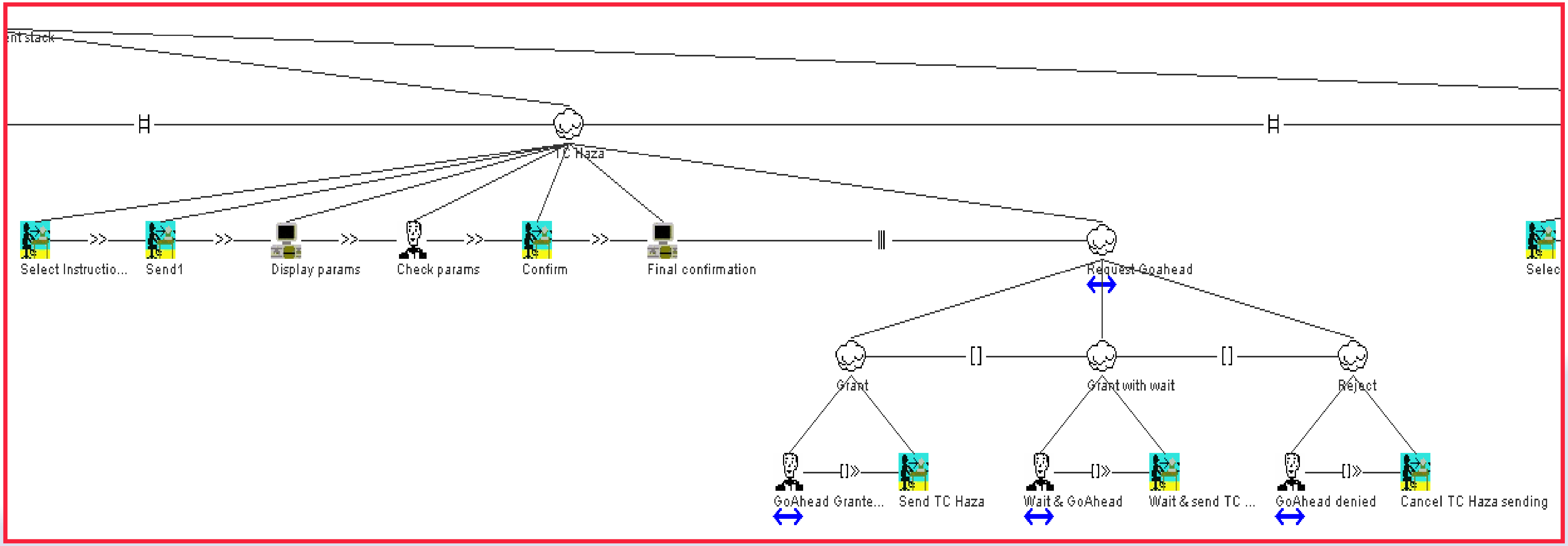
Reminder



Operator task modelling (3/3)

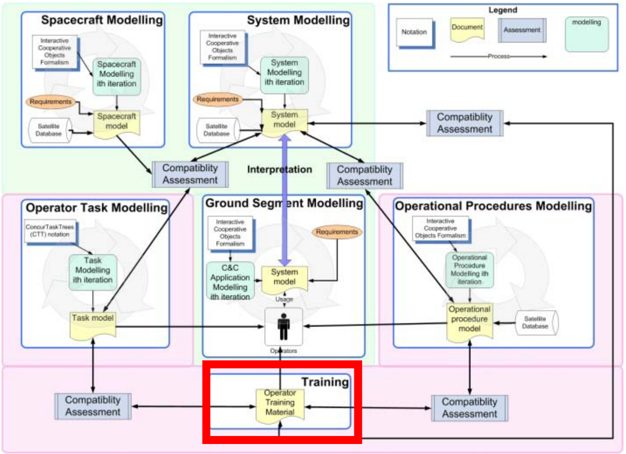


Spacecraft Modelling
Interactive Cooperative Objects Formalism
Spacecraft Modelling ith iteration
Requirements
Spacecraft model
Satellite Database
System Modelling
Interactive Cooperative Objects Formalism
System Modelling ith iteration
Requirements
System model
Satellite Database
Legend
Notation
Document
Assessment
modelling
Process
Compatiblity Assessment
Interpretation
Compatiblity Assessment
Compatiblity Assessment
Operator Task Modelling
ConcurTaskTrees (CTT) notation
Task Modelling ith iteration
Task model
Ground Segment Modelling
Interactive Cooperative Objects Formalism
Requirements
C&C Application Modelling ith iteration
System model
Usage
Operators
Operational Procedures Modelling
Interactive Cooperative Objects Formalism
Operational Procedure Modelling ith iteration
Operational procedure model
Satellite Database
Training
Operator Training Material
Compatiblity Assessment
Compatiblity Assessment



Excerpt only of Commander task model

Training



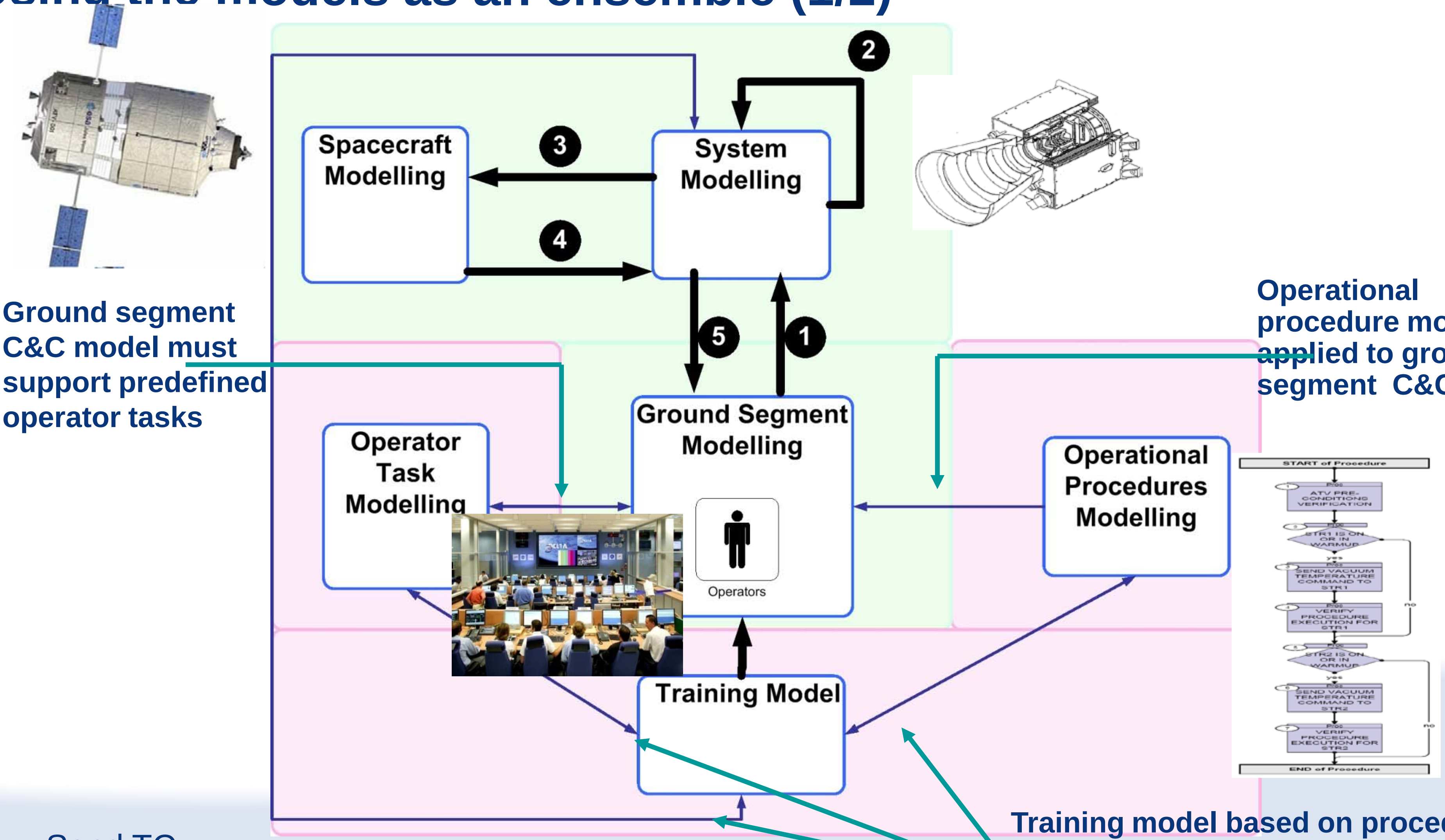
Spacecraft Modelling
Interactive Cooperative Objects Formalism
Spacecraft Modelling ith iteration
Requirements
Spacecraft model
Satellite Database
System Modelling
Interactive Cooperative Objects Formalism
System Modelling ith iteration
Requirements
System model
Satellite Database
Legend
Notation
Document
Assessment
modelling
Process
Compatiblity Assessment
Compatiblity Assessment
Interpretation
Compatiblity Assessment
Operator Task Modelling
ConcurTaskTrees (CTT) notation
Task Modelling ith iteration
Task model
Ground Segment Modelling
Interactive Cooperative Objects Formalism
Requirements
C&C Application Modelling ith iteration
System model
Usage
Operators
Operational Procedures Modelling
Interactive Cooperative Objects Formalism
Operational Procedure Modelling ith iteration
Operational procedure model
Satellite Database
Training
Operator Training Material
Compatiblity Assessment
Compatiblity Assessment

- Inputs
  - STR behaviour model
  - ATV-CC M&C behaviour model
  - Related requirements
  - STR operational procedure

- Work in process
  - Once the other models are complete, start working on training model
  - Based on ensuring that tasks are performed as planned
  - Study how people learn
  - Use formal description techniques to ensure ALL potential C&C system states have been passed through by operators
  - Test all branches of a procedure
  - If problems are encountered, they can be specifically identified via model analysis, can be re-performed, to understand which transition/token caused an erroneous state to occur

CENTRE NATIONAL D'ÉTUDES SPATIALES

Using the models as an ensemble (1/2)


2
Spacecraft Modelling
3
System Modelling
4
5
1
Operator Task Modelling
Ground Segment Modelling
Operators
Operational Procedures Modelling
Training Model
START of Procedure
ATV PRE-CONDITIONS VERIFICATION
STR1 IS ON OR IN WARMUP
yes
no
SEND VACUUM TEMPERATURE COMMAND TO STR1
VERIFY PROCEDURE EXECUTION FOR STR1
STR2 IS ON OR IN WARMUP
yes
no
SEND VACUUM TEMPERATURE COMMAND TO STR2
VERIFY PROCEDURE EXECUTION FOR STR2
END of Procedure

Ground segment C&C model must support predefined operator tasks

Operational procedure model applied to ground segment C&C model

Training model based on procedures, task model ground segment application & system behaviour

1. Send TC
2. Modify STR state
3. Update ATV model
4. Receive feedback from ATV model
5. Update system status on C&C application

Using the models as an ensemble (2/2)

- Compatibility of models
  - Lexical level – information required in one model is made available in other ones (if the user has to trigger a command (in the task model) that command must be offered (by the system model))
  - Syntactic level – if there is required sequencing (for instance the procedure requires to perform a start on the system and then a check, that sequence must be valid on the system model (Ex. For the STR do A then B, must be represented in procedure, reflected in the C&C UI and in the commander task model)
  - Semantic level – corresponds to the meaning of the system or requirements (Ex. 3 click requirement ensures that it's impossible to send a Hazardous TC without 3 clicks) i.e. the safety requirement is compatible with the behaviour of the CC UI
- Synergistic use of models: usage of several models at a time can provide additional benefits e.g. if the user triggers the help system for advice on how to reach a given goal, the synergistic use of that information with the current state of the system will make it possible to provide contextual help i.e. what actions to perform in order to go from the current state to the desired one

Initial results and future work

- Early stage of TORTUGA project
  - Work package 1 (state of the art on modelling techniques) delivered
- Dedicated representative from CNES “operations” providing input into the R&T project
- 4 models produced based on ATV example (STR, Task, C&C, Procedure)
- Shown feasibility of methods and techniques
- Future work (2009-2011)
  - Integration task/system/training model
  - Tool development
  - Selection of a pertinent case study
- Long-term objectives
  - Integration of framework and models within the CNES development process by CNES agents and industrial partners

Questions?

- **Interacting Humans with Computer Systems (IHCS) Team http://ihcs.irit.fr**
- **TORTUGA http://ihcs.irit.fr/tortuga**
- **ICO & Petshop references**
  - Palanque, P. Navarre, D., Basnyat, S., Usability Service Continuation through Reconfiguration of Input and Output Devices in Safety Critical Interactive Systems. The 27th International Conference on Computer Safety, Reliability and Security (SAFECOMP 2008), 22-25 September 2008, Newcastle upon Tyne, UK
  - Navarre, D., Palanque, P., Ladry, J.F., Basnyat, S. (2008). An Architecture and a Formal Description Technique for User Interaction Reconfiguration of Safety Critical Interactive Systems. The XVth International Workshop on the Design, Verification and Specification of Interactive Systems (DSVIS 2008). Kingston, Ontario, Canada. July 16-18 2008.
  - Ladry, JF., Palanque, P., Basnyat, S., Barboni, E., Navarre, D. (2008) Dealing with Reliability and Evolvability in Description Techniques for Next Generation User Interfaces. CHI 2008 Workshop on UIDLs for Next Generation User Interfaces, Florence, Italy. April 5-10 2008
  - Barboni, E., Navarre, D., Palanque, P., Basnyat, S. A Formal Description Technique for the Behavioural Description of Interactive Applications Compliant with ARINC Specification 661. IEEE Second International Symposium on Industrial Embedded Systems - SIES'2007. Special Session on Behavioural Models for Embedded Systems, Hotel Costa da Caparica, Lisbon, Portugal, 4-6 July 2007
  - Eric Barboni, Stéphane Conversy, David Navarre & Philippe Palanque. "Model-Based Engineering of Widgets, User Applications and Servers Compliant with ARINC 661 Specification." Proceedings of the 13th conference on Design Specification and Verification of Interactive Systems (DSVIS 2006), Dublin, Ireland, July 2006, Lecture Notes in Computer Science, Springer Verlag.
- **Application domain: Aeronautics**
  - Palanque, P., Basnyat, S., Poupart, P. (2008) A Model-Based Approach Centred on Operational Procedures for the Development of Reliable and Usable Ground Segment Systems. (SpaceOps 2008) 12-16 May 2008, Heidelberg, Germany.
  - Eric Barboni, David Navarre, Philippe Palanque & Sandra Basnyat. "Exploitation of Formal Specification Techniques for ARINC 661 Interactive Cockpit Applications." Proceedings of HCI aero conference, (HCI Aero 2006), Seatle, USA, Sept. 2006

Sandra STEERE & Erwann POUPART
† Ground Segment Systems Office (DCT/PS/SGE), CNES, Toulouse, France
sandra.steere@cnes.fr, erwann.poupart@cnes.fr

Philippe PALANQUE
†† Interacting Humans with Computing Systems IRIT, University Paul Sabatier, Toulouse, France
palanque@irit.fr   http://ihcs.irit.fr/palanque/

cnes
CENTRE NATIONAL D'ÉTUDES SPATIALES