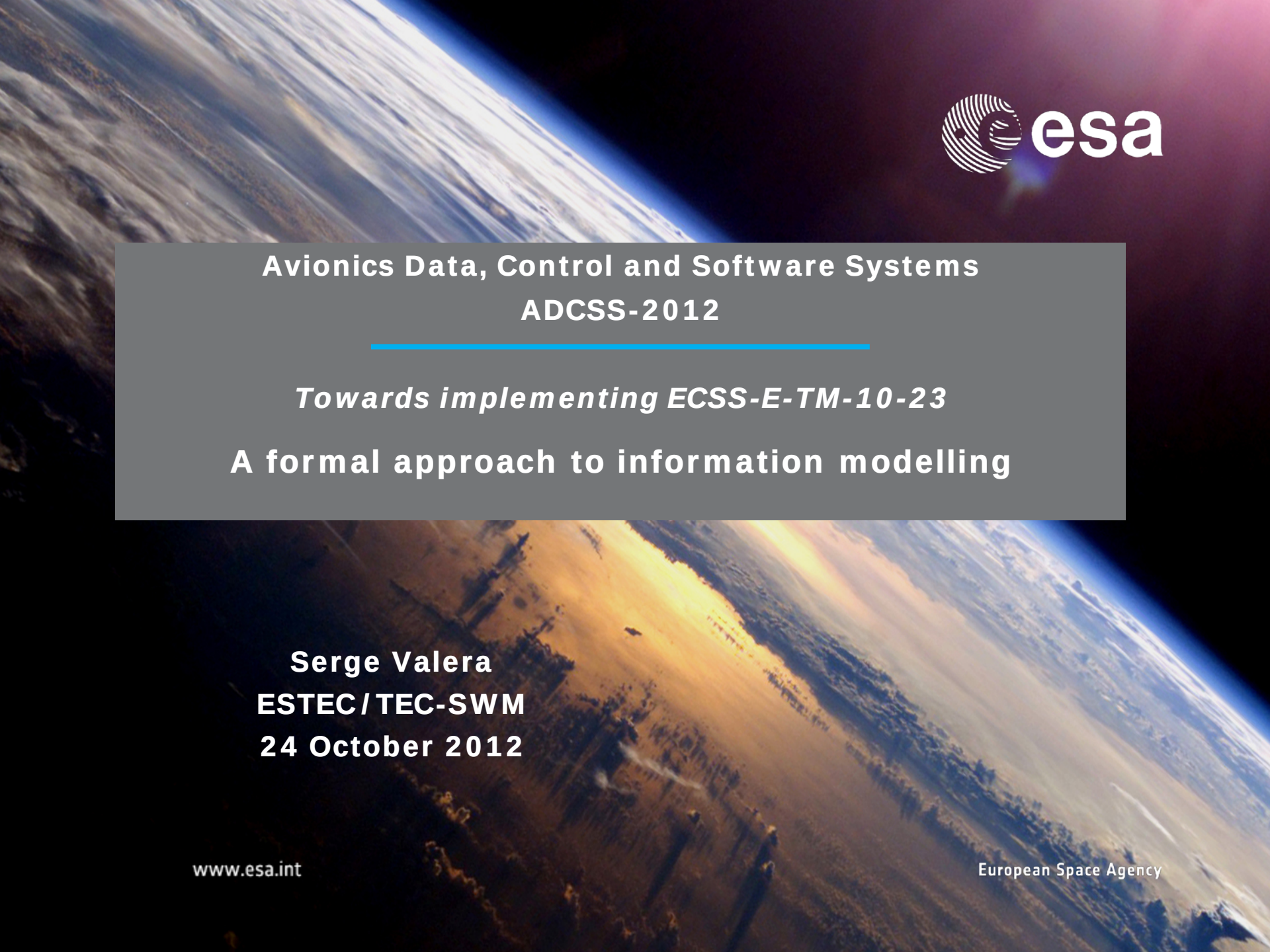


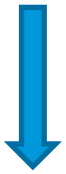
Avionics Data, Control and Software Systems
ADCSS-2012

Towards implementing ECSS-E-TM-10-23

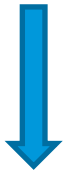
A formal approach to information modelling

Serge Valera
ESTEC / TEC-SWM
24 October 2012

Working Together (interoperability)



Sharing and reusing data, information, knowledge



Semantic (semantic interoperability)

WHAT is DATA, WHAT is INFORMATION

- **DATA**

  "Data" on its own carries no meaning.

  Examples:

  "Val Thorens" , "2300"

- **INFORMATION**

  In order for "data" to become "information", it must be interpretable, that means *extended with Semantics*, e.g. "what the nouns refer to and what the verb means".

  Examples:

  "Val Thorens" refers to the highest ski resort in Europe.

  "2300 is meant to be 2300 meters above sea level"

  The missing verb is "is located at"

WHAT is KNOWLEDGE

- **KNOWLEDGE**

  Knowledge is when we know everything about the validation associated with the information.

  Examples:

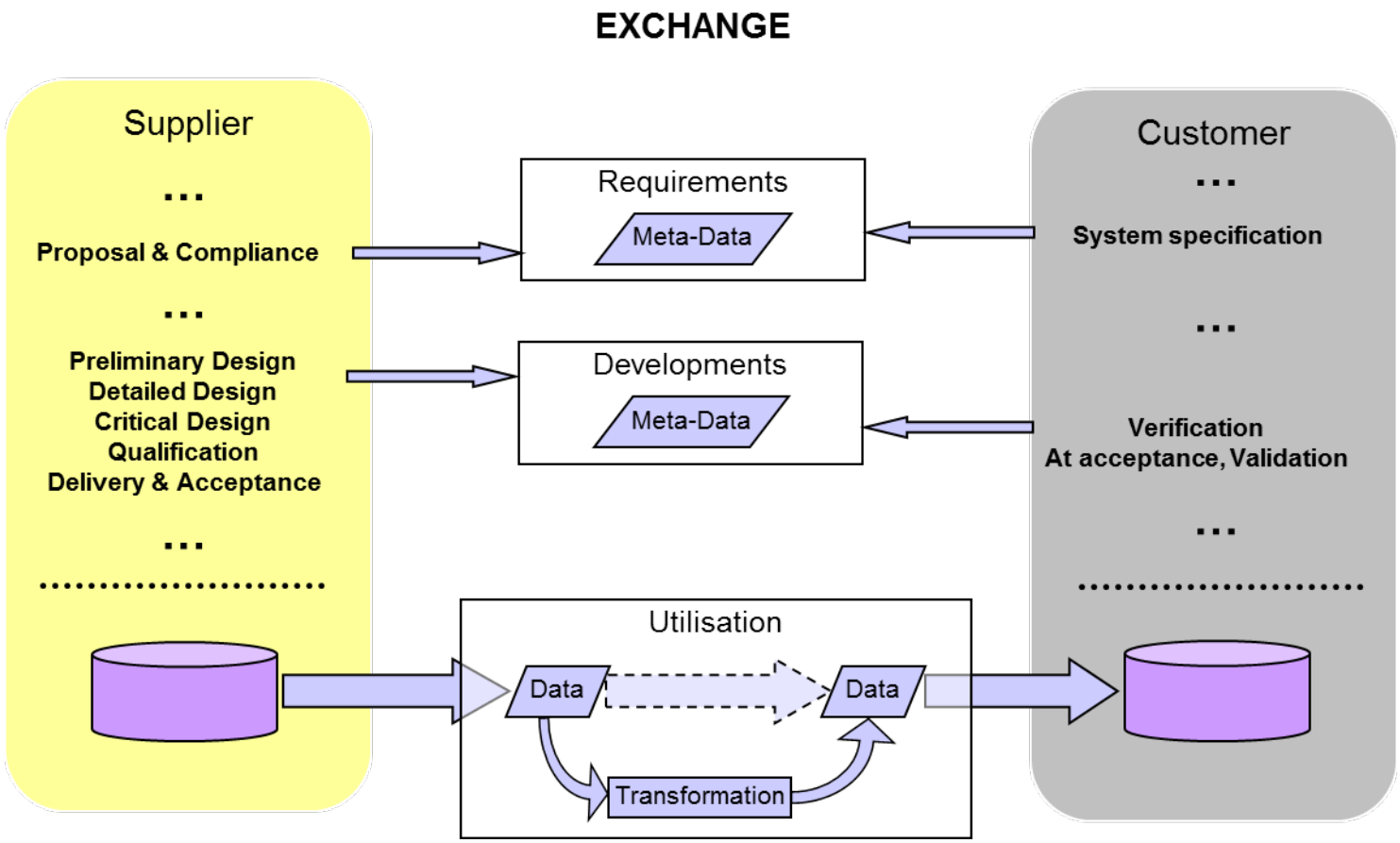
  Val Thorens is a ski resort in Europe !

  True → Val Thorens is located in the Alps.

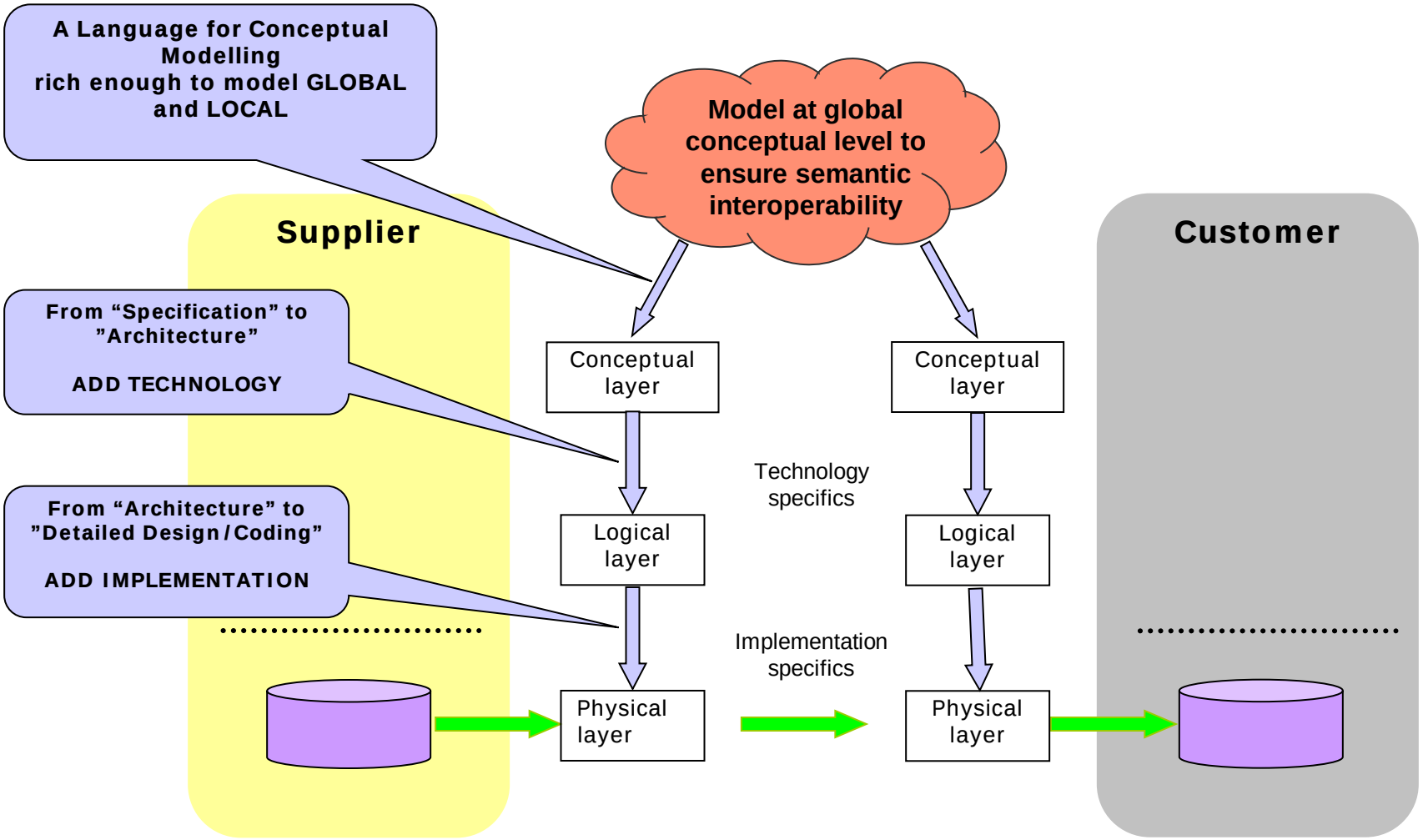
  Val Thorens is the highest ski resort in Europe !

  True → If one populates all ski resorts located in Europe together with their altitude, one can derive and as such validate that Val Thorens is the highest ski resort in Europe.

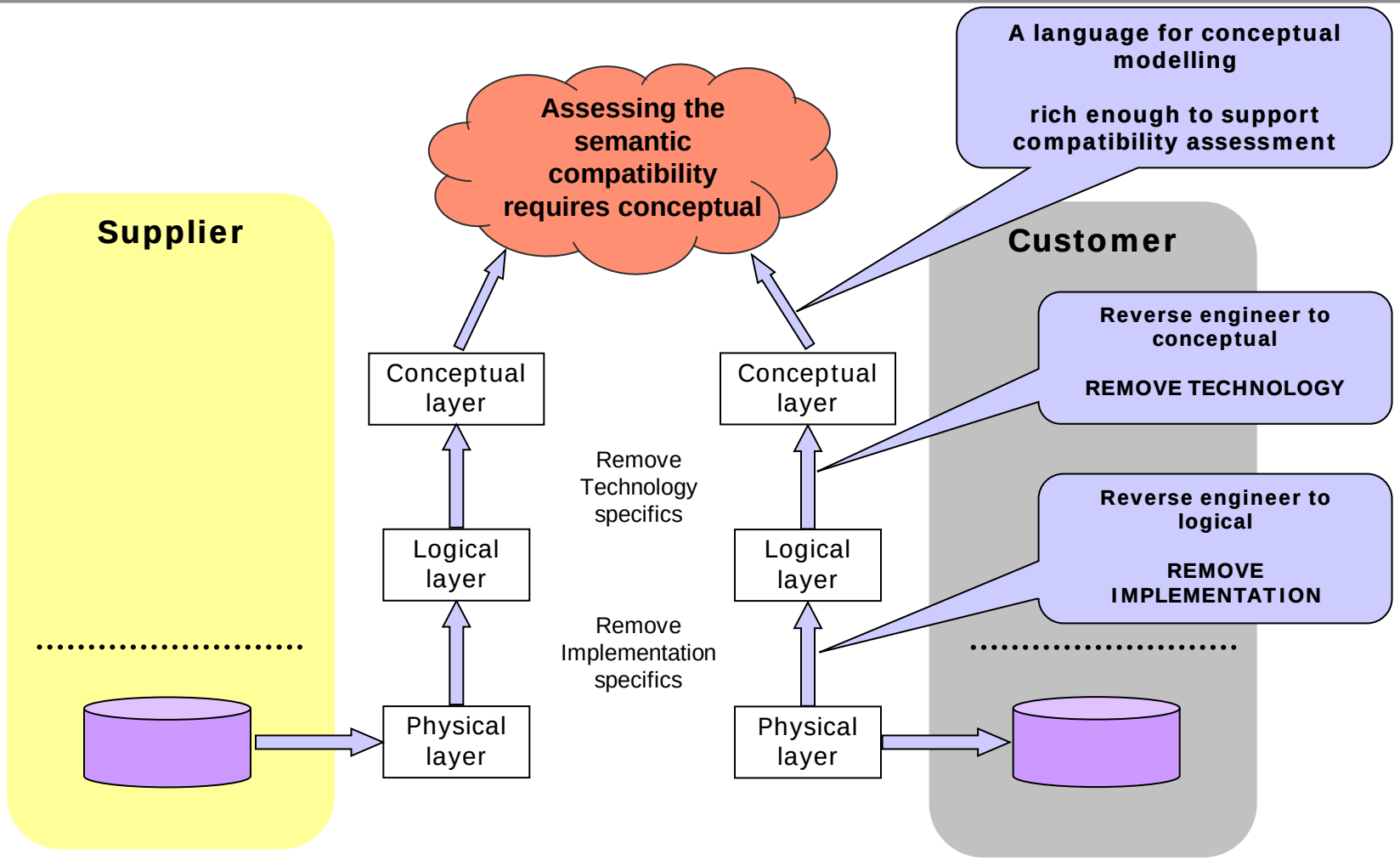
Working together…



Semantic Interoperability - Engineering



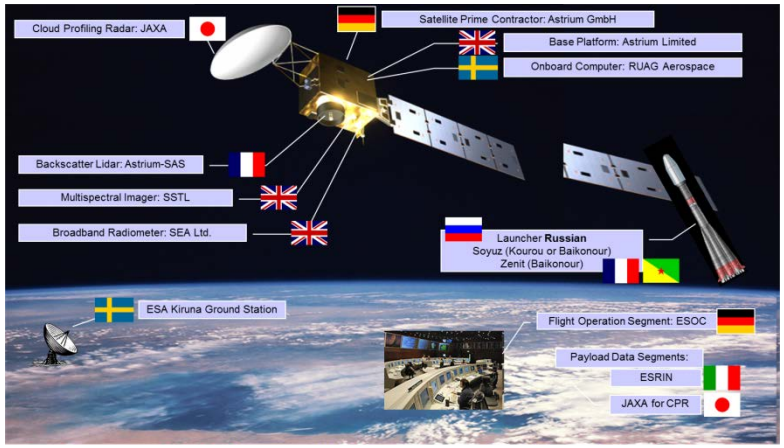
Semantic Interoperability – reverse engineering



The ECSS Vision

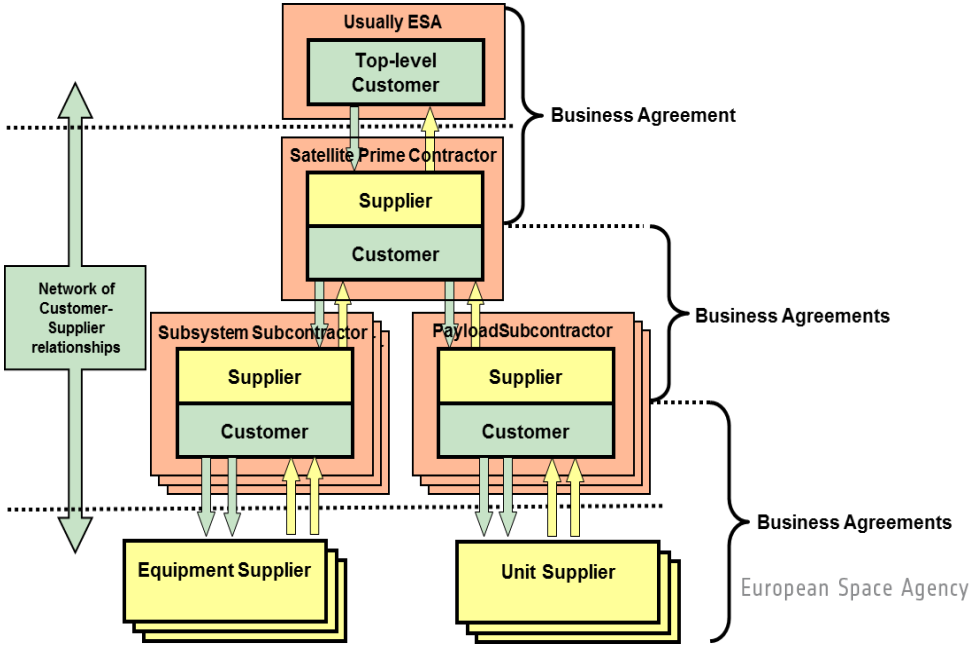
What is the ECSS vision?

Means by which, we, in the European Space Business, can solve the problematic of "**Working Together**".



What is the ECSS-E-TM-10-23A?

A formalization of that vision focusing on **semantic** and **semantic interoperability**.



The ECSS coverage

What does ECSS cover?

The WHAT ! i.e. the System Requirements with, beyond others, the objective to exclude any implementation specifics.

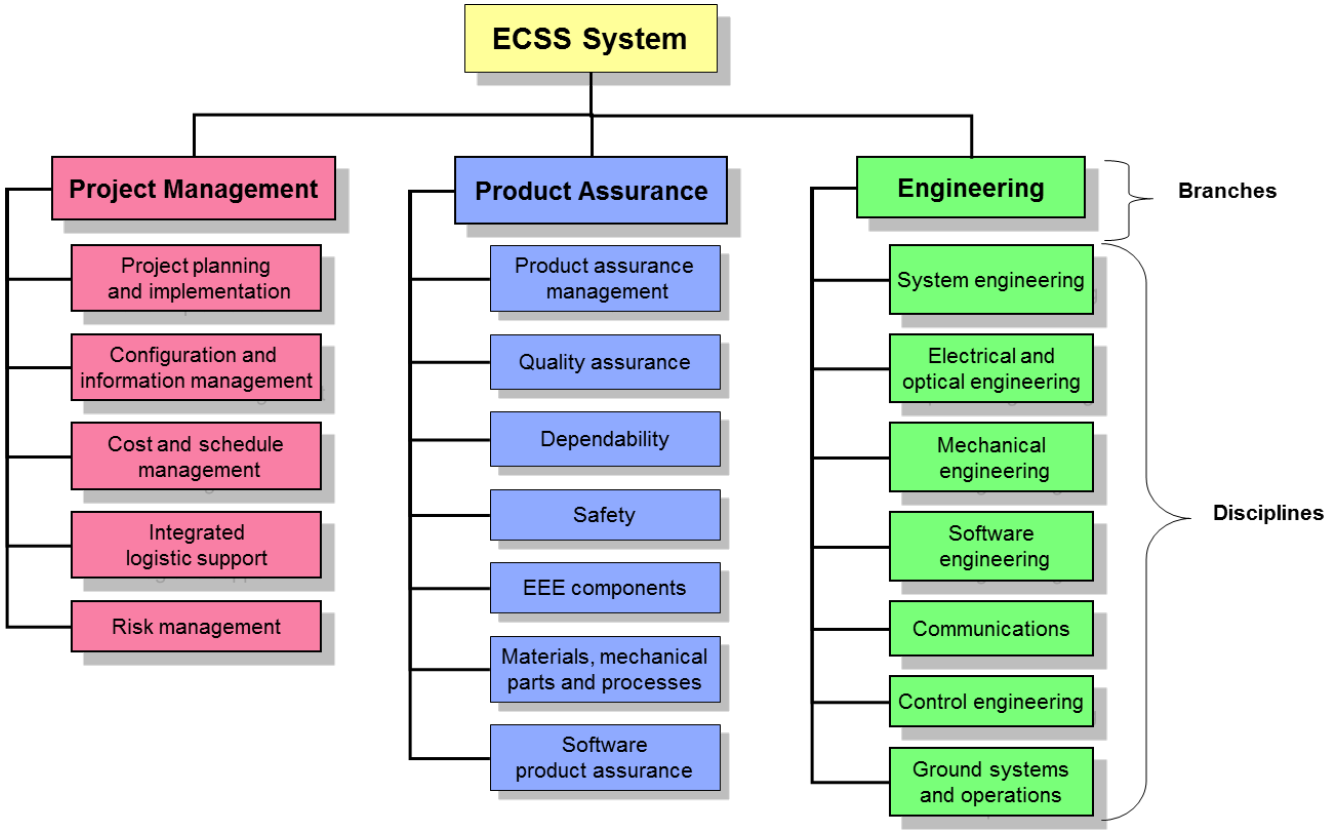
What does ECSS-E-TM-10-23A cover?

The formalization of the WHAT ! i.e. the means to *formally model* all System Requirements whether they are ECSS, Missions or Products related (i.e. supporting the ECSS tailoring concept).

The ECSS System

What is the ECSS System?

THE SPACE SYSTEM

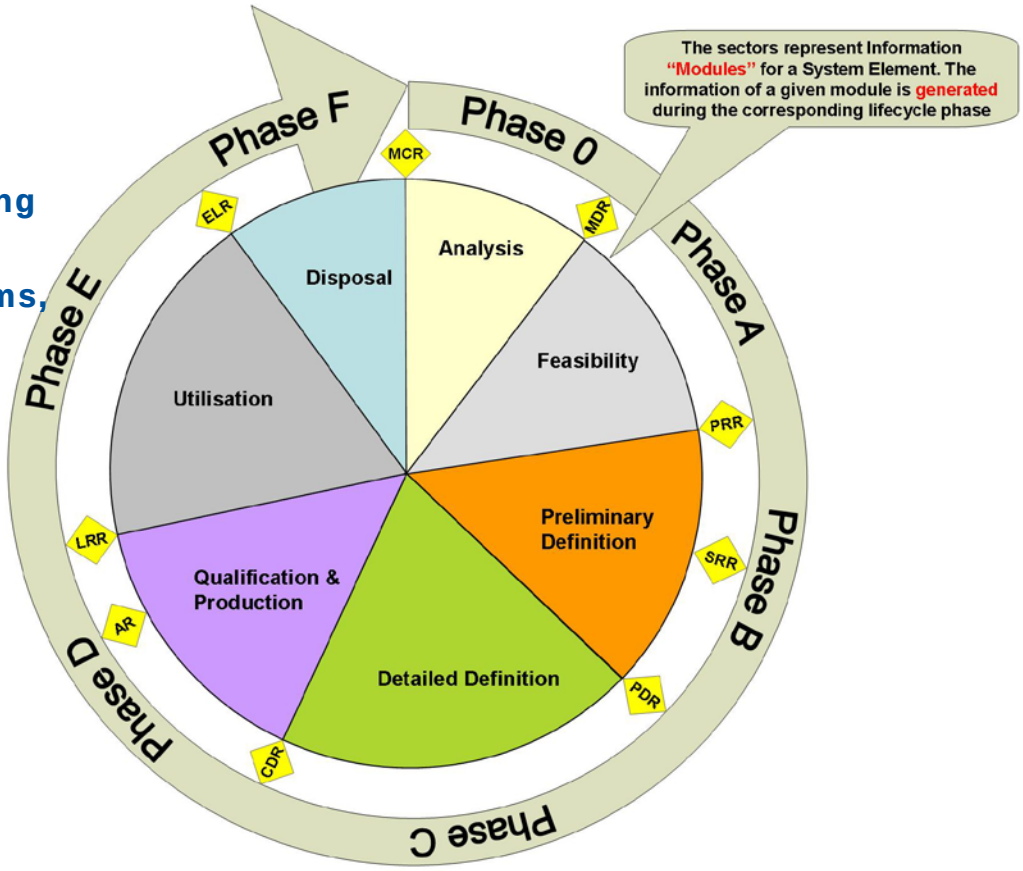


The ECSS-E-TM-10-23 drivers - 1

What does the ECSS-E-TM-10-23 address?

- **It addresses, at global conceptual level, the overall Space System lifecycle, including the life cycle of each of its composing system elements, i.e. segments, systems, subsystems, assemblies, etc.**
- **…**

THE SPACE SYSTEM MODEL

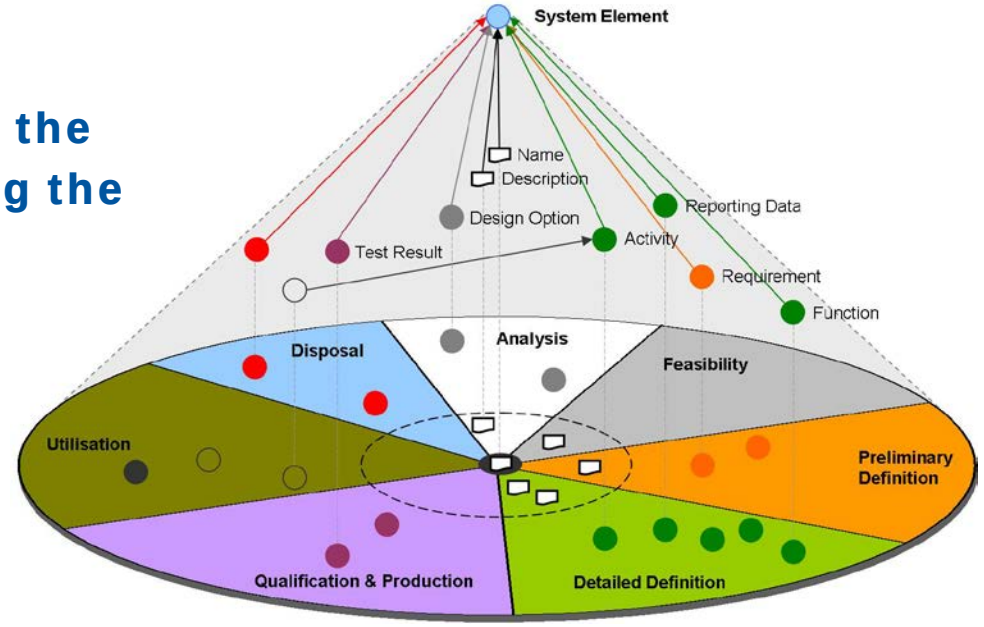


The ECSS-E-TM-10-23 drivers - 2

What does the ECSS-E-TM-10-23 propose?

- …
- It proposes to standardize the information model ensuring the overall consistency of the model through all phases
- …

THE SPACE SYSTEM MODEL

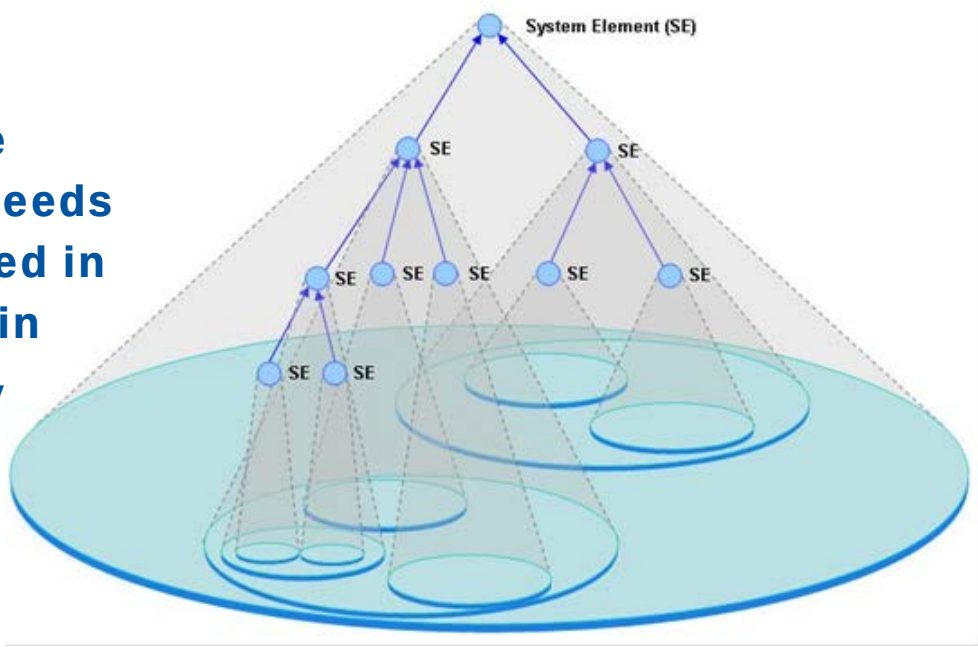


The ECSS-E-TM-10-23 drivers - 3

What does the ECSS-E-TM-10-23 scope?

- …
- It scopes (by tailoring) the information model to the needs of each stakeholder involved in the customer/supplier chain
- It ensures the integrability (by transfer or linking) of the information
- …

THE SPACE SYSTEM MODEL

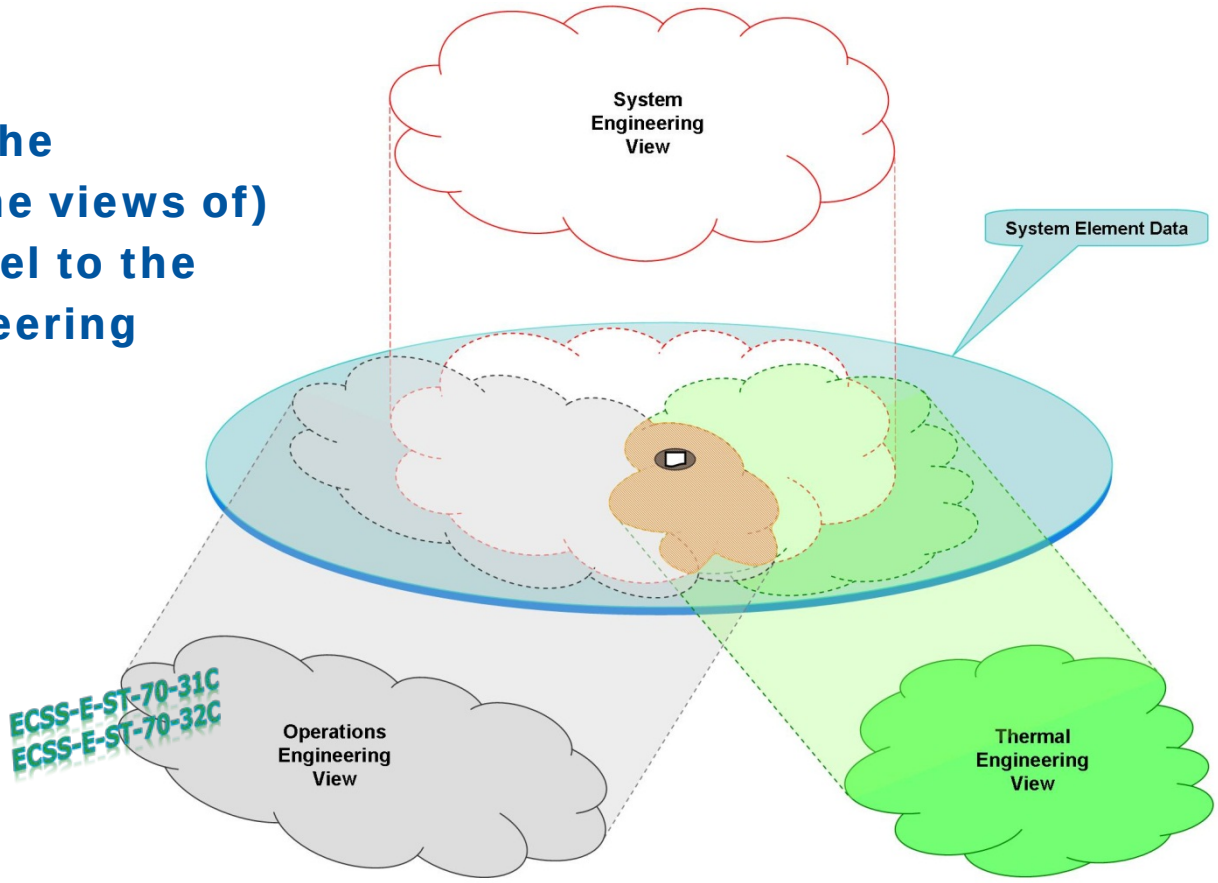


The ECSS-E-TM-10-23 drivers - 4

What does the ECSS-E-TM-10-23 scope?

- …
- It scopes (creating the engineering discipline views of) the information model to the needs of each engineering discipline
- …

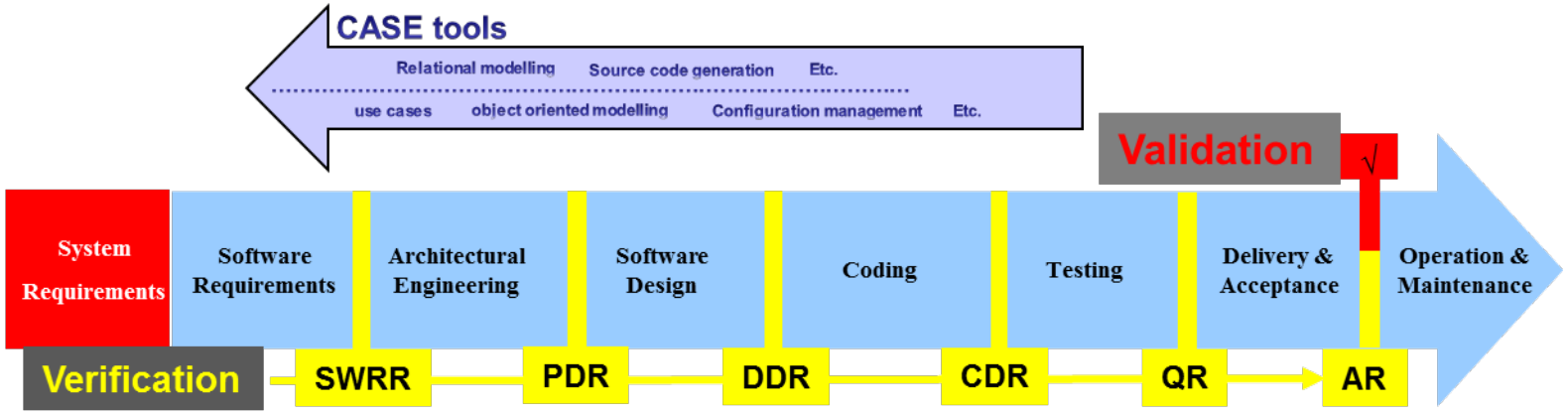
THE SPACE SYSTEM MODEL



How to formally model the WHAT, i.e. the System Requirements?

1. **The Backward approach:**

   Augment the capability of software development methodology and tools



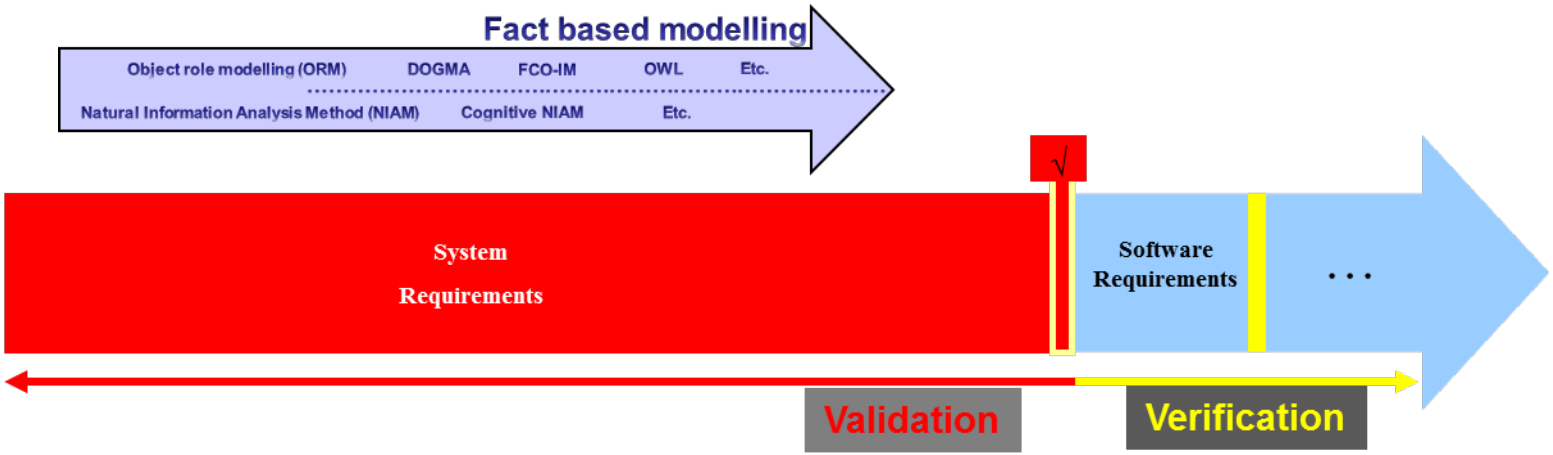
How to formally model the WHAT, i.e. the System Requirements?

1. ...
2. **The Onward approach:**

Apply formal logic and controlled natural language

How data is grouped into structures (e.g. attribute-based entity types, classes, XML schemas) is an implementation issue that is irrelevant to the capturing of business semantics.

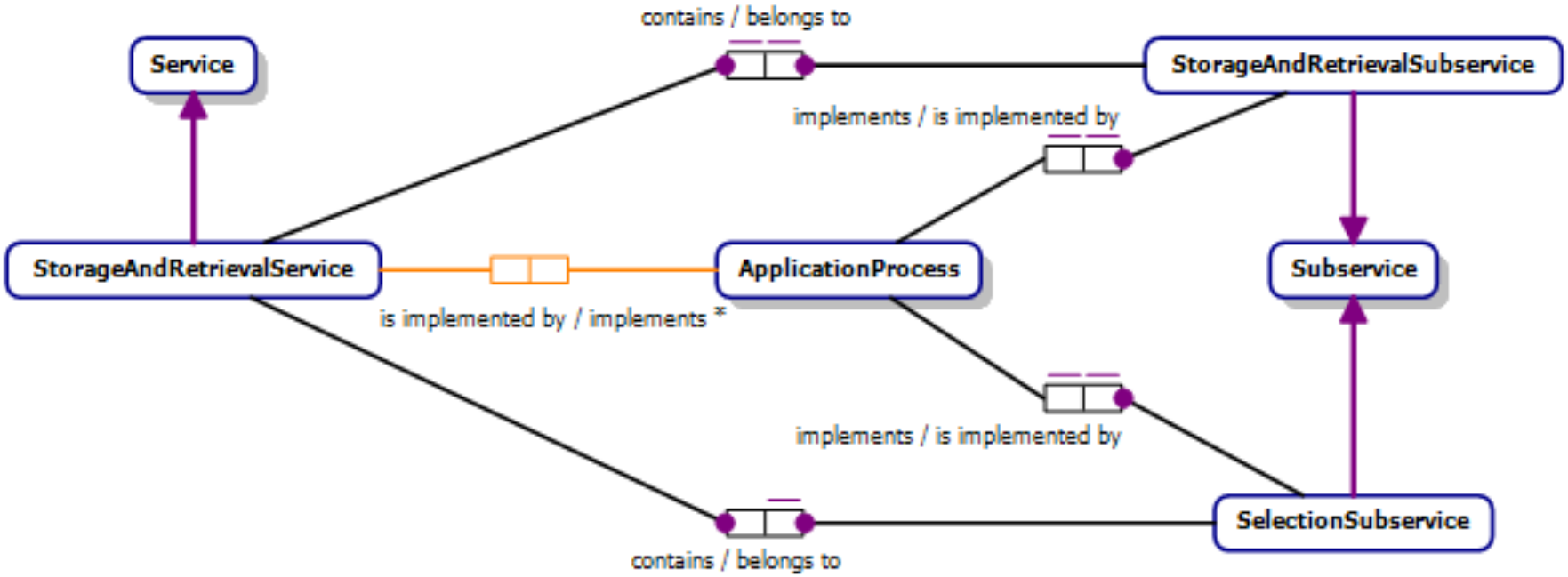
Avoiding the HOW enhances semantic stability, as well as facilitates natural verbalization and more productive communication with all stakeholders.



Conceptual Data Modelling using FBM - 1

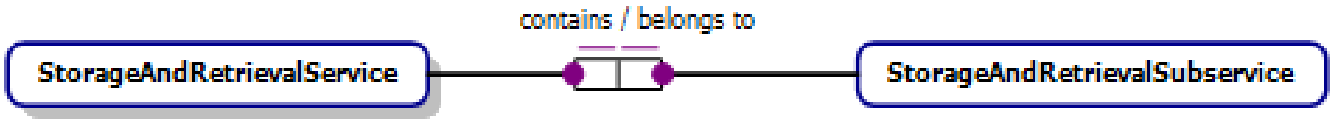
Applying formal logic and controlled natural language ***during the production of the emerging*** ***ECSS-E-ST-70-41C Telemetry and Telecommand Packet Utilization standard (PUS)***

some examples: **A Fact Based Modelling graphical representation of some PUS system requirements:**



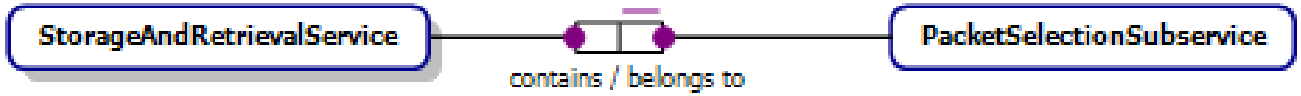
Conceptual Data Modelling using FBM - 2

and related *Controlled Natural Language* verbalization:



A. Storage and retrieval subservice belongs to storage and retrieval service

1. **Each** storage and retrieval subservice shall belong to **exactly one** storage and retrieval service.
2. **Each** storage and retrieval service shall contain **exactly one** storage and retrieval subservice.

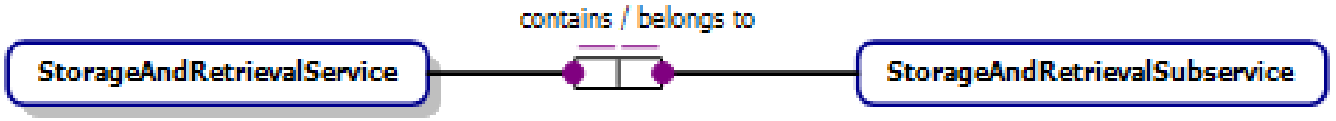


B. Packet selection subservice belongs to storage and retrieval service.

1. **Each** packet selection subservice shall belong to **exactly one** storage and retrieval service.
2. **Each** storage and retrieval service shall contain **one or more** packet selection subservice.

Conceptual Data Modelling using FBM - 3

Fully understanding requirements that have been positively expressed might be difficult



A. Storage and retrieval subservice belongs to storage and retrieval service

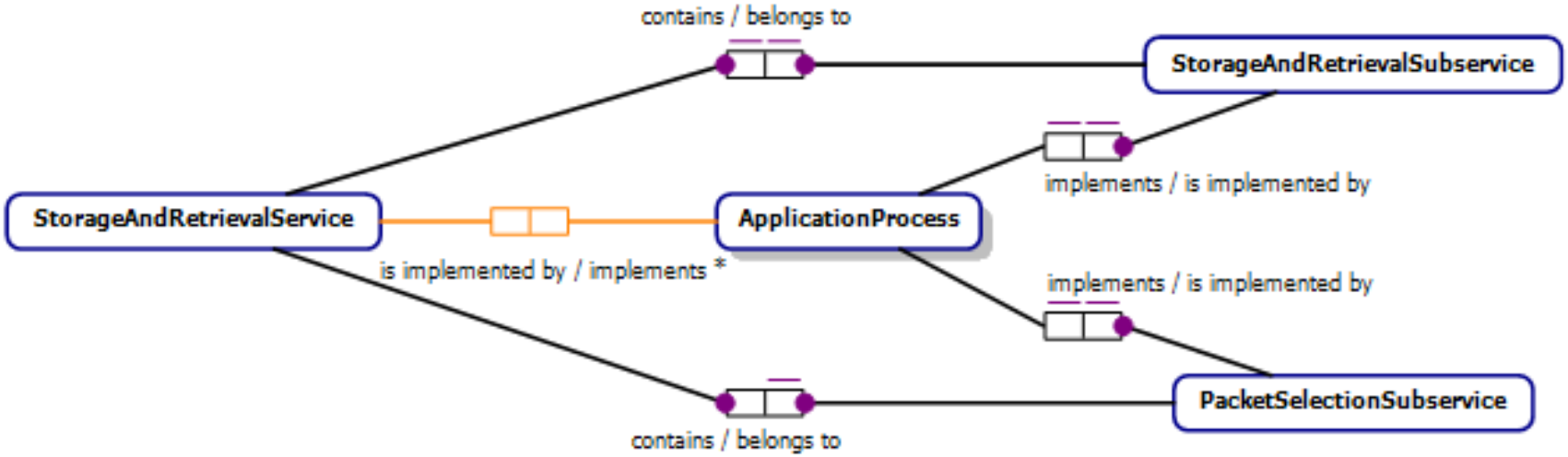
1. **Each** storage and retrieval subservice shall belong to **exactly one** storage and retrieval service.
2. **Each** storage and retrieval service shall contain **exactly one** storage and retrieval subservice.

Negative verbalization might help:

1. **It is impossible that some** storage and retrieval subservice belongs to **more than one** storage and retrieval service.
2. **It is impossible that some** storage and retrieval subservice belongs to **no** storage and retrieval service.
3. **It is impossible that some** storage and retrieval service contains **more than one** storage and retrieval subservice.
4. **It is impossible that some** storage and retrieval service contains **no** storage and retrieval subservice.

Conceptual Data Modelling using FBM - 4

Formally deriving information from *asserted and/or derived* information provides means to enhance the System Specification.



A. * Storage and retrieval service is implemented by application process

if and only if

that storage and retrieval service contains **some** storage and retrieval subservice **that** is implemented by **that** application process

or **that** storage and retrieval service contains **some** packet selection subservice **that** is implemented by **that** application process

Conceptual Data Modelling using FBM - 5

Another example: The PUS packet field Parameter Codes

***PC** represents Booleans **if and only if**
that PC has **some** PTC **where the possible value of that** PTC **is** 1
and has **some** PFC **where the possible value of that** PFC **is** 0.

***PC** represents enumerations **if and only if**
that PC has **some** PTC **where the possible value of that** PTC **is** 2
and has **some** PFC **where the possible values of that** PFC **are at least** 1 **to at most** 16, 24, 32.

***PC** represents ...

Exclusion constraint (derived):
*** For each** PC, **at most one of the following holds:**
that PC represents Booleans;
that PC represents enumerations;
that PC represents unsigned integers;
that PC represents signed integers;
that PC represents reals;
that PC represents bit-strings;
that PC represents octet-strings;
that PC represents character-strings;
that PC represents absolute times;
that PC represents relative times;
that PC represents deduced pc.

Mandatory constraint (asserted):
Each PC represents Booleans
or represents enumerations
or represents unsigned integers
or represents signed integers
or represents reals
or represents bit-strings
or represents octet-strings
or represents character-strings
or represents absolute times
or represents relative times
or represents deduced pc.

Conceptual Data Modelling using FBM - 6

Modelling information using FBM includes:

- Elementary fact type of any arity
- Objectification
- Constraints, including:
  - uniqueness,
  - mandatory,
  - inclusive-or,
  - exclusive-or,
  - value,
  - value comparison,
  - exclusion,
  - subset,
  - equality,
  - subtyping,
  - cardinality
  - ring constraints including e.g. reflexive, irreflexive, symmetric, asymmetric, antisymmetric, transitive, intransitive, acyclic
- Predicate, predicate reading
- Assertion, derivation, semi-derivation
- Alethic, deontic modality
- ...

Applying E-TM-10-23 in ECSS…

Applying ECSS-E-TM-10-23 to produce ECSS

- **2008**
  - **ECSS-E-ST-70-31C Monitoring and Control data definition**
  - **ECSS-E-ST-70-32C Test and operations procedure language**

- **2013, …**
  - **ECSS-E-ST-70-41C Telemetry and telecommand packet utilization**
  - ***ECSS-E-ST-70-11D Spacecraft operability***
  - ***ECSS-E-ST-70-31D Monitoring and control data definition***
  - ***ECSS-E-ST-70-32D Test and operations procedure language***
  - ***…***

to conclude…

Toward semantic interoperability - 1

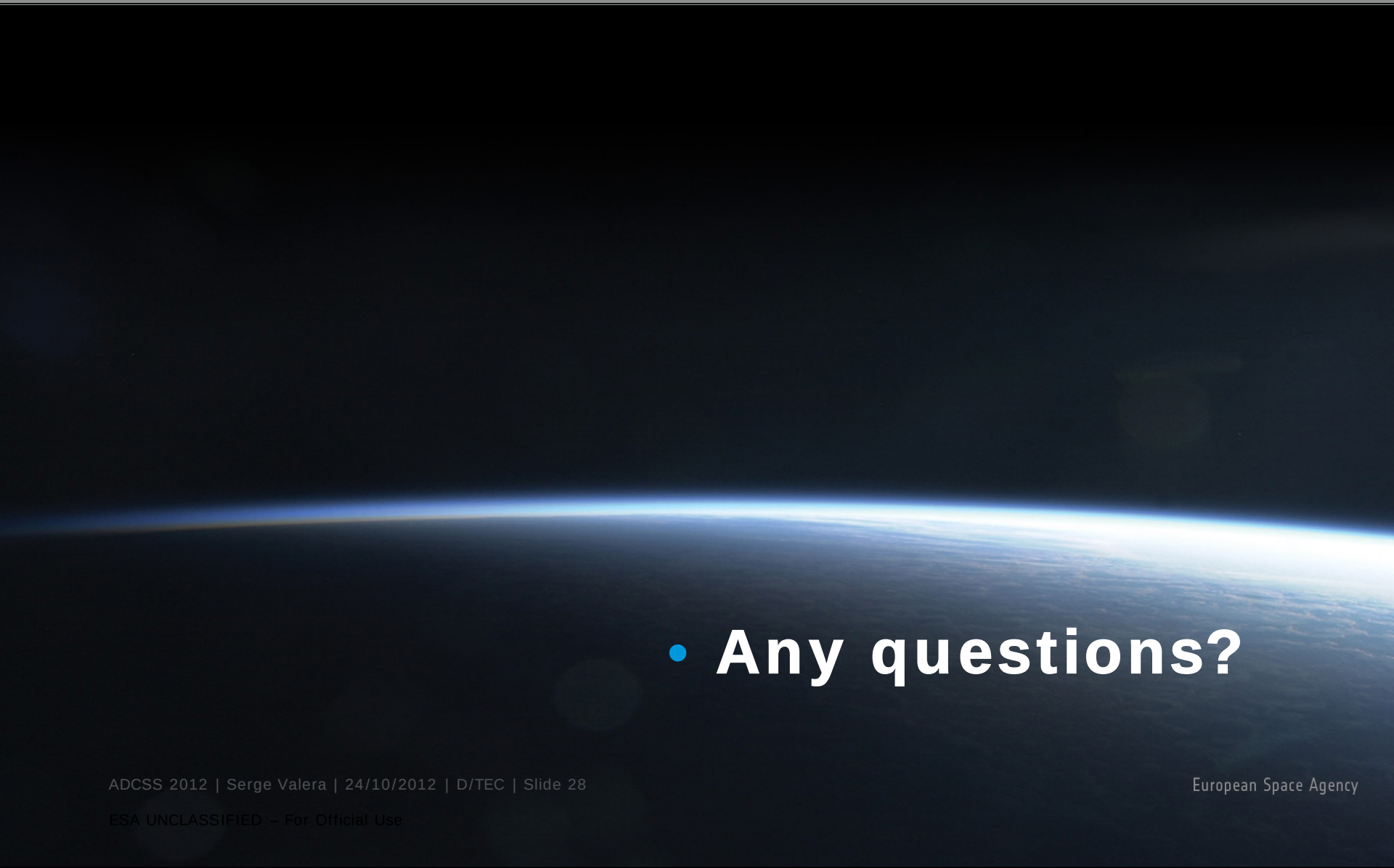
Do not make any assumption !

Any assumption by definition "not validated" has a recovery cost that might increase "exponentially" with the time taken to acknowledge that it was a wrong assumption.

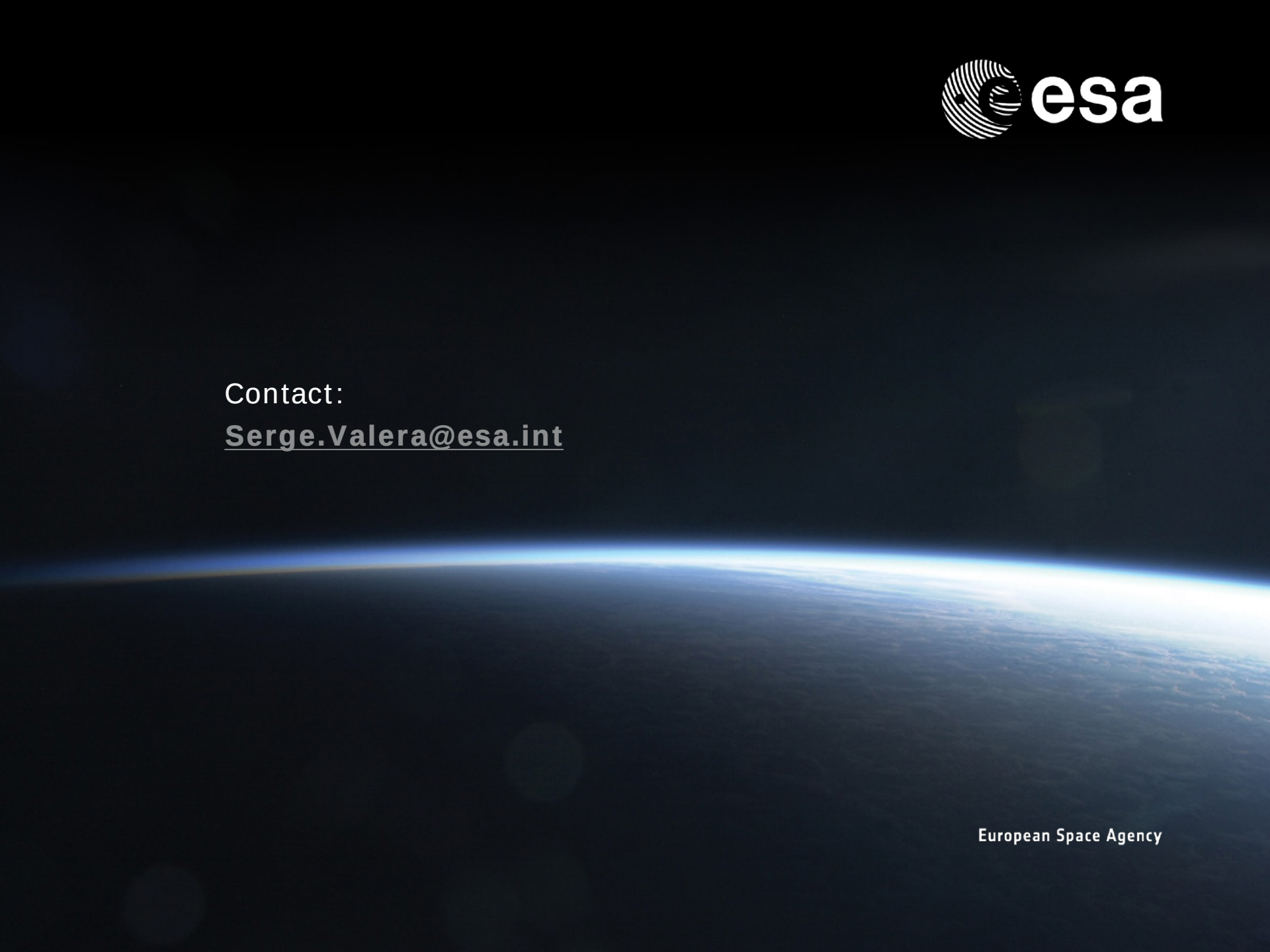
Toward semantic interoperability - 2

Remain in the System Specification phase as long as required to:

1. **Fully identify and specify all stakeholder needs (including external stakeholders);**
2. **Fully conceptual model that specification ensuring:**
    a) **the explicit definition of each concept that may be misinterpreted (terms & definitions);**
    b) **the elementarity (atomicity) of each requirement;**
    c) **the overall consistency of the specification;**
    d) **that all examples (positive and negative) required to verify the adequacy of all validation rules, to permit unit testing are available.**
3. **Fully validate with the stakeholders the *formally-expressed* specification.**



- **Any questions?**



Contact:
Serge.Valera@esa.int

European Space Agency