Avionics Data, Control and Software Systems
ADCSS-2014

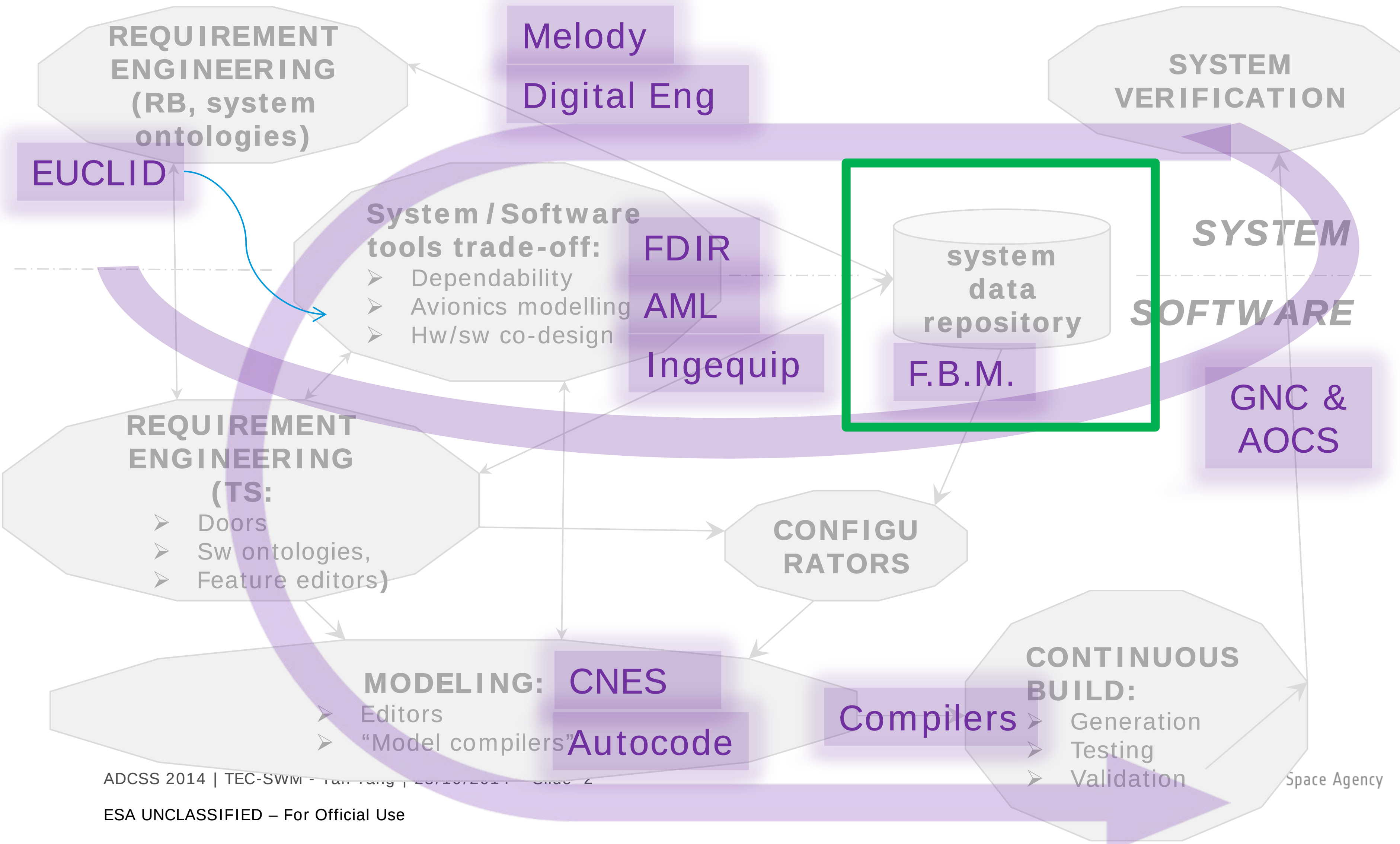
ECSS-E-TM-10-23 Space System Data Repository

using a formal requirement engineering approach

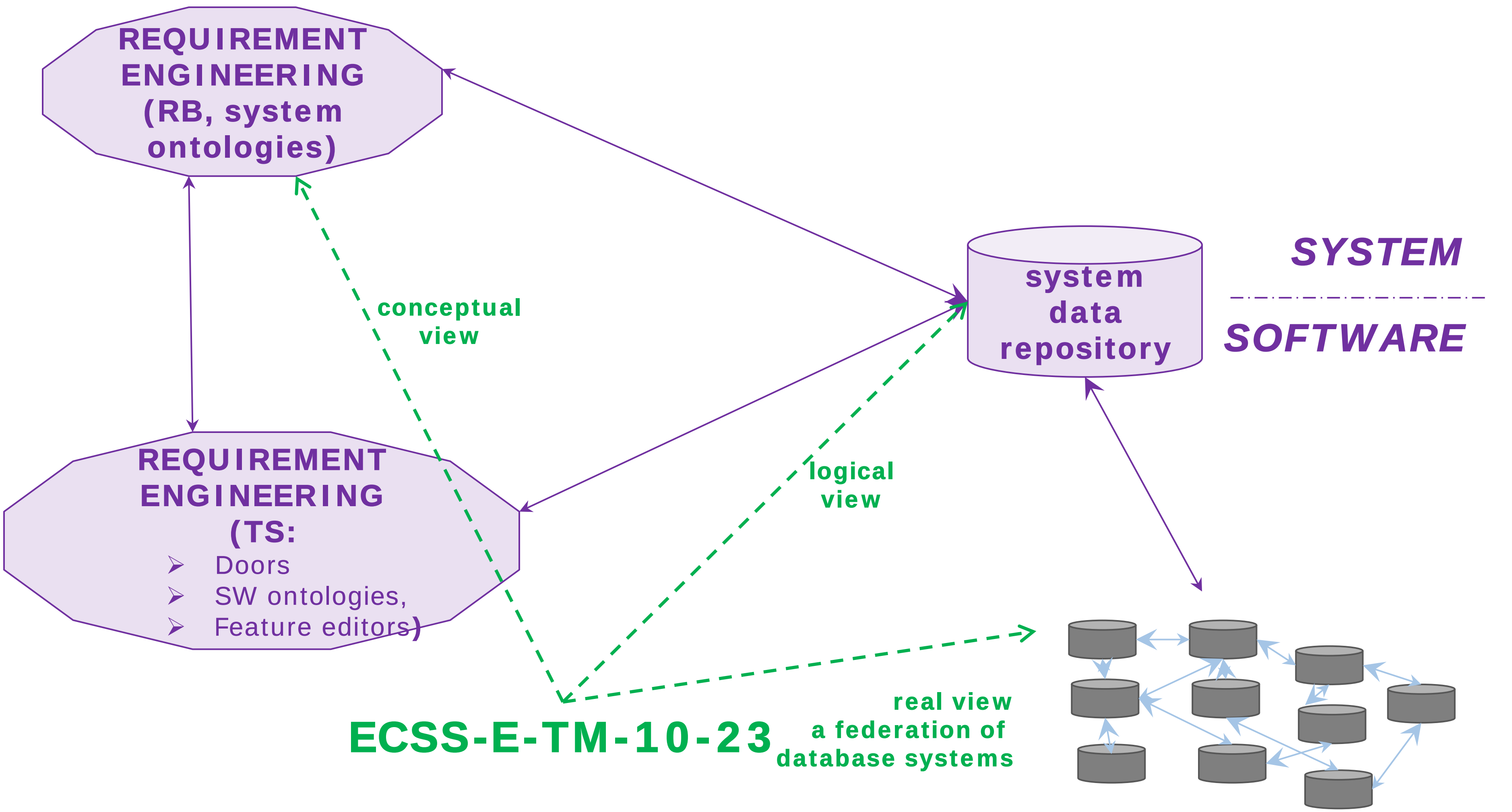
Dr Yan Tang and Mr. Serge Valera

ESTEC/TEC-SWM
28/10/2014

The presentation



System - Software relationship



ECSS-E-TM-10-23A

1. ECSS-E-TM-10-23 addresses means to enable **semantic interoperability** for the purpose of enhancing the way space systems are currently developed and operated, including:
    a. *reducing the risk* inherent to complex systems,
    b. *reducing the overall cost.*
2. ECSS-TM-10-23 promotes the idea of **conceptual modelling** at the GLOBAL level to allow sharing and reuse of *any* space system knowledge between *all involved* partners

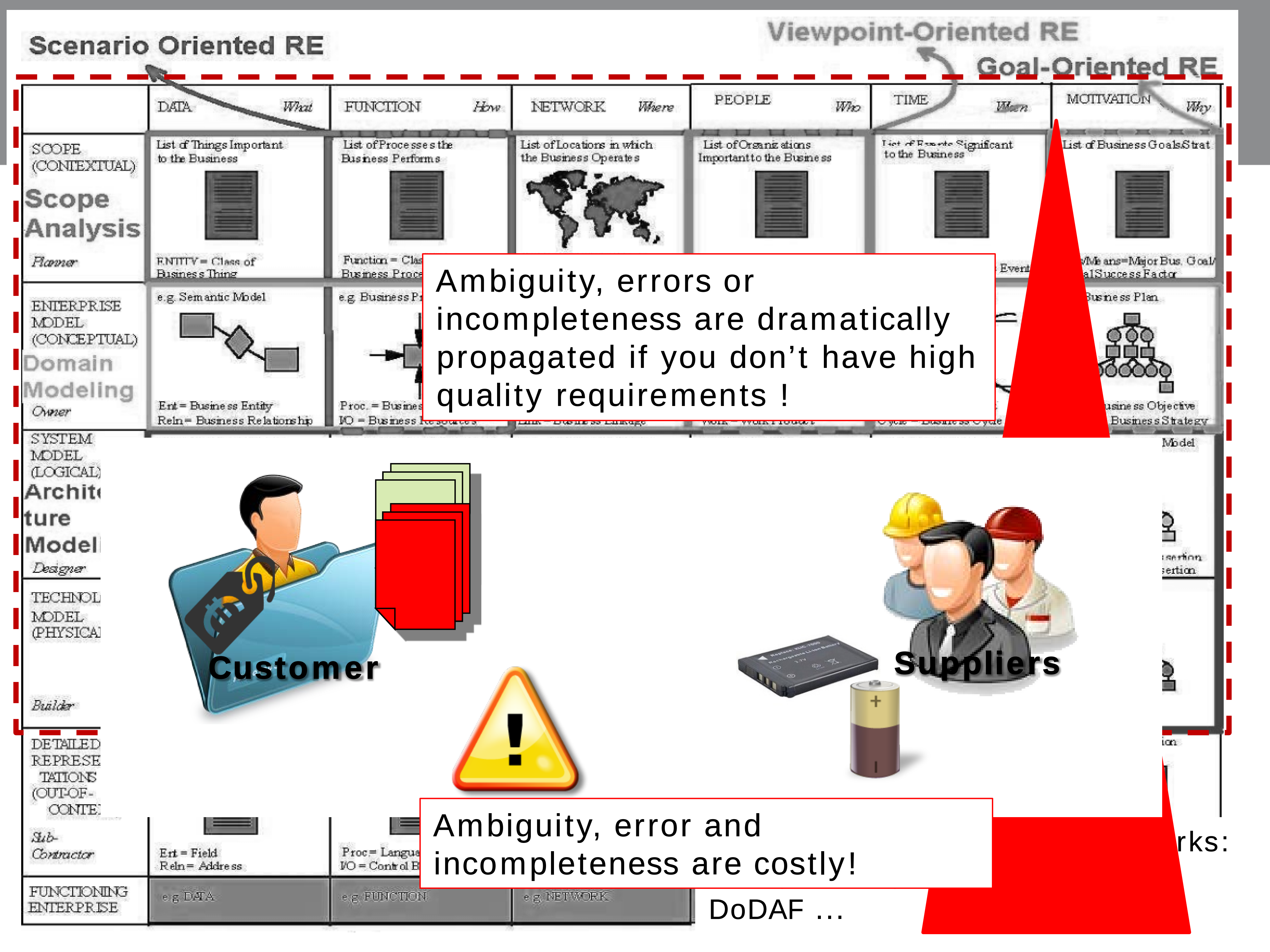
- **Conceptual modelling** is for Requirement Engineering
- **Conceptual modelling**
    - enhances the **quality** of any requirements specifications
    - enables the **validation** of system requirements by their stakeholders *before* any *development*

Requirement Engineering (RE)

1. Requirements must be **complete**, **consistent** & correspond to the intended **need**
2. System requirements (the Customers' requirements) addresses the **WHAT** and should be free of any implementation issues *System requirements shall remain at conceptual level*

Conceptual modeling

- Conceptual modeling is activities of *formally describing* aspects of physical and abstract world for the purpose of human understanding and communication (Mylopoulos, 1992)
- Conceptual models facilitate tasks such as the elicitation, documentation, validation and verification of requirements, which permits to detect and correct possible errors, and, to have stakeholders' requirements as complete as possible at an early stage *prior to implementation* (Pohl, 1997; Wand and Weber, 2002)
- Conceptual modeling is a solution of enhancing *interoperability* (IEEE, 1990)


Scenario Oriented RE
Viewpoint-Oriented RE
Goal-Oriented RE
DATA What
FUNCTION How
NETWORK Where
PEOPLE Who
TIME When
MOTIVATION Why
SCOPE (CONTEXTUAL)
Scope Analysis
Planner
List of Things Important to the Business
ENTITY = Class of Business Thing
List of Processes the Business Performs
List of Locations in which the Business Operates
List of Organizations Important to the Business
List of Business Goals/Strat
ENTERPRISE MODEL (CONCEPTUAL)
Domain Modeling
Owner
e.g. Semantic Model
Ent = Business Entity
Reln = Business Relationship
Business Plan
SYSTEM MODEL (LOGICAL)
Architecture Model
Designer
TECHNOL MODEL (PHYSICA
Builder
DETAILED REPRESENTATIONS (OUT-OF-CONTEXT)
Sub-Contractor
Ent = Field
Reln = Address
FUNCTIONING ENTERPRISE
e.g. DATA
e.g. FUNCTION
e.g. NETWORK
Ambiguity, errors or incompleteness are dramatically propagated if you don’t have high quality requirements !
Customer
Suppliers
Ambiguity, error and incompleteness are costly!
rks:
DoDAF …

Formal conceptual modelling in

REQUIREMENT ENGINEERING

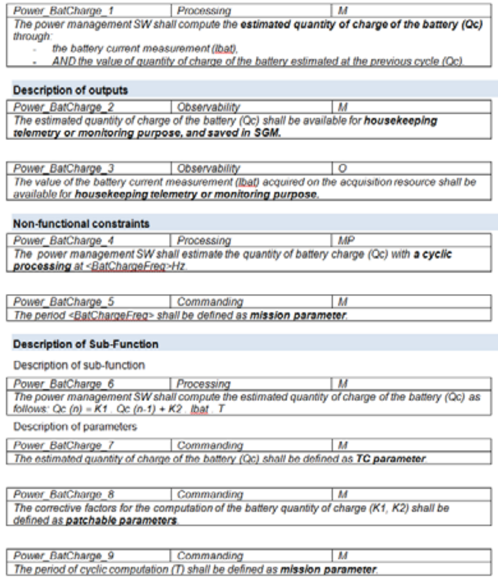
It begins with a need…

Ask stakeholders to express a few req. in whatever format

e.g. requirements for power management software

Modeler

Stakeholder



Power_BatCharge_1	*Processing*	*M*

The power management SW shall compute the ***estimated quantity of charge of the battery (Qc)*** *through:*
- *the battery current measurement (Ibat),*
- *AND the value of quantity of charge of the battery estimated at the previous cycle (Qc).*

Description of outputs

Power_BatCharge_2	*Observability*	*M*

The estimated quantity of charge of the battery (Qc) shall be available for ***housekeeping telemetry or monitoring purpose, and saved in SGM.***

Power_BatCharge_3	*Observability*	*O*

The value of the battery current measurement (Ibat) acquired on the acquisition resource shall be available for ***housekeeping telemetry or monitoring purpose.***

Non-functional constraints

Power_BatCharge_4	*Processing*	*MP*

The power management SW shall estimate the quantity of battery charge (Qc) with ***a cyclic processing*** *at <BatChargeFreq>Hz.*

Power_BatCharge_5	*Commanding*	*M*

The period <BatChargeFreq> shall be defined as ***mission parameter.***

Description of Sub-Function

Description of sub-function

Power_BatCharge_6	*Processing*	*M*

The power management SW shall compute the estimated quantity of charge of the battery (Qc) as follows: Qc (n) = K1 . Qc (n-1) + K2 . Ibat . T

Description of parameters

Power_BatCharge_7	*Commanding*	*M*

The estimated quantity of charge of the battery (Qc) shall be defined as ***TC parameter.***

Power_BatCharge_8	*Commanding*	*M*

The corrective factors for the computation of the battery quantity of charge (K1, K2) shall be defined as ***patchable parameters.***

Power_BatCharge_9	*Commanding*	*M*

The period of cyclic computation (T) shall be defined as ***mission parameter.***

scoping

How to elicit implicit knowledge from stakeholders?

Ask stakeholders to express a few req. in whatever format → Ask competency questions ⇄ Segmentation and highlighting

Power_BatCharge_1	*Processing*	*M*
*The power management SW shall compute the **estimated quantity of charge of the battery (Qc)** through: - the battery current measurement (Ibat), - AND the value of quantity of charge of the battery estimated at the previous cycle (Qc).*		

Description of outputs

Power_BatCharge_2	*Observability*	*M*
*The estimated quantity of charge of the battery (Qc) shall be available for **housekeeping telemetry or monitoring purpose, and saved in SGM.***		

Power_BatCharge_3	*Observability*	*O*
*The value of the battery current measurement (Ibat) acquired on the acquisition resource shall be available for **housekeeping telemetry or monitoring purpose.***		

Non-functional constraints

Power_BatCharge_4	*Processing*	*MP*
*The power management SW shall estimate the quantity of battery charge (Qc) with **a cyclic processing** at <BatChargeFreq>Hz.*		

Power_BatCharge_5	*Commanding*	*M*
*The period <BatChargeFreq> shall be defined as **mission parameter**.*		

Description of Sub-Function

Description of sub-function

Power_BatCharge_6	*Processing*	*M*
The power management SW shall compute the estimated quantity of charge of the battery (Qc) as follows: Qc (n) = K1 . Qc (n-1) + K2 . Ibat . T		

Description of parameters

Power_BatCharge_7	*Commanding*	*M*
*The estimated quantity of charge of the battery (Qc) shall be defined as **TC parameter**.*		

Power_BatCharge_8	*Commanding*	*M*
*The corrective factors for the computation of the battery quantity of charge (K1, K2) shall be defined as **patchable parameters**.*		

Power_BatCharge_9	*Commanding*	*M*
*The period of cyclic computation (T) shall be defined as **mission parameter**.*		

Competency question is a query (posed by a modeler and answered by the stakeholder(s)) in a natural language to determine scopes, extract main concepts, relations or rules. (Wand and Weber, 2002; Uschold and Grüninger, 1996)

Power_BatCharge_1	*Processing*	*M*
*The power management SW shall compute the **estimated quantity of charge of the battery (Qc)** through: - the battery current measurement (Ibat), - AND the value of quantity of charge of the battery estimated at the previous cycle (Qc).*		

segmentation

highlighting

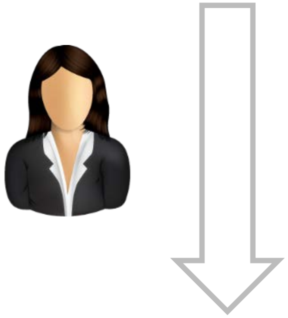
The power management SW shall compute the estimated quantity of charge of the battery (Qc)

- Nouns and nouns with prepositions
- Verbs and prepositions
- words containing constraint information
- Adjunctive

How to elicit implicit knowledge from stakeholders?

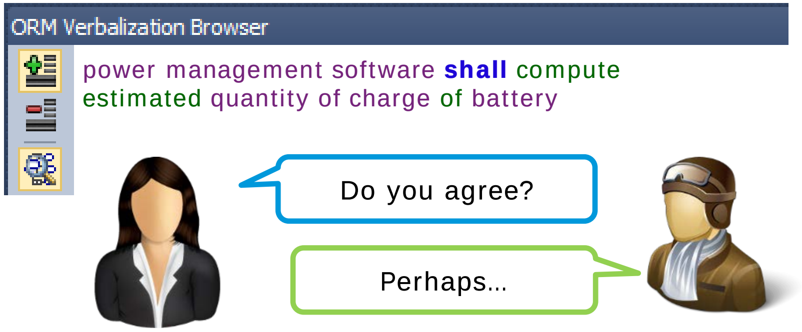
Ask stakeholders to express a few req. in whatever format → Ask competency questions ⇄ Segmentation and highlighting → Build concepts and relations | Ask comp. que

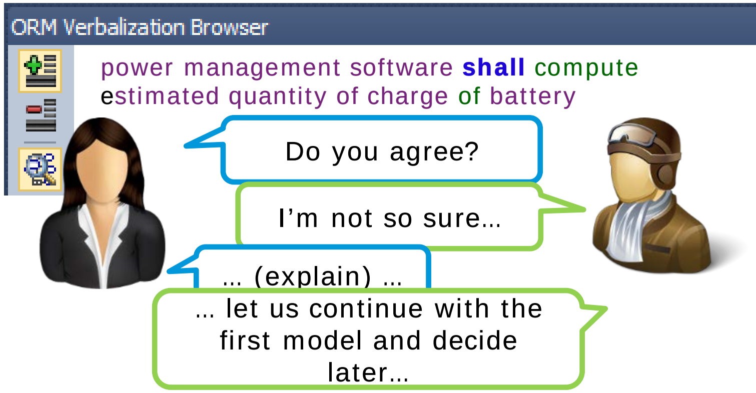
The power management SW shall compute the estimated quantity of charge of the battery (Qc)



- Nouns (sometimes with prepositions) are used to model **concepts**
- Common verbs and prepositions are used to model **relations**
- Adjunctive is used to model either **subtypes** or **relations**

Or





How to elicit implicit knowledge from stakeholders?

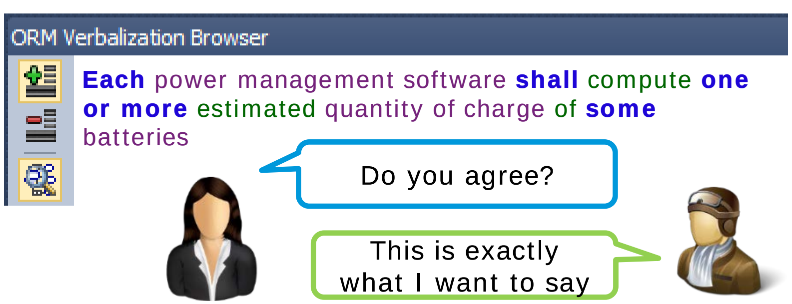
Ask stakeholders to express a few req. in whatever format → Ask competency questions ⇄ Segmentation and highlighting → Build concepts and relations / Specify constraints → Ask comp. questions

The power management SW shall compute the estimated quantity of charge of the battery (Qc)

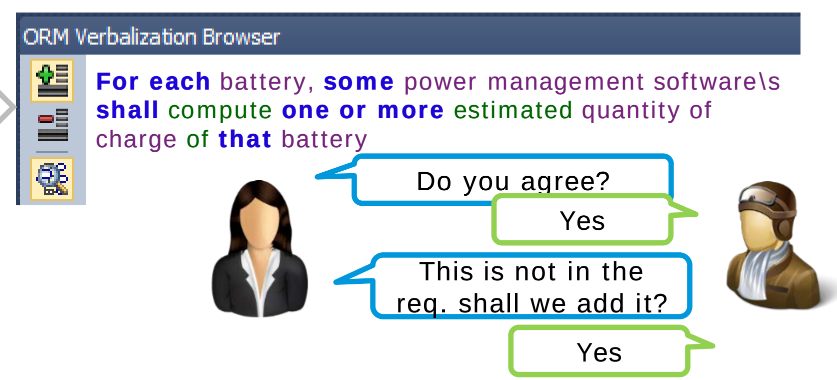
words containing constraint information are used to model **constraints**

Specific verbs and prepositions can be used to model **implied relations**

Mandatory constraint



Process is omitted here



How to elicit implicit knowledge from stakeholders?

Ask stakeholders to express a few req. in whatever format → Ask competency questions ⇄ Segmentation and highlighting → Build concepts and relations / Specify constraints → Ask comp. questions

Uniqueness constraint

ORM Verbalization Browser

For each power management software **and** estimated quantity of charge, **that** power management software **shall** compute **that** estimated quantity of charge of **at most one (zero or one)** battery

Or

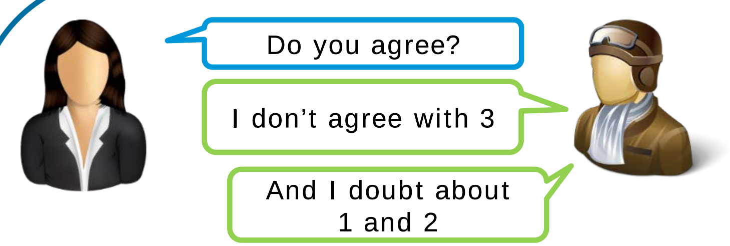
ORM Verbalization Browser

For each estimated quantity of charge **and** battery, **at most one (zero or one)** power management software **shall** compute **that** estimated quantity of charge of **that** battery

Or

ORM Verbalization Browser

For each power management software **and** battery, **that** power management software **shall** compute **at most one (zero or one)** estimated quantity of charge of **that** battery



PMSW	Qc	Battery	
Pmsw1	9AH	Bat11_6OnSONY18650HC	
pmsw1	9AH	**Bat11_6_OnSAFTVES140**	OK
pmsw1	**15AH**	Bat11_6OnSONY18650HC	OK
pmsw2	9AH	Bat11_6OnSONY18650HC	NO

How to elicit implicit knowledge from stakeholders?

Ask stakeholders to express a few req. in whatever format → Ask competency questions ⇄ Segmentation and highlighting → Build concepts and relations

Specify constraints

Ask comp. questions

The power management SW shall compute the estimated quantity of charge of the battery (Qc)

Cardinality constraint

Do you have only one PMSW?

Yes

ORM Verbalization Browser

There shall be one and only one power management software **in the Universe of Discourse**

Ok

Scenario 1

Do you have only one PMSW?

No

The Cardinality constraint is then inapplicable

Scenario 2

Result of modeling

Power_BatCharge_1	*Processing*	*M*
The power management SW shall compute the ***estimated quantity of charge of the battery (Qc)*** *through:* - *the battery current measurement (Ibat),* - *AND the value of quantity of charge of the battery estimated at the previous cycle (Qc).*		

- **Each** power management software **shall** compute **one or more** estimated quantity of charge of **some** batteries
- **For each** battery, **exactly one** power management software **shall** compute **one or more** estimated quantity of charge of **that** battery
- **Each** estimated quantity of charge of **some** batteries **shall be** computed by **one or more** power management software's
- **For each** estimated quantity of charge **and** battery**, exactly one** power management software **shall** compute **that** estimated quantity of charge of **that** battery
- **Each** battery **shall** have **one or more** estimated quantity of charge
- **Each** estimated quantity of charge **shall** be of **exactly one** battery
- Power management software **shall be involved in** computation of estimated quantity of charge
- Quantity of charge **shall be involved in** computation of estimated quantity of charge.
- Battery **shall be involved in** computation of estimated quantity of charge
- **Each** computation of estimated quantity of charge **shall** use **exactly one** battery current measurements and estimated quantity of charge of **exactly one** previous cycle
- **For each** computation of estimated quantity of charge **and** previous cycle, **that** computation of estimated quantity of charge **shall** use **exactly one** battery current measurement **and exactly one** estimated quantity of charge of **that** previous cycle
- **For each** battery current measurement **and** previous cycle, **exactly one** computation of estimated quantity of charge **shall** use **that** battery current measurement **and** estimated quantity of charge of **that** previous cycle
- **For each** computation of estimated quantity of charge **and** battery current measurement, **that** computation of estimated quantity of charge **shall** use **that** battery current measurement **and** estimated quantity of charge of **zero or one** previous cycle
- **Each** computation of estimated quantity of charge **shall** be in **exactly one** cycle
- **Each** battery **shall** have **one or more** battery current measurement
- **Each** battery current measurement **shall** be of **exactly one** battery

1 ***informally expressed*** **requirement → 16 requirements !**

Result of modeling

Power_BatCharge_1	Processing	M
The power management SW shall compute the **estimated quantity of charge of the battery (Qc)** through: - the battery current measurement (Ibat), - AND the value of quantity of charge of the battery estimated at the previous cycle (Qc).		

Description of outputs

Power_BatCharge_2	Observability	M
The estimated quantity of charge of the battery (Qc) shall be available for **housekeeping telemetry or monitoring purpose, and saved in SGM.**		

Power_BatCharge_3	Observability	O
The value of the battery current measurement (Ibat) acquired on the acquisition resource shall be available for **housekeeping telemetry or monitoring purpose.**		

Non-functional constraints

Power_BatCharge_4	Processing	MP
The power management SW shall estimate the quantity of battery charge (Qc) with **a cyclic processing** at <BatChargeFreq>Hz.		

Power_BatCharge_5	Commanding	M
The period <BatChargeFreq> shall be defined as **mission parameter**.		

Description of Sub-Function

Description of sub-function

Power_BatCharge_6	Processing	M
The power management SW shall compute the estimated quantity of charge of the battery (Qc) as follows: Qc (n) = K1 . Qc (n-1) + K2 . Ibat . T		

Description of parameters

Power_BatCharge_7	Commanding	M
The estimated quantity of charge of the battery (Qc) shall be defined as **TC parameter**.		

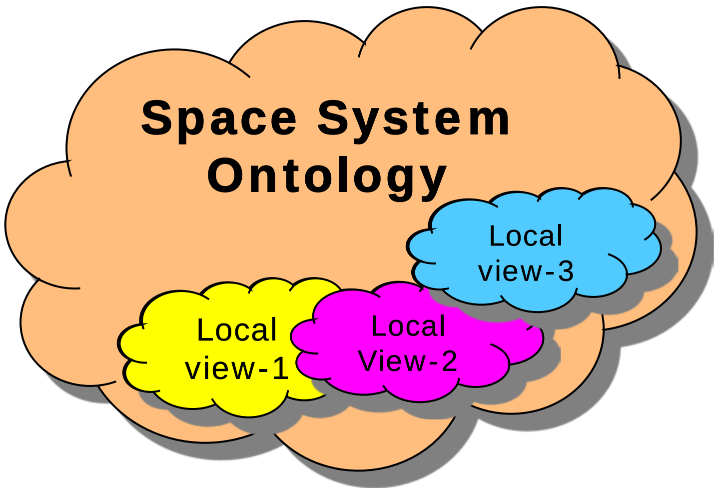
Power_BatCharge_8	Commanding	M
The corrective factors for the computation of the battery quantity of charge (K1, K2) shall be defined as **patchable parameters**.		

Power_BatCharge_9	Commanding	M
The period of cyclic computation (T) shall be defined as **mission parameter**.		

9 ***informally expressed*** **requirements**

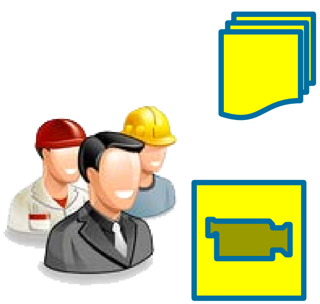
Error	Ambiguous items	Missing relations	Missing constraints	Missing requirements
1 major, 3 minor	1 relations 2+ object types	9	23	to further discuss with the stakeholders

The Space System Global Conceptual Model

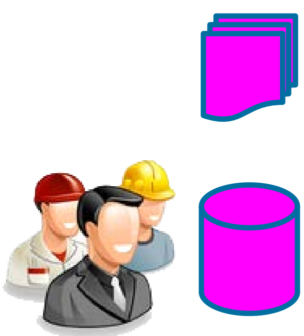


- Space system development partners differ from project to project
- Partners are geographically dispersed
- Different partners participate at different points in time in the project schedule

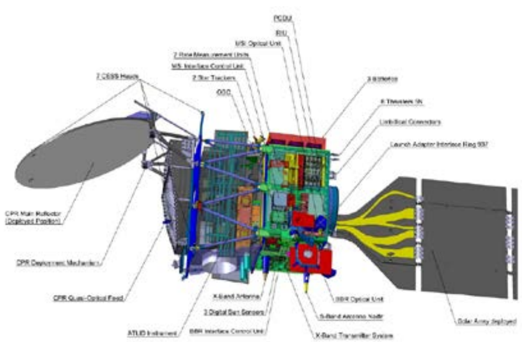
Components manufactures



Software development companies



DB system development companies



- Fact Based Modeling (FBM) standardization Working Group

  http://www.factbasedmodeling.org

Working draft 8 available, including:

a. Elementary fact type of any arity
b. Objectification
c. 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
d. Predicate, predicate reading
e. Assertion, derivation, semi-derivation
f. Alethic, deontic modality
g. Etc.

ESA – FAMOUS, 1

- FAMOUS - ESA/ESTEC contract no. 4000107725/12/NL

  Fact based Modeling Unifying System

  Towards implementing solutions for ECSS-E-TM-10-23A

  – grounded on solid foundations → *logic based*
  – understandable and able to be validated by stakeholders → *controlled natural language*
  – meets the stakeholders' needs of requirement's expressiveness → towards ISO TR9007 100% principle
  – fulfils the quality required for a customer's requirements specification → unambiguity, elementary, testability, consistency, completeness, verifiable, feasibility, traceability, ...
  – aligned to customers' needs, covers the requirement engineering cycle → including from tacit to explicit knowledge modelling

ESA – FAMOUS, 2

1. FBM standard (working draft 8) with extensions:
   a. support for multi models
   b. derivation language
   c. dynamic constraints time and event based
   d. QUDV $_{\text{Quantities, Units, Dimensions and values}}$ compliance
2. Customers' needs – ***specification***
   a. a generic modelling architecture
      → modelling: a term used by everyone with different meanings
      → visualization: a 3-level triangle-based architecture (data, schema, meta-schema)
   b. a conceptual modelling protocol
      → from nothing to a conceptual model
      → to formally specify the *to-be-contracted* system specification, focusing on the real needs, i.e. the WHAT, no over-specification/no HOW
      → conceptual hierarchies (root $_{\text{natural/promoted}}$ concepts, existential dependent fact types/object types, leading roles, assembly concepts, …), customer/supplier root concepts' interactions, root concept's life cycle,

ESA – FAMOUS, 3

3. Supplier's needs - ***realization***
   a. *Engineering:* automatic transformation from conceptual models to Logical & Physical models
   b. *Reverse engineering:* semi-automatic transformation from databases to conceptual models
   c. FBM formalization of logical and physical including:
      – Logical modelling including Relational SQL2011, UML, hierarchies
      – Physical modelling including Oracle SQL, XMI, XSD
4. Semantic interoperability:
   a. Global and locals modelling

THANK YOU!

References

1. The FBM working group, FBM working draft (WD8), 2014 (contact serge.valera@esa.int for the draft)
2. Wand, Y., and Weber, R. 2002. Research Commentary: Information Systems and Conceptual Modeling - A Research Agenda. Information Systems Research 13(4):363–376
3. Mylopoulos, J., Conceptual Modeling and Telos. In Loucopoulos, P., and Zicari, R., eds., Conceptual Modelling, Databases and CASE: An Integrated View of Information Systems Development. Wiley. 49–68, 1992
4. Pohl, K., Requirements Engineering: An Overview. In Kent, A., and Wiliams, J., eds., Encyclopedia of Computer Science and Technology, volume 36. Marcel Dekker, Inc. 40p, 1997
5. Institute of Electrical and Electronics Engineers. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY: 1990
6. Chen, Z., and Pooley, R., Rediscovering Zachman framework using ontology from a requirement engineering perspective. *Computer Software and Applications Conference, 2009. COMPSAC'09. 33rd Annual IEEE International*. Vol. 2. IEEE, 2009
7. Spyns, P., Tang, Y., and Meersman, R., An Ontology Engineering Methodology for DOGMA, Journal of Applied Ontology, special issue on "Ontological Foundations for Conceptual Modeling", Giancarlo Guizzardi and Terry Halpin (eds.), Volume 3, Issue 1-2, p.13-39 (2008)
8. Tang, Y., De Baer, P., Zhao, G. and Meersman, R., On Conducting, Grouping and Using Topical Ontology for Semantic Matching, the 5th international IFIP workshop on Semantic Web and Web Semantics (SWWS'09), proc. of On the Move to Meaningful Internet Systems: (OTM) 2009 Workshops, Springer, LNCS 5872, ISBN -978-3-642-05289-7, pp 816-825, Vilamoura, Portugal, Nov. 1 - Nov. 6, 2009
9. Object-role modeling (ORM): http://www.ormfoundation.org/