



1st Review, October 18, 2012, Rome

Concluding Remarks (Extract: Need for Formal Modeling)

Von: Josef Noll <josefnoll@gmail.com>
Gesendet: 10.10.2012 08:59
An: frank.j.furrer@bluewin.ch
Kopie/Cc: Luigi Trono, (SELEX GALILEO, Italy) <luigi.trono@selexgalileo.com>
Betreff: Re: nSHIELD

Frank,

good to hear that you will loan your expertise to help nSHIELD becoming the "star of all Artemis projects"

Kind regards
Josef

Josef,

My pleasure – but it will be quite hard work to become "Best of (Artemis) Show"

Frank



... let's start with some homework for the project 😊

The nSHIELD consortium recognizes the necessity and value of a clearly defined architecture and of well specified concepts
(Demonstrated in various deliverables, e.g. D2.4 & D2.5)

... however:

There is not sufficient precision and semantics in the pSHIELD descriptions of the architecture, the concepts and the relationships between the concepts

(Sorry – no criticism, but a well-founded experience from large systems engineering)

... what is needed:

- a conceptual, structural model of the overall architecture (**all concepts, their relationships, and constraints**) in a formal modeling language and a consistent, complete glossary
- a specification for the definition of contracts (relationships), possibly using an existing CSL (Contract specification language)
- a more formalized model for the metrics-composition

Illustrative examples follow ...



Pilot SHIELD

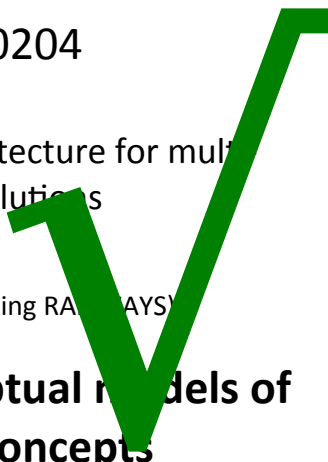
pilot embedded Systems architecture for multi-Layer Dependable solutions

SEVEN FRAMEWORK PROGRAMME

Project no: 100204

pSHIELD

pilot embedded Systems architecture for multi-layer dependable solutions



Instrument type: Capability Project

Priority name: Embedded Systems (including RA and AYS)

M0.1: Formalized conceptual models of the key pSHIELD concepts

Due date of deliverable: 15th April 2011

Actual submission date: 15th April 2011

Start date of project: 1st June 2010

Duration: 12 months

Organisation name of lead contractor for this deliverable:

pSHIELD Consortium

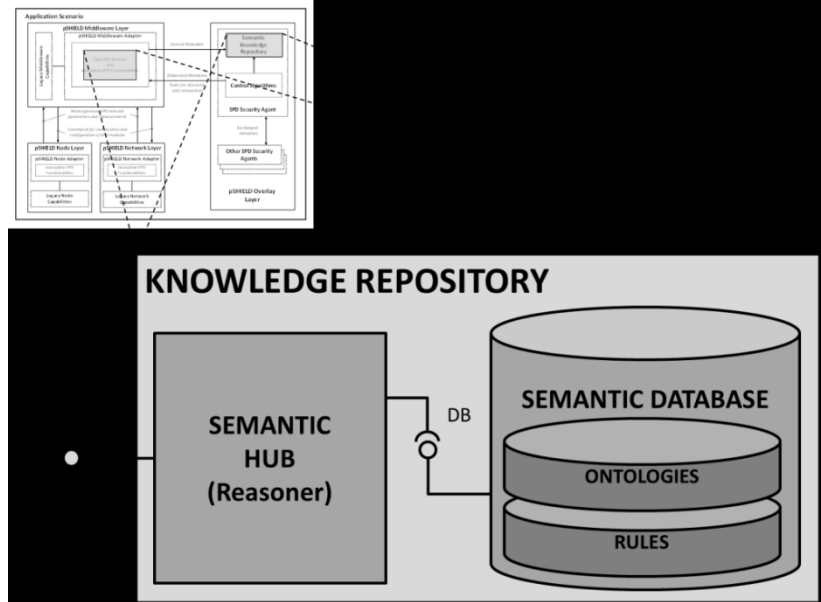


Figure 5.11 Knowledge Repository conceptual model

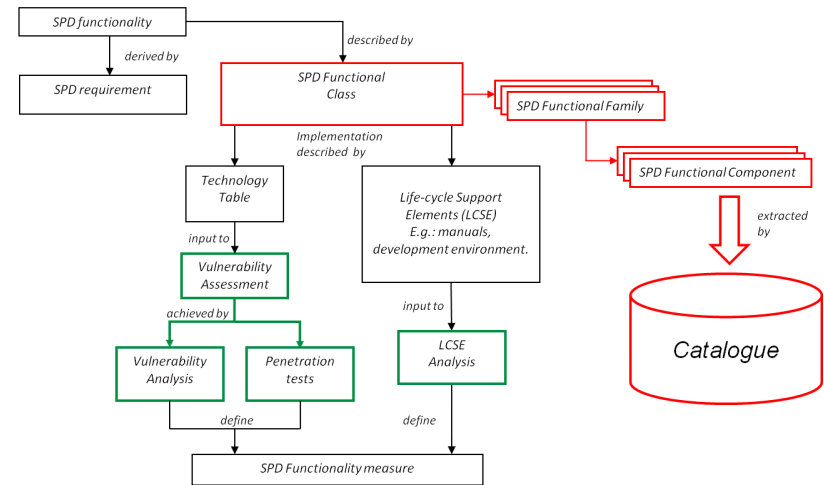
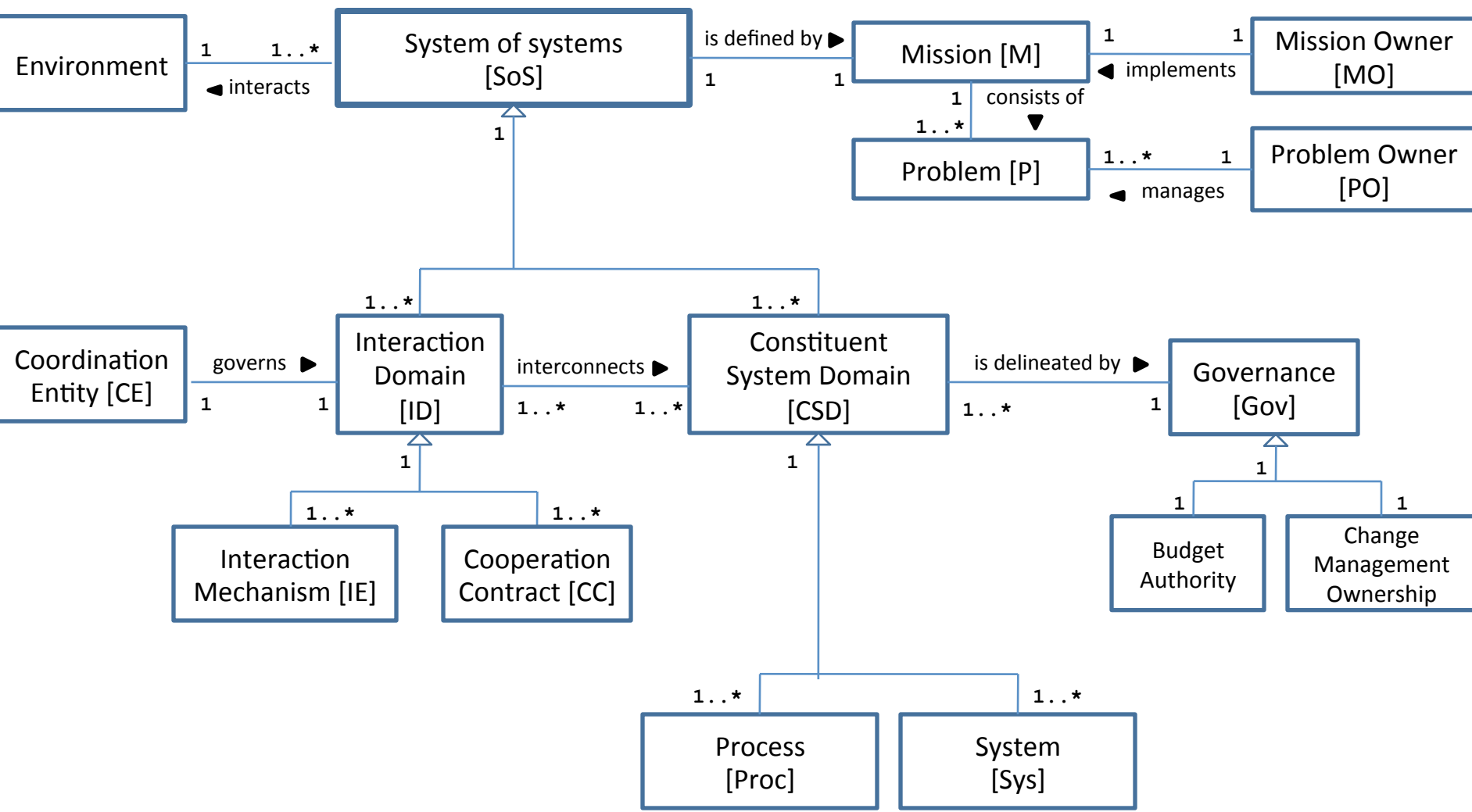


Figure 5.25 conceptual model for the calculation of SPD status

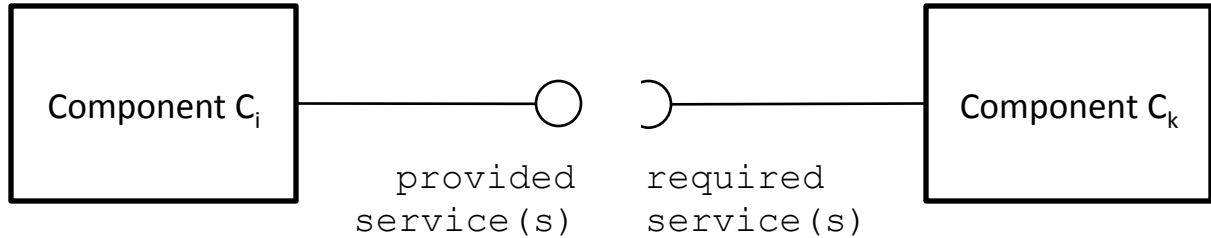
We need more precision, consistency and formalization (UML2, SysML ?)

Example for a top-level structural (architectural) model:

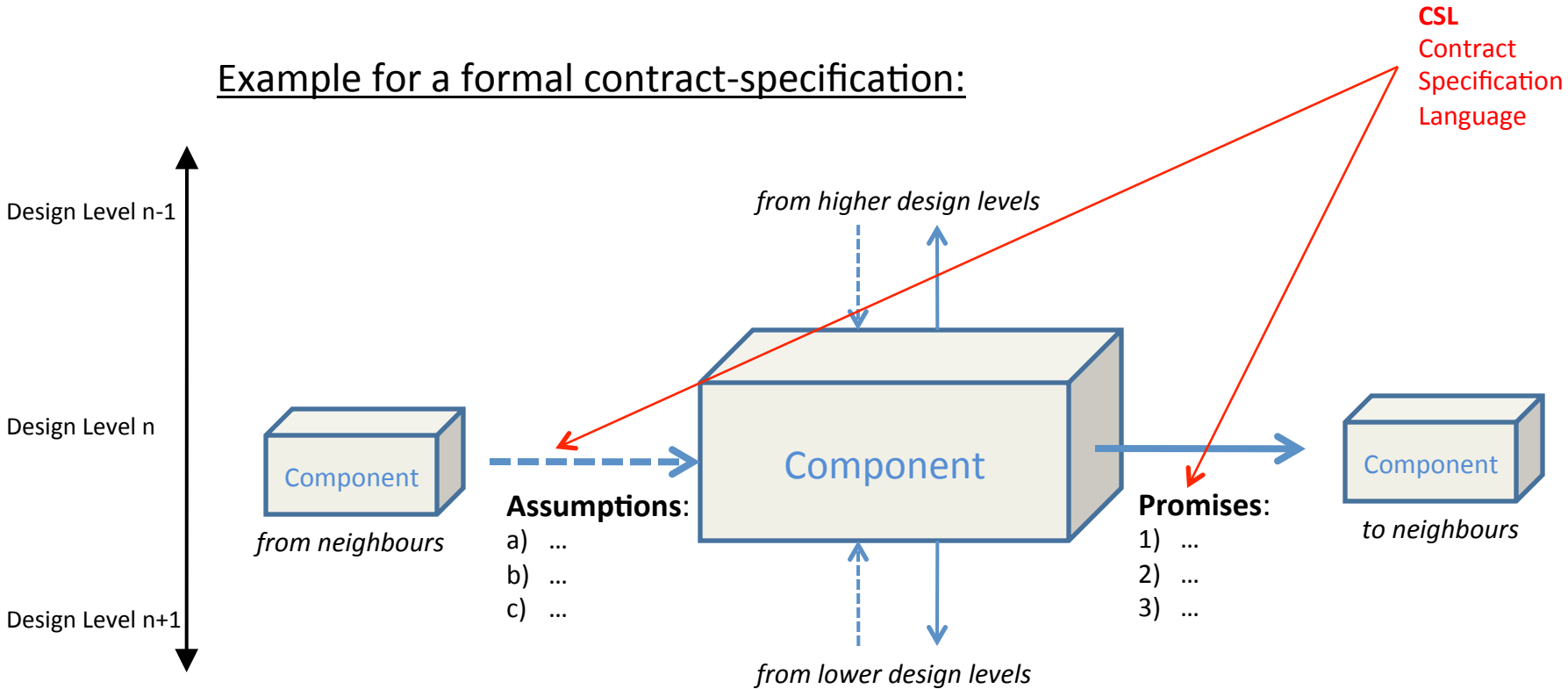
Top Level Structural Model of System-of-Systems



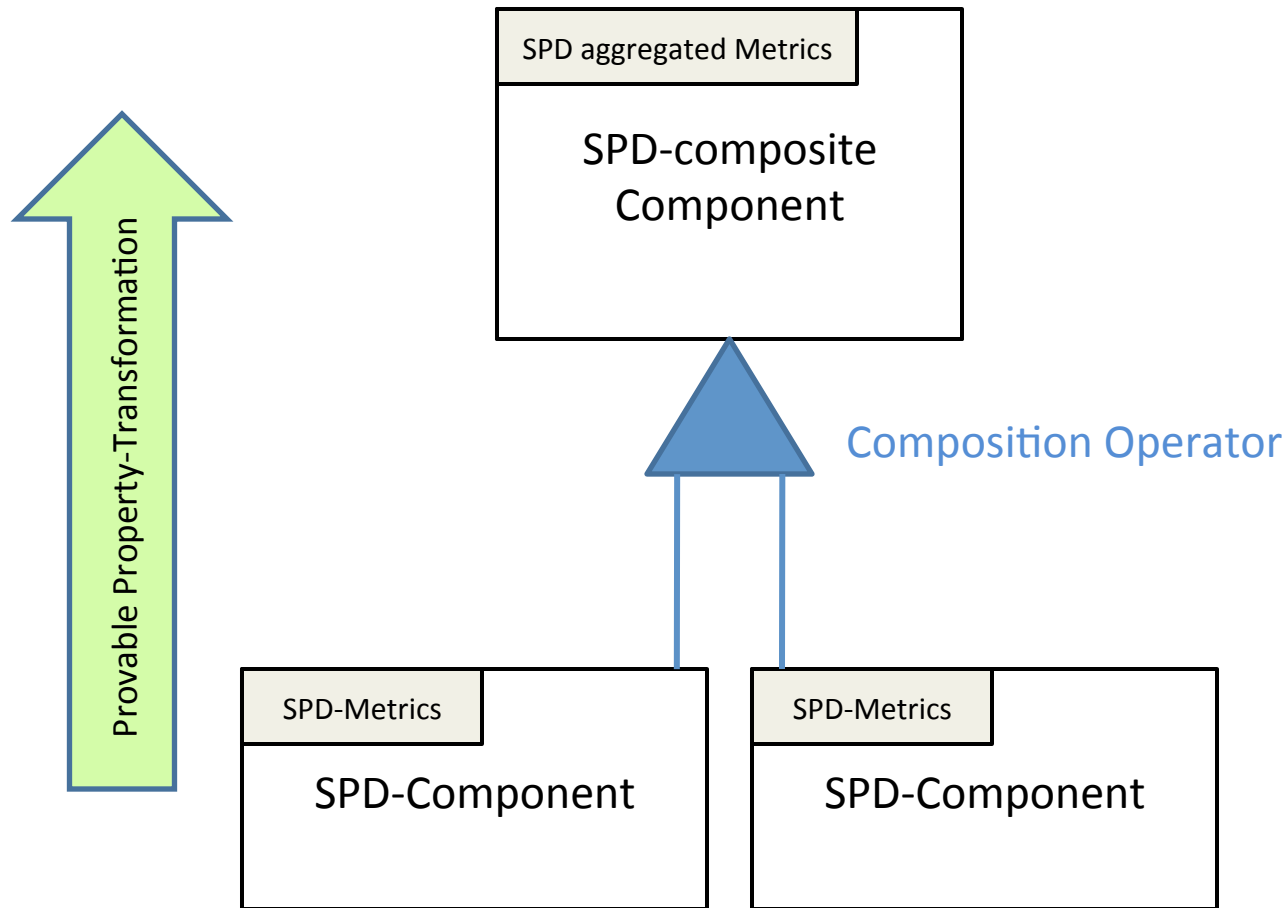
Component Contract Specifications



Example for a formal contract-specification:



SPD-Metric Composition



Kung-Kiu Lau, Ioannis Ntalamagkas, Cuong M. Tran, and Tauseef Rana:
Design Patterns as Composition Operators

Available from: <http://www.cs.man.ac.uk/~kung-kiu/pub/cbse10.pdf>

In: Component-Based Software Engineering

13th International Symposium, CBSE 2010, Prague, Czech Republic, June 23-25, 2010

Series: LNCS, Vol. 6092 (Editors: Grunke, Lars; Reussner, Ralf H.; Plasil, Frantisek)

Springer, Berlin, 1st Edition., 2010, ISBN 978-3-642-13237-7, pp. 232–251.



Pilot SHIELD

pilot embedded Systems
archItecturE for multi-Layer Dependable solutions



Project no: 100204

p-SHIELD

pilot embedded Systems architecture for multi-Layer
Dependable solutions

Instrument type: Capability Project

Priority name: Embedded Systems (including RAILWAYS)

M0.2: Proposal for the aggregation of SPD metrics during composition

Due date of deliverable: 15th April 2011

Actual submission date: 13th April 2011

Start date of project: 1st June 2010 Duration: 12 months

Organisation name of lead contractor for this deliverable:

pSHIELD Consortium

Revision [1.0]

**Project co-funded by the European Commission within the
ARTEMIS-JU (2007-2013)**

This paper presents a step towards modeling SPD system by a divide and conquer approach as it is widely known from the area of reliability/availability modeling.

For this purpose, basic SPD measures are provided by Common Criteria approach summarized in chapter 4. Then Chapter 5-6 explain the basic ideas of how to compute a system's SPD measure from measures of its components. Repeatedly, two SPD measures of components are combined into a single value by operators. In chapter 6 an example shows how to apply the proposed method in an application scenario

Proposed (pSHIELD):
OR, MIN, MEAN
strictly hierarchical (tree)

Questions:

- topological constraints?
- Congruency with the component composition model?
- completeness of composition operators?
- provable SPD-transformation attributes?
- formalization (syntax, semantics)?

„Projects fail and disasters occur for many reasons.

However, there are three underlying reasons why things go wrong in life, which are known as the **„three evils‘ of systems engineering:**

- Complexity
- Lack of understanding
- Communication issues“

Jon Holt and Simon Perry: **SysML for Systems Engineering.**

The Institution of Engineering and Technology, Herts, UK, 2008. ISBN 978-0-86341-825-9

Formal Models are excellent instruments for managing complexity, force exact understanding and enable precise communication