The Rôle of Domain Engineering in Software Development

Why Current Requirements Engineering Seems Flawed

NWPT, 16 October 2009

Dines Bjørner
Fredsvej 11, DK-2840 Holte, Danmark
E–Mail: bjorner@gmail.com, URL: www.imm.dtu.dk/~db

October 12, 2009: 12:02

Abstract

Dogma

- Before **software** can be **design**ed (S)
- we must make sure we understand the **requirements** (R),
- and before we can express the **requirements**
- we must make sure that we understand the application **domain** (D):
  - ⋆ the area of activity of the users of the required software,
  - ⋆ before and after installment of such software.

[**Abstract**]

Consequences of Dogma

- So we shall, in this talk, outline a development process:
  - ⋆ that startse with **domain engineering**
  - ⋆ proceeds to **requirements engineering**
  - ⋆ and "ends" with software design.
- Emphasis is on domain engineering.
- But we briefly touch upon **relation**
  - ⋆ of requirements prescriptions
  - ⋆ to domain description.

The Software Development Dogma

What Do We Mean by 'Domain' ?

- By a domain we shall loosely understand an 'area' of
  - ⋆ natural or
  - ⋆ human

  activity, or both,
- where the 'area' is "well-delineated" such as, for example,
  - ⋆ for physics:
    - ◇ mechanics or
    - ◇ electricity or
    - ◇ chemistry or
    - ◇ hydrodynamics;
  - ⋆ or for an infrastructure component:
    - ◇ banking,
    - ◇ railways,
    - ◇ hospital health-care,
    - ◇ "the market":
      - ○ consumers,
      - ○ retailers,
      - ○ wholesalers,
      - ○ producers and
      - ○ the distribution chain.

By a *domain* we shall thus, less loosely, understand

- a universe of discourse, small or large, a structure of **entities**:
  - ⋆ (i) of **simple entities**, that is, of “things”, individuals, particulars
    - ◇ some of which are designated as **state** components;
  - ⋆ (ii) of **functions**, say over **entities**,
    - ◇ which when applied become possibly state-changing **actions** of the domain;
  - ⋆ (iii) of **events**,
    - ◇ possibly involving **entities**, occurring in **time** and
    - ◇ expressible as **predicates** over single or pairs of (before/after) **states**; and
  - ⋆ (iv) of **behaviours**,
    - ◇ sets of possibly interrelated sequences of **actions** and **events**.

Dialectics

- Can we develop software requirements without understanding the domain ?
  - ⋆ No, of course we cannot !
  - ⋆ But we, you, do develop software for hospitals (railways, banks) without understanding health-care (transportation, the financial markets) anyway !

- In other engineering disciplines professionalism is ingrained:
  - ⋆ Aeronautics engineers understand the domain of aerodynamics;
  - ⋆ naval architects (i.e., ship designers) understand the domain of hydrodynamics;
  - ⋆ telecommunications engineers understand the domain of electromagnetic field theory;
  - ⋆ and so forth.
- Well, how much of the domain should we understand ?
  - ⋆ A basic answer is this:
    - ◇ enough for us to understand formal descriptions of such a domain.

[The Software Development Dogma, Dialectics]

- This is so in classical engineering:
  - ⋆ Although the telecommunications engineer has not herself researched and made mathematical models of electromagnetic wave propagation in the form of Maxwell's equations:
    - ◇ Gauss's Law for Electricity,
    - ◇ Gauss's Law for Magnetism,
    - ◇ Faraday's Law of Induction,
    - ◇ Ampéres Law:

$$\oint \vec{E}\cdot d\vec{A} = \frac{q}{\varepsilon_0} \quad \oint \vec{B}\cdot d\vec{A} = 0 \quad \oint \vec{E}\cdot d\vec{s} = -\frac{d\Phi_B}{dt} \quad \oint \vec{B}\cdot d\vec{s} = \mu_0 i + \frac{1}{c^2}\frac{\partial}{\partial t}\int \vec{E}\cdot d\vec{A}$$

  - ⋆ the telecommunications engineer certainly understands these laws.
- And how well should we understand it ?
  - ⋆ Well, enough, as an engineer, to manipulate the formulas,
  - ⋆ to further develop these for engineering calculations.

The Triptych of Software Development

- We recall the dogma:
  - ⋆ before software can be designed
  - ⋆ we must understand the requirements.
  - ⋆ Before requirements can be finalised
  - ⋆ we must have understood the domain.

[The Triptych of Software Development]

Three Phases of SE

- We conclude from that, that an “ideal” software development proceeds, in three major development phases, as follows:
- **Domain engineering**: The results of domain engineering include a domain model: a description,
  - ⋆ both informal, as a precise narrative,
  - ⋆ and formal, as a specification.
- The domain is described **as it is.**

- **Requirements engineering**: The results of requirements engineering include a requirements model: a prescription,
  - ⋆ both informal, as a precise narrative,
  - ⋆ and formal, as a specification.
- The requirements are described
  as we would like the software to be,
- and the requirements must be
  clearly related to the domain description.

[The Triptych of Software Development, Three Phases of SE]

- **Software design**: The results of software design include
  - ⋆ executable code
  - ⋆ and all documentation that goes with it.
- The software design specification must be **correct with respect to the requirements.**

Technicalities: An Overview

Domain Engineering

- Below we outline techniques of domain engineering. But just as a preview:
  - ⋆ Based on extensive domain acquisition and analysis
  - ⋆ an informal and a formal domain model is established, a model which is centered around sub-models of:
    - ◇ intrinsics,
    - ◇ supporting technologies,
    - ◇ mgt. and org.,
    - ◇ rules and regulations,
    - ◇ script [or contract] languages and
    - ◇ human behaviours,

    which are then
  - ⋆ validated and verified.

Requirements Engineering

- Below we outline techniques of requirements engineering. But just as a preview:
  - ⋆ Based on presentations of the domain model to requirements stakeholders
  - ⋆ requirements can now be “derived” from the domain model and as follows:
    - ◇ First a **domain requirements** model:
      - ○ **projection**,
      - ○ **instantiation**,
      - ○ **determination**,
      - ○ **extension** and
      - ○ **fitting** of several, separate domain requirements models;
    - ◇ then an **interface requirements** model,
    - ◇ and finally a **machine requirements** model.
  - ⋆ These are simultaneously verified and validated
  - ⋆ and the feasibility and satisfiability of the emerging model is checked.
- We show only the briefly explained specifications of an example “derivation” of (and in this case only of, and then only some aspects of) domain requirements.

Software Design

- We do not cover techniques of software design in detail — so only this summary.
  - ⋆ From the requirements prescription one develops,
    - ◇ in stages and steps of transformation (refinement),
    - ◇ the system architecture, then the program (code) organisation (structure), and then, in further steps of development,
      - ◦ the component design, the module design and the code.
  - ⋆ These stages and step can be verified, model checked and tested.
- One can then assert that the $\mathcal{S}$oftware design is correct with respect to the $\mathcal{R}$equirements in the context of the assumptions expressed about the $\mathcal{D}$omain:

$$\mathcal{D},\ \mathcal{S} \models \mathcal{R}$$

Domain Engineering

- We shall focus only on the actual modelling, thus omitting any treatment of
  - ⋆ the preparatory administrative and informative work,
  - ⋆ the identification of and liaison with domain stakeholders,
  - ⋆ the domain acquisition and analysis, and
  - ⋆ the establishment of a domain terminology (document).
- So we go straight to the descriptive work.
  - ⋆ We first illustrate the ideas of modelling domain phenomena and concepts in terms of simple entities, operations, events and behaviours,
  - ⋆ then we model the domain in terms of domain facets.
- We do not have time for any treatment of domain verification, domain validations and the establishment of a domain theory.

[**Domain Engineering**]

Domain Facets

- By a **domain facet** we mean
  - ⋆ one amongst a finite set of generic ways
  - ⋆ of analysing a domain:
  - ⋆ a view of the domain,
  - ⋆ such that the different facets cover conceptually different views,
  - ⋆ and such that these views together cover the domain
- We shall postulate the following domain facets:
  - ⋆ intrinsics,
  - ⋆ support technologies,
  - ⋆ management & organisation,
  - ⋆ rules & regulations,
  - ⋆ script languages [contract languages] and
  - ⋆ human behaviour.
- Each facet covers simple entities, operations, events and behaviours.
- We shall now illustrate these.

[**Domain Engineering**, **Domain Facets**]

Intrinsics

- By **domain intrinsics** we mean
  - ⋆ those phenomena and concepts of a domain which are basic to any of the other facets (listed earlier and treated, in some detail, below),
  - ⋆ with such domain intrinsics initially covering at least one specific, hence named, stakeholder view.

Example 1: Intrinsics, I: Narrative

1. There are hubs and links.
2. There are nets, and a net consists of a set of two or more hubs and one or more links.
3. There are hub and link identifiers.
4. Each hub (and each link) has an own, unique hub (respectively link) identifiers (which can be observed from the hub [respectively link]).

[Domain Engineering, Domain Facets, Intrinsics]

Example 2: Intrinsics, I: Formalisation

type

1 $\mathrm{H}, \mathrm{L},$

2 $\mathrm{N} = \mathrm{H}\textbf{-set} \times \mathrm{L}\textbf{-set}$

axiom

2 $\forall\ (\mathrm{hs},\mathrm{ls}){:}\mathrm{N} \cdot \textbf{card}\ \mathrm{hs} \geq 2 \wedge \textbf{card}\ \mathrm{hs} \geq 1$

type

3 HI, LI

value

4a $\mathrm{obs\_HI}{:}\ \mathrm{H} \rightarrow \mathrm{HI},\ \mathrm{obs\_LI}{:}\ \mathrm{L} \rightarrow \mathrm{LI}$

axiom

4b $\forall\ \mathrm{h},\mathrm{h}'{:}\mathrm{H},\ \mathrm{l},\mathrm{l}'{:}\mathrm{L} \cdot \mathrm{h} \neq \mathrm{h}' \Rightarrow \mathrm{obs\_HI}(\mathrm{h}) \neq \mathrm{obs\_HI}(\mathrm{h}') \wedge \mathrm{l} \neq \mathrm{l}' \Rightarrow \mathrm{obs\_LI}(\mathrm{l}) \neq \mathrm{obs\_LI}(\mathrm{l}')$

[Domain Engineering, Domain Facets, Intrinsics]

Example 3: Intrinsics, II

5. From any link of a net one can observe the two hubs to which the link is connected.
   (a) We take this ‘observing’ to mean the following: From any link of a net one can observe the two distinct identifiers of these hubs.
6. From any hub of a net one can observe the one or more links to which are connected to the hub.
   (a) Again: by observing their distinct link identifiers.
7. Extending Item 5: the observed hub identifiers must be identifiers of hubs of the net to which the link belongs.
8. Extending Item 6: the observed link identifiers must be identifiers of links of the net to which the hub belongs.

value

5a $\mathrm{obs\_HIs}: \mathrm{L} \rightarrow \mathrm{HI}\textbf{-set}$,

6a $\mathrm{obs\_LIs}: \mathrm{H} \rightarrow \mathrm{LI}\textbf{-set}$,

axiom

5b $\forall\ \mathrm{l:L} \cdot \textbf{card}\ \mathrm{obs\_HIs(l)}=2 \wedge$

6b $\forall\ \mathrm{h:H} \cdot \textbf{card}\ \mathrm{obs\_LIs(h)}\geq 1 \wedge$

$\forall\ \mathrm{(hs,ls):N} \cdot$

5(a) $\forall\ \mathrm{h:H} \cdot \mathrm{h} \in \mathrm{hs} \Rightarrow \forall\ \mathrm{li:LI} \cdot \mathrm{li} \in \mathrm{obs\_LIs(h)} \Rightarrow$

$\exists\ \mathrm{l'{:}L} \cdot \mathrm{l'} \in \mathrm{ls} \wedge \mathrm{li}=\mathrm{obs\_LI(l')} \wedge \mathrm{obs\_HI(h)} \in \mathrm{obs\_HIs(l')} \wedge$

6(a) $\forall\ \mathrm{l:L} \cdot \mathrm{l} \in \mathrm{ls} \Rightarrow$

$\exists\ \mathrm{h',h''{:}H} \cdot \{\mathrm{h',h''}\}\subseteq\mathrm{hs} \wedge \mathrm{obs\_HIs(l)}=\{\mathrm{obs\_HI(h')},\mathrm{obs\_HI(h'')}\}$

7 $\forall\ \mathrm{h:H} \cdot \mathrm{h} \in \mathrm{hs} \Rightarrow \mathrm{obs\_LIs(h)} \subseteq \mathrm{iols(ls)}$

8 $\forall\ \mathrm{l:L} \cdot \mathrm{l} \in \mathrm{ls} \Rightarrow \mathrm{obs\_HIs(h)} \subseteq \mathrm{iohs(hs)}$

value

$\mathrm{iohs}: \mathrm{H}\textbf{-set} \rightarrow \mathrm{HI}\textbf{-set},\ \mathrm{iols}: \mathrm{L}\textbf{-set} \rightarrow \mathrm{LI}\textbf{-set}$

$\mathrm{iohs(hs)} \equiv \{\mathrm{obs\_HI(h)}|\mathrm{h:H}\cdot\mathrm{h} \in \mathrm{hs}\}$

$\mathrm{iols(ls)} \equiv \{\mathrm{obs\_LI(l)}|\mathrm{l:L}\cdot\mathrm{l} \in \mathrm{ls}\}$

[Domain Engineering, Domain Facets]

Support Technologies

- By **domain support technologies** we mean
  - ⋆ ways and means of concretesing
  - ⋆ certain observed (abstract or concrete) phenomena or
  - ⋆ certain conceived concepts
  - ⋆ in terms of (possibly combinations of)

◇ human work,	◇ pneumatic,	◇ electronic,
◇ mechanical,	◇ aero-mechanical,	◇ telecommunication,
◇ hydro mechanical,	◇ electro-mechanical,	◇ photo/opto-electric,
◇ thermo-mechanical,	◇ electrical,	◇ chemical, etc.

(possibly computerised) sensor, actuator tools.

- In this example of a support technology
  - ⋆ we shall illustrate an abstraction
  - ⋆ of the kind of semaphore signalling
  - ⋆ one encounters at road intersections, that is, hubs.
- The example is indeed an abstraction:
  - ⋆ we do not model the actual "machinery"
    - ◇ of road sensors,
    - ◇ hub-side monitoring & control boxes, and
    - ◇ the actuators of the **green**/yellow/**red** sempahore lamps.
  - ⋆ But, eventually, one has to,
  - ⋆ all of it,
  - ⋆ as part of domain modelling.

Example 4: Hub Sempahores

- To model signalling we need to model hub and link states.
- A hub (link) state is the set of all traversals that the hub (link) allows.
  - ⋆ A hub traversal is a triple of identifiers:
    - ◇ of the link from where the hub traversal starts,
    - ◇ of the hub being traversed, and
    - ◇ of the link to where the hub traversal ends.
  - ⋆ A link traversal is a triple of identifiers:
    - ◇ of the hub from where the link traversal starts,
    - ◇ of the link being traversed, and
    - ◇ of the hub to where the link traversal ends.
  - ⋆ A hub (link) state space is the set of all states that the hub (link) may be in.
  - ⋆ A hub (link) state changing operation can be designated by
    - ◇ the hub and a possibly new hub state (the link and a possibly new link state).

```
type
  $\mathrm{L\Sigma' = L\_Trav}$-**set**
  $\mathrm{L\_Trav = (HI \times LI \times HI)}$
  $\mathrm{L\Sigma = \{|\ lnk\sigma{:}L\Sigma' \cdot syn\_wf\_L\Sigma\{lnk\sigma\}\ |\}}$
  $\mathrm{H\Sigma' = H\_Trav}$-**set**
  $\mathrm{H\_Trav = (LI \times HI \times LI)}$
  $\mathrm{H\Sigma = \{|\ hub\sigma{:}H\Sigma' \cdot wf\_H\Sigma\{hub\sigma\}\ |\}}$
  $\mathrm{H\Omega = H\Sigma}$-**set**, $\mathrm{L\Omega = L\Sigma}$-**set**
value
  $\mathrm{obs\_L\Sigma{:}\ L \to L\Sigma,\ obs\_L\Omega{:}\ L \to L\Omega}$
  $\mathrm{obs\_H\Sigma{:}\ H \to H\Sigma,\ obs\_H\Omega{:}\ H \to H\Omega}$
axiom
  $\mathrm{\forall\ h{:}H \cdot obs\_H\Sigma(h) \in obs\_H\Omega(h) \wedge \forall\ l{:}L \cdot obs\_L\Sigma(l) \in obs\_L\Omega(l)}$
value
  $\mathrm{chg\_H\Sigma{:}\ H \times H\Sigma \to H,\ chg\_L\Sigma{:}\ L \times L\Sigma \to L}$
  $\mathrm{chg\_H\Sigma(h,h\sigma)}$ **as** $\mathrm{h'}$ **pre** $\mathrm{h\sigma \in obs\_H\Omega(h)}$ **post** $\mathrm{obs\_H\Sigma(h')=h\sigma}$
  $\mathrm{chg\_L\Sigma(l,l\sigma)}$ **as** $\mathrm{l'}$ **pre** $\mathrm{l\sigma \in obs\_L\Omega(h)}$ **post** $\mathrm{obs\_H\Sigma(l')=l\sigma}$
```

- Well, so far we have indicated that there is an operation that can change hub and link states.
- But one may debate whether those operations shown are really examples of a support technology. (That is, one could equally well claim that they remain examples of intrinsic facets.)
- We may accept that and then ask the question:
  - ⋆ How to effect the described state changing functions ?
  - ⋆ In a simple street crossing a semaphore does not instantaneously change from red to green in one direction while changing from green to red in the cross direction.
  - ⋆ Rather there is are intermediate sequences of, for example, not necessarily synchronised **green**/yellow/**red** and **red**/yellow/**green** states to help avoid vehicle crashes and to prepare vehicle drivers.
- Our "solution" is to modify the hub state notion.

[Domain Engineering, Domain Facets, Support Technologies]

```
type
  Colour == red | yellow | green
  X = LI×HI×LI×Colour [crossings of a hub]
  HΣ = X-set [hub states]
value
  obs_HΣ: H → HΣ, xtr_Xs: H → X-set
  xtr_Xs(h) ≡
    {(li,hi,li′,c)|li,li′:LI,hi:HI,c:Colour•{li,li′}⊆obs_LIs(h)∧hi=obs_HI(h)}
axiom
  ∀ n:N,h:H • h ∈ obs_Hs(n) ⇒ obs_HΣ(h)⊆xtr_Xs(h) ∧
    ∀ (li1,hi2,li3,c),(li4,hi5,li6,c′):X •
      {(li1,hi2,li3,c),(li4,hi5,li6,c′)}⊆obs_HΣ(h) ∧
      li1=li4 ∧ hi2=hi5 ∧ li3=li6 ⇒ c=c′
```

- We consider the colouring, or any such scheme, an aspect of a support technology facet.
- There remains, however, a description of how the technology that supports the intermediate sequences of colour changing hub states.
- We can think of each hub being provided with a mapping from pairs of "stable" (that is non-yellow coloured) hub states (hσ_i,hσ_f) to well-ordered sequences of intermediate "un-stable' (that is yellow coloured) hub states
  - ⋆ paired with some time interval information
  - ⋆ $\langle(h\sigma', t\delta'), (h\sigma'', t\delta''), \ldots, (h\sigma'^{\cdots\prime}, t\delta'^{\cdots\prime})\rangle$
  - ⋆ and so that each of these intermediate states can be set,
  - ⋆ according to the time interval information,[1]
  - ⋆ before the final hub state (hσ_f) is set.

[1] Hub state $h\sigma''$ is set $t\delta'$ time unites after hub state $h\sigma'$ was set.

[Domain Engineering, Domain Facets, Support Technologies]

```
type
  TI [ time interval ]
  Signalling = $(H\Sigma \times TI)^*$
  Sema = $(H\Sigma \times H\Sigma) \overrightarrow{m}$ Signalling
value
  obs_Sema: H $\rightarrow$ Sema, chg_H$\Sigma$: H $\times$ H$\Sigma$ $\rightarrow$ H, chg_H$\Sigma$_Seq: H $\times$ H$\Sigma$ $\rightarrow$ H
  chg_H$\Sigma$(h,h$\sigma$) as h$'$ pre h$\sigma$ $\in$ obs_H$\Omega$(h) post obs_H$\Sigma$(h$'$)=h$\sigma$
  chg_H$\Sigma$_Seq(h,h$\sigma$) $\equiv$
    let sigseq = (obs_Sema(h))(obs_$\Sigma$(h),h$\sigma$) in sig_seq(h)(sigseq) end

  sig_seq: H $\rightarrow$ Signalling $\rightarrow$ H
  sig_seq(h)(sigseq) $\equiv$
    if sigseq=$\langle\rangle$ then h else
    let (h$\sigma$,t$\delta$) = hd sigseq in
    let h$'$ = chg_H$\Sigma$(h,h$\sigma$); wait t$\delta$;
    sig_seq(h$'$)(tl sigseq) end end end
```

[Domain Engineering, Domain Facets]

Management and Organisation

Management

- By **domain management** we mean people
  - ⋆ (i) who determine, formulate and thus set standards (cf. rules and regulations, a later lecture topic) concerning
    - ◇ strategic, tactical and operational decisions;
  - ⋆ (ii) who ensure that these decisions are passed on to (lower) levels of management, and to “floor” staff;
  - ⋆ (iii) who make sure that such orders, as they were, are indeed carried out;
  - ⋆ (iv) who handle undesirable deviations in the carrying out of these orders cum decisions;
  - ⋆ and (v) who “backstop” complaints from lower management levels and from floor staff.

Organisation

- By **domain organisation** we mean
  - ⋆ the structuring of management and non-management staff levels;
  - ⋆ the allocation of
    - ◇ strategic, tactical and operational concerns
    - ◇ to within management and non-management staff levels;
  - ⋆ and hence the "lines of command":
    - ◇ who does what and
    - ◇ who reports to whom —
      - ○ administratively and
      - ○ functionally.

Examples

Example 5: Bus Transport Management & Organisation

- On Slides 51–57 we illustrate what is there called a contract language.
  - ⋆ "Programs" in that language are either contracts or are orders to perform the actions permitted or obligated by contracts.
  - ⋆ The language in question is one of managing bus traffic on a net.
  - ⋆ The **management & organisation** of bus traffic involves
    - ◇ contractors issuing contracts,
    - ◇ contractees acting according to contracts,
    - ◇ busses (owned or leased) by contractees,
    - ◇ and the bus traffic on the (road) net.
  - ⋆ Contractees, i.e., bus operators,
    - ◇ `"start"` buses according to a contract timetable,

◇ `"cancel"` buses if and when deemed necessary,

◇ `"insert"` rush-hour and other buses if and when deemed necessary,

◇ and, acting as contractors, `"sub-contract"` sub-contractees to operate bus lines,

  ∘ for example, when the issuing contractor is not able to operate these bus lines,

  ∘ i.e., not able to fulfill contractual obligations,

  ∘ due to unavailability of buses or staff.

- Clearly the programs of bus contract languages

  ⋆ are "executed" according to **management** decisions

  ⋆ and the sub-contracting "hierarchy" reflects **organisational** facets.

[Domain Engineering, Domain Facets]

Rules and Regulations

- Human stakeholders act in the domain, whether
  - ⋆ clients,
  - ⋆ workers,
  - ⋆ managers,
  - ⋆ suppliers,
  - ⋆ regulatory authorities,
  - ⋆ or other.
- Their actions are guided and constrained by rules and regulations.
- These are sometimes implicit, that is, not “written down”.
- But we can talk about rules and regulations as if they were explicitly formulated.

[Domain Engineering, Domain Facets, Rules and Regulations]

- The main difference between rules and regulations is that
  - ⋆ rules express properties that must hold and
  - ⋆ regulations express state changes that must be effected if rules are observed broken.
- Rules and regulations are directed
  - ⋆ not only at human behaviour
  - ⋆ but also at expected behaviours of support technologies.
- Rules and regulations are formulated
  - ⋆ by enterprise staff, management or workers,
  - ⋆ and/or by business and industry associations,
    - ◇ for example in the form of binding or guiding
    - ◇ national, regional or international standards,
  - ⋆ and/or by public regulatory agencies.

Domain Rules

- By a **domain rule** we mean
  - ⋆ some text
  - ⋆ which prescribes how people or equipment
  - ⋆ are expected to behave when dispatching their duty,
  - ⋆ respectively when performing their functions.

Domain Regulations

- By a **domain regulation** we mean
  - ⋆ some text
  - ⋆ which prescribes what remedial actions are to be taken
  - ⋆ when it is decided that a rule has not been followed according to its intention.

[Domain Engineering, Domain Facets, Rules and Regulations]

Two Informal Examples

Example 6: Trains at Stations: Available Station Rule and Regulation

- Rule:
  - ⋆ In China the arrival and departure of trains at, respectively from, railway stations is subject to the following rule:
  - ⋆ *In any three-minute interval at most one train may either arrive to or depart from a railway station.*
- Regulation:
  - ⋆ *If it is discovered that the above rule is not obeyed*, then there is some regulation which prescribes administrative or legal management and/or staff action, as well as some correction to the railway traffic.

Example 7: Trains Along Lines: Free Sector Rule and Regulation

- Rule:
  - ⋆ In many countries railway lines (between stations) are segmented into blocks or sectors. The purpose is to stipulate that if two or more trains are moving along the line, then:
  - ⋆ *There must be at least one free sector (i.e., without a train) between any two trains along a line.*
- Regulation:
  - ⋆ *If it is discovered that the above rule is not obeyed*, then there is some regulation which prescribes administrative or legal management and/or staff action, as well as some correction to the railway traffic.

[Domain Engineering, Domain Facets, Rules and Regulations]

A Formal Example

- We shall develop the above example (7, Slide 39) into a partial, formal specification.
- That is, not complete, but "complete enough" for the reader to see what goes on.

Example 8: Continuation of Example 7 Slide 39

- We start by analysing the text of the rule and regulation.
  - ⋆ The rule text: *There must be at least one free sector (i.e., without a train) between any two trains along a line.* contains the following terms:
    - ◇ free (a predicate),
    - ◇ sector (an entity),
    - ◇ train (an entity) and
    - ◇ line (an entity).
- We shall therefore augment our formal model to reflect these terms.
- We start by modelling
  - ⋆ sectors and sector descriptors,
  - ⋆ lines and train position descriptors,
  - ⋆ trains, and
  - ⋆ the predicate free.

```
type
  Sect′ = H × L × H,
  SectDescr = HI × LI × HI
  Sect = {|(h,l,h′):Sect′ • obs_HIs(l)={obs_HI(h),obs_HI(h′)}|}
  SectDescr =  {|(hi,li,hi′):SectDescr′ •
                   ∃ (h,l,j′):Sect•obs_HIs(l)={obs_HI(h),obs_HI(h′)}|}
  Line′ = Sect*,
  Line = {|line:Line′•wf_Line(line)|}
  TrnPos′ = SectDescr*
  TrnPos = {|trnpos′:TrnPos′•∃ line:Line•conv_Line_to_TrnPos(line)=trnpos′|}
value
  wf_Line: Line′ → Bool
  wf_Line(line) ≡
    ∀ i:Nat • {i,i+1}⊆inds(line) ⇒
      let (_,l,h)=line(i),(h′,l′,_)=line(i+1) in h=h′ end
  conv_Line_to_TrnPos: Line → TrnPos
  conv_Line_to_TrnPos(line) ≡
    ⟨(obs_HI(h),obs_LI(l),obs_HI(h′))|1≤i≤len line∧line(i)=(h,l,h′)⟩


value
  lines: N → Line-set
  lines(hs,ls) ≡
```

```
    **let** lns = $\{\langle(h,l,h')\rangle | h,h'{:}H,l{:}L \bullet proper\_line((h,l,h'),(hs,ls))\}$
            $\cup \{ln \frown ln' | ln,l'{:}Line \bullet \{ln,ln'\} \subseteq lns \wedge adjacent(ln,ln')\}$ **in**
    lns **end**

  adjacent: Line $\times$ Line $\to$ **Bool**
  adjacent((_,l,h),(h',l',_)) $\equiv$ h=h'
    **pre** $\{obs\_LI(l),obs\_LI(l')\} \subseteq obs\_LIs(h)$

**type**
  TF = T $\underset{m}{\to}$ (N $\times$ (TN $\underset{m}{\to}$ TrnPos))

**value**
  wf_TF: TF $\to$ **Bool**
  wf_TF(tf) $\equiv$
    $\forall$ t:T$\bullet$t $\in$ **dom** tf $\Rightarrow$
      **let** ((hs,ls),trnposs) = tf(t) **in**
      $\forall$ trn:TN $\bullet$ trn $\in$ **dom** trnposs $\Rightarrow$
        $\exists$ line:Line $\bullet$ line $\in$ lines(hs,ls) $\wedge$
          trnposs(trn) = conv_Line_to_TrnPos(line) **end**
```

- Nothing prevents two or more trains from occupying overlapping train positions.

- They have "merely" – and regrettably – crashed. But such is the domain.
- So wf_TF(tf) is not part of an axiom of traffic, merely a desirable property.

```
value
  has_free_Sector: $\mathrm{TN} \times \mathrm{T} \to \mathrm{TF} \to$ **Bool**
  has_free_Sector(trn,(hs,ls),t)(tf) $\equiv$
    **let** ((hs,ls),trnposs) = tf(t) **in**
    (trn $\notin$ **dom** trnposs $\vee$ (tn $\in$ **dom** trnposs(t) $\wedge$
     $\exists$ ln:Line • ln $\in$ lines(hs,ls) $\wedge$
       is_prefix(trnposs(trn),ln))(hs,ls)) $\wedge$
       $\sim\exists$ trn′:TN • trn′ $\in$ **dom** trnposs $\wedge$ trn′$\neq$trn $\wedge$
         trnposs(trn′)=conv_Line_to_TrnPos($\langle$follow_Sect(ln)(hs,ls)$\rangle$))
    **end**
    **pre** exists_follow_Sect(ln)(hs,ls)

  is_prefix: Line $\times$ Line $\to$ N $\to$ **Bool**
  is_prefix(ln,ln′)(hs,ls) $\equiv$ $\exists$ ln″:Line • ln″ $\in$ lines(hs,ls) $\wedge$ ln$\frown$ln″=ln′

  exists_follow_Sect: Line $\to$ Net $\to$ **Bool**
  exists_follow_Sect(ln)(hs,ls) $\equiv$
    $\exists$ ln′:Line•ln′ $\in$ lines(hs,ls)$\wedge$ln$\frown$ln′ $\in$ lines(hs,ls)
    **pre** ln $\in$ lines(hs,ls)
```

```
follow_Sect: Line → Net $\xrightarrow{\sim}$ Sect
follow_Sect(ln)(hs,ls) ≡
  let ln′:Line•ln′ ∈ lines(hs,ls)∧ln⌢ln′ ∈ lines(hs,ls) in hd ln′ end
  pre line ∈ lines(hs,ls)∧exists_follow_Sect(ln)(hs,ls)
```

- We doubly recursively define a function free_sector_rule(tf)(r).
- tf is that part of the traffic which has yet to be "searched" for non-free sectors.
  - ⋆ Thus tf is "counted" up from a first time t till the traffic tf is empty.
  - ⋆ That is, we assume a finite definition set tf .
- r is like a traffic but without the net.
  - ⋆ Initially r is the empty traffic.
  - ⋆ r is "counted" up from "earliest" cases of trains with no free sector ahead of them.
- The recursion stops, for a given time when
  - ⋆ there are no more train positions to be "searched" for that time;
  - ⋆ and when the "to-be-searched" traffic is empty.

```
type
  TNPoss = T $\xrightarrow[m]{}$ (TN → TrnPos)
value
```

```
free_sector_rule: TF × TF → TNPoss
free_sector_rule(tf)(r) ≡
  if tf=[ ] then r else
  let t:T•t ∈ dom tf∧smallest(t)(tf) in
  let ((hs,ls),trnposs)=tf(t) in
  if trnposs=[ ] then free_sector_rule(tf\{t})(r) else
  let tn:TN•tn ∈ dom trnposs in
  if exists_follow_Sect(trnposs(tn))(hs,ls)∧∼has_free_Sector(tn,(hs,ls),t)(tf)
    then
      let r′ = if t ∈ dom r then r else r ∪ [t↦[ ]] end in
      free_sector_rule(tf†[t↦((hs,ls),trnposs\{tn})])
                 (r†[t↦r(t)∪[tn↦trnposs(tn)]]) end
    else
      free_sector_rule(tf†[t↦((hs,ls),trnposs\{trn})])(r)
  end end end end end end

smallest(t)(tf) ≡ ∼∃ t′:T• t′isin dom tf∧t′<t pre t ∈ dom tf
```

[**Domain Engineering**, **Domain Facets**]

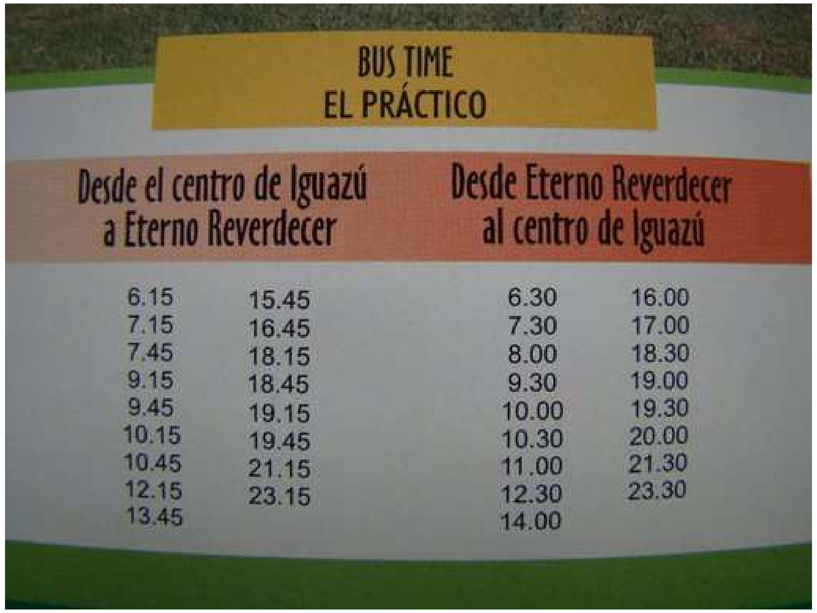
Script Languages [Contract Languages]

- By a **domain** $\boxed{\text{script}}$ **language** we mean
  - ⋆ the definition of a set of licenses and actions
  - ⋆ where these licenses when issued
  - ⋆ and actions when performed have morally obliging power.
- By a **domain** $\boxed{\text{contract}}$ **language**
  - ⋆ a domain script language whose licenses and actions have legally binding power,
  - ⋆ that is, their issuance and their invocation may be contested in a court of law.

[Domain Engineering, Domain Facets, Script Languages [Contract Languages]]

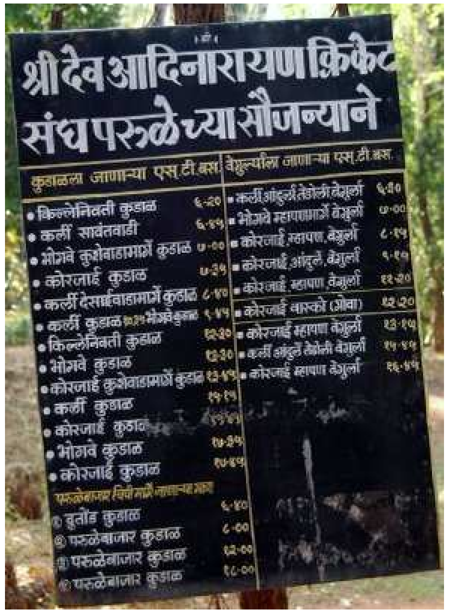
A Script Language

- Some common, visual forms of bus timetables are shown in Fig. 4.1.



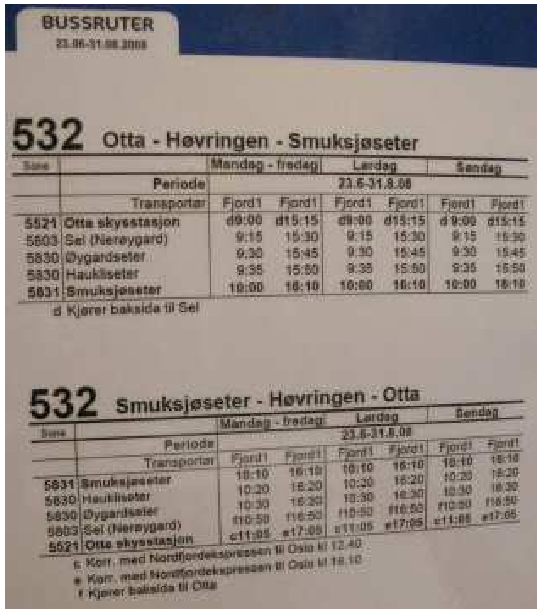
BUS TIME
EL PRÁCTICO

Desde el centro de Iguazú a Eterno Reverdecer		Desde Eterno Reverdecer al centro de Iguazú	
6.15	15.45	6.30	16.00
7.15	16.45	7.30	17.00
7.45	18.15	8.00	18.30
9.15	18.45	9.30	19.00
9.45	19.15	10.00	19.30
10.15	19.45	10.30	20.00
10.45	21.15	11.00	21.30
12.15	23.15	12.30	23.30
13.45		14.00	



श्री देव आदिनारायण क्रिकेट संघ परुळे च्या सौजन्याने

कुडाळला जाणाऱ्या एस.टी.बस		वेंगुर्ल्याला जाणाऱ्या एस.टी.बस	
• किल्लेनिवती कुडाळ	६-२०	• कर्ली आंदुर्ले तेंडोली वेंगुर्ले	६-४०
• कर्ली सावंतवाडी	६-४५	• भोगवे म्हापणमार्गे वेंगुर्ले	७-००
• भोगवे कुशेवाडामार्गे कुडाळ	७-००	• कोरजाई म्हापण वेंगुर्ले	८-१५
• कोरजाई कुडाळ	७-३५	• कोरजाई आंदुर्ले वेंगुर्ले	९-१५
• कर्ली देसाईवाडामार्गे कुडाळ	८-४०	• कोरजाई म्हापण वेंगुर्ले	१२-२०
• कर्ली कुडाळ [illegible]	९-४५	• कोरजाई वास्को (गोवा)	१२-२०
• किल्लेनिवती कुडाळ	१२-३०	• कोरजाई म्हापण वेंगुर्ले	१३-१५
• भोगवे कुडाळ	१२-३०	• कर्ली आंदुर्ले तेंडोली वेंगुर्ले	१५-४५
• कोरजाई कुशेवाडामार्गे कुडाळ	१३-४५	• कोरजाई म्हापण वेंगुर्ले	१६-४५
• कर्ली कुडाळ	१४-१५		
• कोरजाई कुडाळ	[illegible]		
• भोगवे कुडाळ	१७-३५		
• कोरजाई कुडाळ	१७-४५		
परुळेबाजार [illegible] मार्गे जाणाऱ्या बसेस			
दुतोंड कुडाळ	६-४०		
परुळेबाजार कुडाळ	८-००		
परुळेबाजार कुडाळ	१२-००		
परुळेबाजार कुडाळ	१८-००		



BUSSRUTER
23.06-31.08.2008

532 Otta - Høvringen - Smuksjøseter

Sone		Mandag - fredag		Lørdag		Søndag	
	Periode	23.6-31.8.08					
	Transportør	Fjord1	Fjord1	Fjord1	Fjord1	Fjord1	Fjord1
5521	Otta skysstasjon	d9:00	d15:15	d9:00	d15:15	d 9:00	d15:15
5803	Sel (Nerøygard)	9:15	15:30	9:15	15:30	9:15	15:30
5830	Øygardseter	9:30	15:45	9:30	15:45	9:30	15:45
5830	Haukliseter	9:35	15:50	9:35	15:50	9:35	15:50
5831	Smuksjøseter	10:00	16:10	10:00	16:10	10:00	16:10

d Kjører baksida til Sel

532 Smuksjøseter - Høvringen - Otta

Sone		Mandag - fredag		Lørdag		Søndag	
	Periode	23.6-31.8.08					
	Transportør	Fjord1	Fjord1	Fjord1	Fjord1	Fjord1	Fjord1
5831	Smuksjøseter	10:10	16:10	10:10	16:10	10:10	16:10
5830	Haukliseter	10:20	16:20	10:20	16:20	10:20	16:20
5830	Øygardseter	10:30	16:30	10:30	16:30	10:30	16:30
5803	Sel (Nerøygard)	f10:50	f16:50	f10:50	f16:50	f10:50	f16:50
5521	Otta skysstasjon	c11:05	e17:05	c11:05	e17:05	c11:05	e17:05

c Korr. med Nordfjordekspressen til Oslo kl 12.40
e Korr. med Nordfjordekspressen til Oslo kl 18.10
f Kjører baksida til Otta

Figure 4.1: Some bus timetables: Spain, India and Norway

[Domain Engineering, Domain Facets, Script Languages [Contract Languages], A Script Language]

Example 9: Narrative Syntax of a Bus Timetable Script Language

9. Time is a concept covered earlier. Bus lines and bus rides have unique names (across any set of time tables). Hub and link identifiers, HI, LI, were treated from the very beginning.
10. A TimeTable associates to Bus Line Identifiers a set of Journies.
11. Journies are designated by a pair of a BusRoute and a set of BusRides.
12. A BusRoute is a triple of the Bus Stop of origin, a list of zero, one or more intermediate Bus Stops and a destination Bus Stop.
13. A set of BusRides associates, to each of a number of Bus Identifiers a Bus Schedule.
14. A Bus Schedule a triple of the initial departure Time, a list of zero, one or more intermediate bus stop Times and a destination arrival Time.
15. A Bus Stop (i.e., its position) is a Fraction of the distance along a link (identified by a Link Identifier) from an identified hub to an identified hub.
16. A Fraction is a **Real** properly between 0 and 1.
17. The Journies must be well_formed in the context of some net.

Example 10: Formal Syntax of a Bus Timetable Script Language

type

9. T, BLId, BId
10. TT = BLId $\overrightarrow{m}$ Journies
11. Journies′ = BusRoute × BusRides
12. BusRoute = BusStop × BusStop* × BusStop
13. BusRides = BId $\overrightarrow{m}$ BusSched
14. BusSched = T × T* × T
15. BusStop == mkBS(s_fhi:HI,s_ol:LI,s_f:Frac,s_thi:HI)
16. Frac = {|r:**Real**·0<r<1|}
17. Journies = {|j:Journies′·∃ n:N · wf_Journies(j)(n)|}

[Domain Engineering, Domain Facets, Script Languages [Contract Languages], A Script Language]

Example 11: Semantics of a Bus Timetable Script Language

type
  Bus
value
  $\text{obs\_X: Bus} \rightarrow \text{X}$
type
  $\text{BusTraffic} = \text{T} \underset{m}{\overrightarrow{\ \ }} (\text{N} \times (\text{BusNo} \underset{m}{\overrightarrow{\ \ }} (\text{Bus} \times \text{BPos})))$
  $\text{BPos} = \text{atHub} \mid \text{onLnk} \mid \text{atBS}$
  $\text{atHub} == \text{mkAtHub(s\_fl:LIs\_hi:HI,s\_tl:LI)}$
  $\text{onLnk} == \text{mkOnLnk(s\_fhi:HI,s\_ol:LI,s\_f:Frac,s\_thi:HI)}$
  $\text{atBSt} == \text{mkAtBS(s\_fhi:HI,s\_ol:LI,s\_f:Frac,s\_thi:HI)}$
  $\text{Frac} = \{|\text{r:}\mathbf{Real}\cdot 0<\text{r}<1|\}$
value
  $\text{gen\_BusTraffic: TT} \rightarrow \text{BusTraffic-}\mathbf{infset}$
  $\text{gen\_BusTraffic(tt)}$ **as** btrfs
    post $\forall\ \text{btrf:BusTraffic} \cdot \text{btrf} \in \text{btrfs} \Rightarrow \text{on\_time(btrf)(tt)}$

[Domain Engineering, Domain Facets, Script Languages [Contract Languages]]

A Contract Language

- We shall, as for the timetable script, just hint at a contract language.

Example 12: Informal Syntax of Bus Transport Contracts

- An example contract can be ‘schematised’:

con_id: **contractor** corn **contracts contractee** ceen
 to perform operations `"start","cancel","insert","subcontract"`
 with respect to bus timetable tt.

[Domain Engineering, Domain Facets, Script Languages [Contract Languages], A Contract Language]

Example 13: Formal Syntax of a Bus Transport Contracts

type

CId, CNm

Contract = CId × CNm × CNm × Body

Body = Op-**set** × TT

Op == ″`conduct`″ | ″`cancel`″ | ″`insert`″ | ″`subcontract`″

an example contract:

(cid,cor,cee,({″`start`″,″`cancel`″,″`insert`″,″`subcontract`″},tt))

Example 14: Informal Syntax of a Bus Transport Actions

- Example actions can be schematised:

(a) cid: **start bus ride** (blid,bid) **at time** t
(b) cid: **cancel bus ride** (blid,bid) **at time** t
(c) cid: **insert bus ride like** (blid,bid) **at time** t

- The schematised license (Slide 51) shown earlier is almost like an action; here is the action form:

(d) cid: **contractee** cee **is granted a license** cid′
to perform operations {"start","cancel","insert",subcontract"}
with respect to timetable tt′.

[Domain Engineering, Domain Facets, Script Languages [Contract Languages], A Contract Language]

Example 15: Formal Syntax of a Bus Transport Actions

type

$\text{Action} = \text{CNm} \times \text{CId} \times (\text{SubLic} \mid \text{SmpAct}) \times \text{Time}$

$\text{SmpAct} = \text{Start} \mid \text{Cancel} \mid \text{Insert}$

$\text{DoRide} == \text{mkSta}(\text{s\_blid:BLId,s\_bid:BId})$

$\text{Cancel} == \text{mkCan}(\text{s\_blid:BLId,s\_bid:BId})$

$\text{Insert} = \text{mkIns}(\text{s\_blid:BLId,s\_bid:BId})$

$\text{SubCon} == \text{mkCon}(\text{s\_cid:ConId,s\_cee:CNm,s\_body:(s\_ops:Op}\textbf{-set}\text{,s\_tt:TT}))$

examples:

(a) (cee,cid,mkRid(blid,id),t)

(b) (cee,cid,mkCan(blid,id),t)

(c) (cee,cid,mkIns(blid,id),t)

(d) (cee,cid,mkCon(cid′,({″`start`″,″`cancel`″,″`insert`″,″`subcontract`″},tt′),t))

where: $\text{cid}' = \text{generate\_ConId}(\text{cid,cee,t})$

Example 16: Semantics of a Bus Transport Contract Language: States

type

$\mathrm{Body} = \mathrm{Op}\text{-}\mathbf{set} \times \mathrm{TT}$

$\mathrm{Con}\Sigma = \mathrm{RcvCon}\Sigma\times\mathrm{SubCon}\Sigma\times\mathrm{CorBus}\Sigma$

$\mathrm{RcvCon}\Sigma = \mathrm{CNm} \xrightarrow[m]{} (\mathrm{CId} \xrightarrow[m]{} (\mathrm{Body}\times\mathrm{TT}))$

$\mathrm{SubCon}\Sigma = \mathrm{CNm} \xrightarrow[m]{} (\mathrm{CId} \xrightarrow[m]{} \mathrm{Body})$

BusNo

$\mathrm{Bus}\Sigma = \mathrm{FreeBuses}\Sigma \times \mathrm{ActvBuses}\Sigma \times \mathrm{BusHists}\Sigma$

$\mathrm{FreeBuses}\Sigma = \mathrm{BusStop} \xrightarrow[m]{} \mathrm{BusNo}\text{-}\mathbf{set}$

$\mathrm{ActvBuses}\Sigma = \mathrm{BusNo} \xrightarrow[m]{} \mathrm{BusInfo}$

$\mathrm{BusInfo} = \mathrm{BLId}\times\mathrm{BId}\times\mathrm{CId}\times\mathrm{CNm}\times\mathrm{BusTrace}$

$\mathrm{BusHists}\Sigma = \mathrm{Bno} \xrightarrow[m]{} \mathrm{BusInfo}^*$

$\mathrm{BusTrace} = (\mathrm{Time}\times\mathrm{BusStop})^*$

$\mathrm{CorBus}\Sigma = \mathrm{CNm} \xrightarrow[m]{} (\mathrm{CId} \xrightarrow[m]{} ((\mathrm{BLId}\times\mathrm{BId}) \xrightarrow[m]{} (\mathrm{BNo}\times\mathrm{BusTrace})))$

$\mathrm{AllBs}{=}\mathrm{CNm} \xrightarrow[m]{} \mathrm{BusNo}\text{-}\mathbf{set}$

[Domain Engineering, Domain Facets, Script Languages [Contract Languages], A Contract Language]

Example 17: Semantics of a Bus Transport Contract Language: Constants and Functions

value

$\text{cns:CNm-}\mathbf{set}\text{, busnos:BNo-}\mathbf{set}\text{, ib}\sigma\text{:IB}\Sigma\text{s=CNm} \underset{m}{\rightarrow} \text{Bus}\Sigma\text{,}$
$\text{rcor,icee:CNm} \cdot \text{rcor} \notin \text{cns} \wedge \text{icee} \in \text{cns, itr:BusTraffic,}$
$\text{rcid:ConId, iops:Op-}\mathbf{set}\text{=}\{\text{"}\mathtt{subcontract}\text{"}\}\text{, itt:TT, } t_0\text{:Time}$
$\text{allbs:AllBs} \cdot \mathbf{dom}\text{ allbs=cns} \cup \{\text{rcor}\} \wedge \cup\ \mathbf{rng}\text{ allbs=busnos,}$
$\text{icon:Contract=(rcid,rcor,icee,(iops,itt)),}$
$\text{ic}\sigma\text{:Con}\Sigma\text{=([icee} \mapsto \text{[rcid} \mapsto \text{[icee} \mapsto \text{icon]]]}$
$\qquad \cup \text{ [cee} \mapsto \text{[ ] | cee:CNm} \cdot \text{cee} \in \text{cnms} \backslash \{\text{icee}\}\text{],[ ],[ ]),}$
system: $\mathbf{Unit} \rightarrow \mathbf{Unit}$
system() $\equiv$
  cntrcthldr(icee)(ilσ(icee),ibσ(icee))
  $\|$($\|${**cntrcthldr**(cee)(ilσ(cee),ibσ(cee))|cee:CNm$\cdot$cee $\in$ cns$\backslash${icee}})
  $\|$($\|${**bus_ride**(b,cee)(rcor,"`nil`")
    | cee:CNm,b:BusNo$\cdot$cee $\in$ **dom** allbs $\wedge$ b $\in$ allbs(cee)})
  $\|$**time_clock**(t_0) $\|$ **bus_traffic**(itr)

[Domain Engineering, Domain Facets, Script Languages [Contract Languages], A Contract Language]

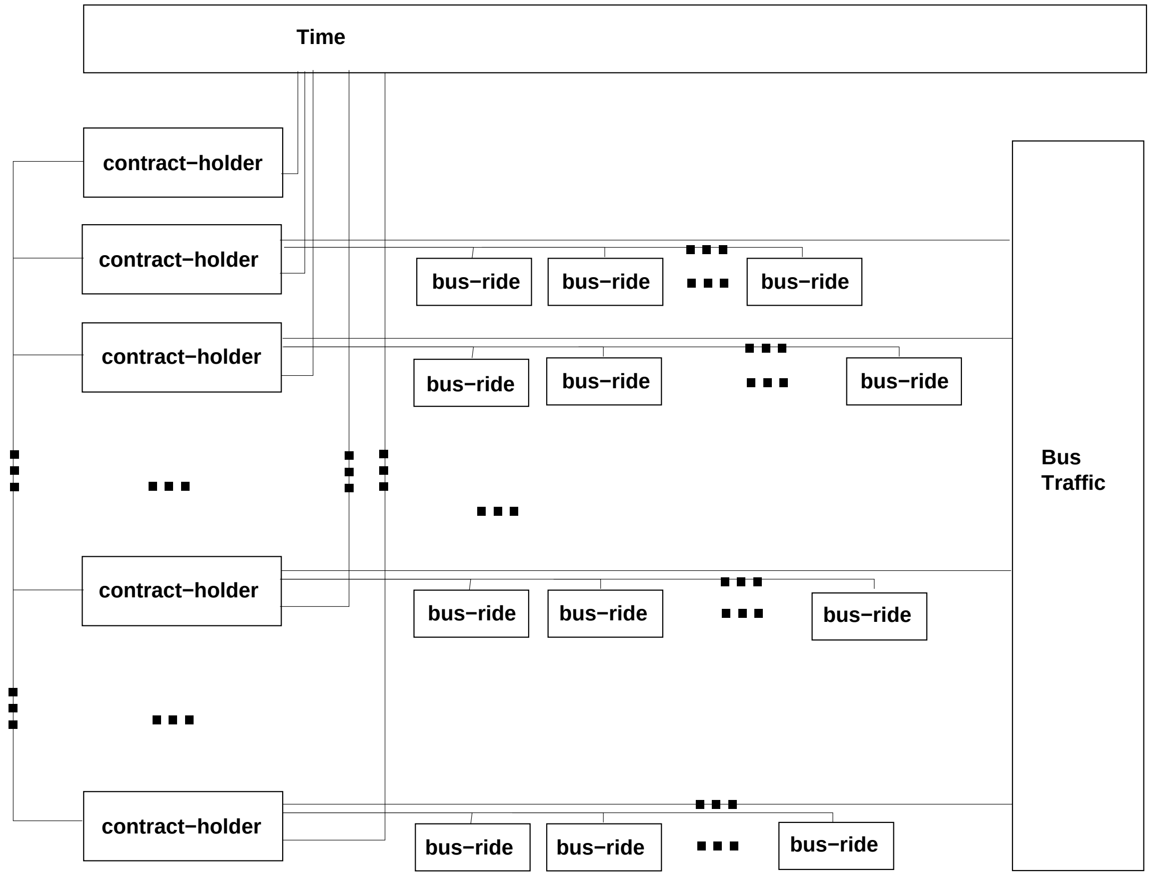


Figure 4.2: An organisation

- The thin lines of Fig. 4.2 denote communication "channels".

[Domain Engineering, Domain Facets]

Human Behaviour

- By **human behaviour** we mean any of
  a quality spectrum of carrying out assigned work:

  ⋆ from **careful, diligent** and **accurate**,

  via

  ⋆ **sloppy** dispatch, and

  ⋆ **delinquent** work,

  to

  ⋆ outright **criminal** pursuit.

[Domain Engineering, Domain Facets, Human Behaviour]

Example 18: A Diligent Operation

- The int_Insert operation of Slide ??
  - ⋆ was expressed without stating necessary pre-conditions:

18. The insert operation takes an Insert command and a net and yields either a new net or **chaos** for the case where the insertion command "is at odds" with, that is, is not semantically well-formed with respect to the net.
19. We characterise the "is not at odds", i.e., is semantically well-formed, that is: pre_int_Insert(op)(hs,ls), as follows: it is a propositional function which applies to Insert actions, op, and nets, (hs.ls), and yields a truth value if the below relation between the command arguments and the net is satisfied.
    Let (hs,ls) be a value of type N.
20. If the command is of the form 2oldH(hi′,l,hi′) then

    ⋆1 hi′ must be the identifier of a hub in hs,

    ⋆2 l must not be in ls and its identifier must (also) not be observable in ls, and

    ⋆3 hi″ must be the identifier of a(nother) hub in hs.
21. If the command is of the form 1oldH1newH(hi,l,h) then

    ⋆1 hi must be the identifier of a hub in hs,

    ⋆2 l must not be in ls and its identifier must (also) not be observable in ls, and

$\star$3 h must not be in hs and its identifier must (also) not be observable in hs.

22. If the command is of the form 2newH(h′,l,h″) then

  $\star$1 h′ — left to the reader as an exercise (see formalisation !),

  $\star$2 l — left to the reader as an exercise (see formalisation !), and

  $\star$3 h″ — left to the reader as an exercise (see formalisation !).

```
value
 19′  pre_int_Insert: Ins → N → Bool
 19″  pre_int_Insert(Ins(op))(hs,ls) ≡
 ⋆2     s_l(op)∉ ls ∧ obs_LI(s_l(op)) ∉ iols(ls) ∧
        case op of
 20       2oldH(hi′,l,hi″) → {hi′,hi″}⊆iohs(hs),
 21       1oldH1newH(hi,l,h) → hi ∈ iohs(hs)∧h∉ hs∧obs_HI(h)∉ iohs(hs),
 22       2newH(h′,l,h″) → {h′,h″}∩ hs={}∧{obs_HI(h′),obs_HI(h″)}∩ iohs(hs)={}
        end
```

- These must be **carefully** expressed and adhered to
- in order for staff to be said to carry out the link insertion operation **accurately**.

[Domain Engineering, Domain Facets, Human Behaviour]

Example 19: A Sloppy via Delinquent to Criminal Operation

- We replace systematic checks ($\wedge$) with partial checks ($\vee$), etcetera,
- and obtain various degrees of **sloppy** to **delinquent**, or even **criminal** behaviour.

```
value
19′  pre_int_Insert: Ins → N → Bool
19″  pre_int_Insert(Ins(op))(hs,ls) ≡
⋆2     s_l(op)∉ ls ∧ obs_LI(s_l(op)) ∉ iols(ls) ∧
      case op of
20        2oldH(hi′,l,hi″) → hi′ ∈ iohs(hs)∨hi″isin iohs(hs),
21        1oldH1newH(hi,l,h) → hi ∈ iohs(hs)∨h∉ hs∨obs_HI(h)∉ iohs(hs),
22        2newH(h′,l,h″) → {h′,h″}∩ hs={}∨{obs_HI(h′),obs_HI(h″)}∩ iohs(hs)={}
      end
```

[Domain Engineering, Domain Facets]

Dialectics

- So now you should have a practical and technical "feel" for domain engineering:
  - ⋆ What it takes to express a domain model.
- But there is lots' more: We have not shown you
  - ⋆ (i) the rôle of domain stakeholders:
    - ◇ (i.1) how to identify them,
    - ◇ (i.2) how to involve them and
    - ◇ (i.3) how they help validate resulting domain descriptions.
  - ⋆ (ii) the domain (ii.1) knowledge acquisition and (ii.2) analysis processes,
  - ⋆ (ii) the domain (ii.1) model verification and (ii.2) validation and processes, and
  - ⋆ (iii) the domain theory R&D process.

- Can we agree that we cannot,
  - ⋆ as professional software engineers,
  - ⋆ start on gathering requirements,
  - ⋆ let alone prescribing these
  - ⋆ before we have understood the domain ?
- Can we agree that, "ideally", we must therefore
  - ⋆ first R&D the domain model
  - ⋆ before we can embark on any requirements prescription process ?
- By "ideally" we mean the following:
  - ⋆ Ideally domain engineering should fully precede requirements engineering,
  - ⋆ but for many practical reasons we must co-develop domain descriptions "hand-in-hand" with requirements prescriptions.
  - ⋆ And that is certainly feasible, when done with care.
  - ⋆ So we shall, for years assume this to be the case.

[Domain Engineering, Domain Facets]

Pragmatics

- While the software industry “humps along”:
  - ⋆ co-developing domain descriptions and requirements
  - ⋆ with their clients, or, for COTS, with their marketing departments,
- private and public research centres should and will embark on
  - ⋆ large scale (5–8 manyears/year),
  - ⋆ long range projects (5–8 year)
  - ⋆ foundational research and development (R&D) of

infrastructure component domain models of

- ⋆ **the financial service industry:**
  - ◇ banking (all forms);
  - ◇ insurance (all forms);
  - ◇ portfolio management;
  - ◇ securities trading:
    - ○ brokers,
    - ○ traders,
    - ○ commodities and
    - ○ stock etc. exchanges;
- ⋆ **transportation:**
  - ◇ road,
  - ◇ rail,
  - ◇ air, and
  - ◇ sea;
- ⋆ **healthcare:**
  - ◇ physicians,
  - ◇ hospitals,
  - ◇ clinics,
  - ◇ pharmacies, etc.;
- ⋆ **"the market":**
  - ◇ consumers,
  - ◇ retailers,
  - ◇ wholesalers, and
  - ◇ the supply chain;
- ⋆ **etcetera.**

Requirements Engineering

- We cannot possibly,
  - ⋆ within the confines of a seminar talk
  - ⋆ and a reasonably sized paper
- cover, however superficially,
  - ⋆ both informal
  - ⋆ and formal

examples of requirements engineering.

- Instead we shall just briefly mention the major stages and sub-stages of requirements modeling:
  - ⋆ **Domain Requirements:** those which can be expressed sôlely using terms from the domain description;
  - ⋆ **Interface Requirements:** those which can be expressed using terms both from the domain description and from IT; and
  - ⋆ **Machine Requirements:** those which can be expressed sôlely using terms from IT.

IEEE Definition of Requirements

- ⋆ By IT requirements we understand (cf. IEEE Standard 610.12):
  - ◇ *"A condition or capability needed by a user to solve a problem or achieve an objective on a computing machine".*

- By computing **machine** we shall understand a, or the, combination of computer (etc.) **hardware** and **software** that is the target for, or result of the required computing systems development.

[Requirements Engineering]

Domain Requirements

Domain Requirements

- By *domain requirements*
  - ⋆ we mean such which can be expressed
  - ⋆ sôlely using terms from the domain description

- To construct the domain requirements
  - ⋆ the domain engineer
  - ⋆ together with the various groups of requirements stakeholder

  "apply" the following "domain-to-requirements" operations
  to a copy of the domain description:

  - ⋆ **projection**,
  - ⋆ **instantiation**,
  - ⋆ **determination**,
  - ⋆ **extension** and
  - ⋆ **fitting**.

- First we briefly charaterise these.

[Requirements Engineering, Domain Requirements]

The Domain-to-Requirements Operations

- The ‘domain-to-requirements’ operations cannot be automated.
- They increasingly “turn” the copy of the domain description into a domain requirements prescription.

Projection

removes the domain phenomena and concepts for which the customer does not need IT support.

Simple Linear Road: Projection

Our requirements is for a simple road: a linear sequence of links and hubs:

```
type
  N, L, H, LI, HI
value
  obs_Hs: N → H-set, obs_Ls: N → L-set
  obs_HI: H → HI, obs_LI: L → LI
  obs_HIs: L → HI-set, obs_LIs: H → LI-set
axiom
  See Items 5–8 Pages 21–21
```

Instantiation

makes a number of entities: *simple, operations, events and behaviours*, less abstract, more concrete.

Simple Linear Road: Instantiation

The linear sequence consists of eaxtly 34 links.

```
type
   H, L,
   $N' = H \times (L \times H)^*$
   $N'' = \{|n{:}N' \bullet wf(n)|\}$
value
   wf_N'': $N' \to$ Bool
   wf_N''(h,(l,h)^lhl) ≡
      len lhl = 33 ∧
      obs_Hl(l)=obs_Hl(h) ∧
      ∀ i,j:Nat • {i,i+1,j}⊆inds lhl ⇒
         let (li,hi)=lhl(i),(li',hi')=lhl(i+1),(lj,hj)=lhl(j) in
         h≠hi∧i≠j⇒li≠lj∧hi≠hj∧
         obs_HIs(li')={obs_HI(hi),obs_HI(hi')}∧
         obs_LIs(hi)∩ obs_LI(li)≠{}∧obs_LIs(hi')∩ obs_LI(li')≠{} end
   obs_N: $N'' \to N$
   obs_N(h,lhl) ≡
      ({h}∪{hi|(hi,li):(L×H)•(hi,li)∈ elems lhl},
            {li|(hi,li):(L×H)•(hi,li)∈ elems lhl})
```

wf_N' secures linearity; obs_N allows abstraction from more concrete N'' to more abstract N.

Determination

makes the emerging requirements entities more determinate.

Simple Linear Road: Determination

All links and all non-end hubs are open in both directions; we leave end-hub states undefined — but see below, under ‘Extension’.

```
type
  $L\Sigma$ = (HI$\times$HI)-**set**, $L\Omega$
  $H\Sigma$ = (LI$\times$LI)-**set**, $H\Omega$
value
  obs_$L\Omega$: L $\rightarrow$ $L\Omega$
  obs_$H\Omega$: H $\rightarrow$ $H\Omega$
axiom
  $\forall$ (h,$\langle$(l1,h2)$\rangle$$^\frown$lhl):N$''$ •
    obs_$L\Sigma$(l1)={obs_HI(h),obs_HI(h2)}$\wedge$
    $\forall$ i,i+1:**Nat** • {i,i+1}$\subseteq$**inds** lhl $\Rightarrow$
      **let** (li,hi)=lhl(i),(li$'$,hi$'$)=lhl(i+1),(lj,hj)=lhl(j) **in**
      obs_$L\Omega$(li$'$)={{(obs_HI(hi),obs_HI(hi$'$)),(obs_HI(hi$'$),obs_HI(hi))}}$\wedge$
      obs_$H\Omega$(hi)={{(obs_LI(li),obs_LI(li$'$)),(obs_LI(li$'$),obs_LI(li))}} **end**
```

The last two lines of the axiom express that links are always open two ways and that hubs are always open for through traffic.

Extension

introduces new, computable entities that were not possible in the non-IT domain.

Simple Linear Road: Extension

We extend the model of linear roads by introducing the concept of a Hub-Plaza: this is an area “around” each hub from where and into where there is always access onto, respectively from the hub:

```
type
   HP, HPI
   $H\Sigma' = (LI \times LI)\textbf{-set} \cup (LI \times HPI)\textbf{-set} \cup (HPI \times LI)\textbf{-set}$
   $H\Omega' = H\Sigma'\textbf{-set}$
value
   $obs\_H\Omega'$: $H \to H\Omega'$
   obs_HP: $H \to HP$
   obs_HPI: $HP \to HPI$
axiom
   $\forall$ h,h':H • $h \neq h' \Rightarrow$ obs_HP(h)$\neq$obs_HP(h')$\wedge$obs_HPI(obs_HP(h))$\neq$obs_HPI(obs_HP(h'))
   $\forall$ (h,(l,h)$^\frown$lhl):N'' •
      $\forall$ i,j:Nat • {i,i+1,j}$\subseteq$inds lhl $\Rightarrow$
         let (li,hi)=lhl(i),(li',hi')=lhl(i+1),(lj,hj)=lhl(j) in
         $obs\_H\Omega'$(h)={{(obs_LI(l),obs_HPI(obs_HP(h))),(obs_HPI(obs_HP(h)),obs_LI(l))}}
         $\forall$ i,i+1:Nat • {i,i+1}$\subseteq$inds lhl $\Rightarrow$
            let (_,hi)=lhl(i),(_,hi')=lhl(i+1),(_,hj)=lhl(j) in
            $obs\_H\Omega'$(hi)={{(obs_LI(li),obs_LI(li')),(obs_LI(li'),obs_LI(li)),
                           (obs_HPI(obs_HP(hi)),obs_LI(li)),(obs_HPI(obs_HP(hi)),obs_LI(li'))
                           (obs_LI(li),obs_HPI(obs_HP(hi))),(obs_LI(li'),obs_HPI(obs_HP(hi)))}}
            end end
```

The $obs\_H\Omega'$ lines of the axiom with respect to that of ‘Determination’ express plaza access.

Fitting

merges the domain requirements prescription with those of other IT developments.

• • •

The domain requirements examples are necessarily “microscopic”.
The very briefly outlined domain requirements methodology has many fascinating aspects.

[Requirements Engineering]

Interface Requirements

Interface Requirements

- By *interface requirements*
  - ⋆ we mean such which those which can be expressed using terms
  - ⋆ from both the domain description and from IT,
  - ⋆ that is, terminology of hardware and of software.

- When phenomena and concepts of the domain
  - ⋆ are also to be represented by the machine,
  - ⋆ these phenomena and concepts are said to be **shared** between the domain and the machine;
  - ⋆ the requirements therefore need be expressed both
    - ◇ in terms of phenomena and concepts of the domain and
    - ◇ in terms of phenomena and concepts of the machine.

[Requirements Engineering, Interface Requirements]

Shared Phenomena and Concepts

- A shared phenomenon or concept is either
  - ⋆ a simple entity,
  - ⋆ an operation,
  - ⋆ an event or
  - ⋆ a behaviour.

- **Shared simple entities** need
  - ⋆ to be initially input to the machine and
  - ⋆ their machine representation need to be
  - ⋆ regularly, perhaps real-time refreshed.
- **Shared operations** need
  - ⋆ to be interactively performed by
  - ⋆ human or other agents of the domain
  - ⋆ and by the machine.

[Requirements Engineering, Interface Requirements, Shared Phenomena and Concepts]

- **Shared events** are shared in the sense that
  - ⋆ their occurrence in the domain (in the machine)
  - ⋆ must be made known to the machine (to the domain).
- **Shared behaviours** need
  - ⋆ to occur in the domain and in the machine
  - ⋆ by alternating means,
  - ⋆ that is, a protocol need be devised.

- For each of these four kinds of interface requirements
  - ⋆ the reqs. engineers work with the reqs. stakeholders
  - ⋆ to determine the properties of these forms of sharing.
- These interface requirements are then narrated and formalised.
- They are always "anchored" in specific items of the domain description.

• • •

The very briefly outlined interface requirements methodology has many fascinating aspects.

[Requirements Engineering]

Machine Requirements

Machine Requirements

- By *machine requirements*
  - ⋆ we mean those which can be expressed
  - ⋆ sôlely using terms from the machine,
  - ⋆ that is, terminology of hardware and of software.

- We shall not cover any principles or techniques for developing machine requirements,
- but shall just list the very many issues that must be captured by a machine requirements.

[**Requirements Engineering**, **Machine Requirements**]

- Performance
  - ⋆ Storage
  - ⋆ Time
  - ⋆ Software Size
- Dependability
  - ⋆ Accessibility
  - ⋆ Availability
  - ⋆ Reliability
  - ⋆ Robustness
  - ⋆ Safety
  - ⋆ Security
- Maintenance
  - ⋆ Adaptive
  - ⋆ Corrective
  - ⋆ Perfective
  - ⋆ Preventive
- Platform (P)
  - ⋆ Development P
  - ⋆ Demonstration P
  - ⋆ Execution P
  - ⋆ Maintenance P
- Documentation Requirements
- Other Requirements

- The machine requirements are usually not so easily, formalised, if at all, with today's specification language tools.
- Extra great care must therefore be exerted in their narration.
- Some formal modelling calculations, like fault (tree) analysis, can be made in order to justify quantitative requirements.

Why “Current” Requirements Engineering (RE) Seems Flawed

- Current, conventional requirements engineering has no scientific basis.
  - ⋆ The requirements engineering sketched in this paper starts with a domain model.
  - ⋆ The domain model provides the scientific basis.
  - ⋆ “Derivation” of domain and interface requirement provides a further scientific basis.
  - ⋆ The fact that the requirements engineering models advocated in this paper also are formalised provides a final scientific basis.

[**Why "Current" Requirements Engineering Seems Flawed**]

- The separation of concerns:
  - ⋆ (the formalised) domain model, in-and-by-itself, and
  - ⋆ the (the formalised) requirements projection, instantiation, determination, extension and fitting operations

  provide a basis for scientific analysis.
- Current, conventional RE does not have these bases.
- If we are to pursue Software Engineering in a professionally responsible manner then requirements engineering must be pursued in a scientifically responsible manner.

Conclusion

Summary — A Wrap Up

- We have illustrated the triptych concept:
  - ⋆ from domains via requirements to software.
- We spent most time on domain engineering.
- We just sketched major requirements engineering concepts.
- Enough, we think, to cast doubt on current requirements engineering:
  - ⋆ studies and
  - ⋆ practice.
- And we assumed you know how to turn formal requirements into correct software designs !

[Conclusion]

Dialectics

- So, are we clear on this:
  1. That we must understand the domain before we express the requirements ?
  2. That we can "derive" major parts of the requirements prescription from the domain description ?
  3. That domains are far more "stable" than requirements ?
  4. That prescribing requirements with no prior domain description is unsound ?
  5. That describing [prescribing] domains [requirements] both informally (narratives) and formally (formal specifications) helps significantly towards consistent specifications ?
  6. That we must therefore embrace the triptych: from domains via requirements to software ?

Acknowledgements

- Thanks to Michael Reichhardt Hansen for inviting me to NWPT.
- Thanks to NWPT for fundimng my travel (Edinburgh–Copenhagen return).
- Thanks for your patience.

Questions ?