Topic 47

Domain Verification and Validation

- The **prerequisite** for following this (part of the) lecture is that you have a reasonable grasp of the previous stages of domain engineering: from domain acquisition, via analysis and concept formation, to domain description (i.e., domain modelling).
- The **aims** are
  - ⋆ to briefly introduce the concepts of domain verification (including model checking and testing) and validation, and
  - ⋆ to cover some of the attendant principles and techniques.

- The **objective** is
  - ⋆ to complete your education and training so as to become a professional domain engineer.
- The **treatment** is informal.

The Right Domain — The Domain Right

- Domain Validation: Validate to get the right domain.
- Domain Verification: Verify (model check, test) to get the domain right.

Introduction

- Let us first review where we are in the process of describing the domain development process and its method principles and techniques:
  - ⋆ (i) First we focused on the core aspects of domain modelling: The “whats” and “hows” of a domain model. We could call this the “production technology”.
    - ⋄ (i.1) We covered the concepts of abstraction of phenomena and concepts, and
    - ⋄ (i.2) the attributes and facets of what is being described in domain models.
    - ⋄ (i.3) We covered, in between, the issues of stakeholders and their perspectives.
  - ⋆ That coverage explained “what” a domain model should contain, the abstractions possible, the facets “mirrored”, and — notably — with respect to the stakeholders and the perspectives to be dealt with.

- (ii) Then we focused more on “how”. In contrast to “production technology” we could call this “how” the “process technology”.
  - ⋆ (ii.1) First, we focused on the process, principles and techniques of domain acquisition, that which “begins” the domain development work.
  - ⋆ (ii.2) Then we covered the process, principles and techniques of domain analysis and concept formation.
- After domain acquisition, domain analysis and concept formation follows the domain modelling proper.
  - ⋆ Finally, we focus on domain validation and verification — the topic of this lecture.
- The purpose of the above review has been to put
  - ⋆ the somehow “reverse” ordering of the previous lectures “straight”
  - ⋆ with respect to the ordering of the domain development processes.

- We can now summarise the domain development process (even before we have covered the notions of verification and validation).
  - ⋆ After producing the appropriate informative documents:
    - ⋄ needs and ideas, concepts, scope and span, synopsis, and contracts,
  - ⋆ one proceeds to identifying domain stakeholders and establishing liaison with members of domain stakeholder groups.
  - ⋆ Then we move on to domain acquisition:
    - ⋄ interviews, studies, questionnaire formulation and domain stakeholders’ replies to these, ending wit domain description unit indexing and an elicitation report.
  - ⋆ This acquisition is followed by domain analysis and concept formation.
  - ⋆ Then we do the actual domain modelling.
  - ⋆ And, finally, we perform domain verification and validation.

Domain Verification

In this lecture (as we shall also do in in a later lecture on requirements validation and verification) we use the term verification to also cover the concepts of model checking and testing.

Characterisation 14.200 By *domain verification* we shall understand

- a process, and the resulting (analytic) documents,
- in which some domain descriptions
- are being analysed in order to ascertain whether what is being described
- satisfies certain (claimed or otherwise expected) properties

. ■

- So what — really — is the difference between domain validation and domain verification?
  - ⋆ In validation we examine the domain model to make sure we are modelling what the domain stakeholders think that domain is: *Validation gets the right domain model.*
  - ⋆ In verification we examine whether our domain model “hangs together,” such as the domain engineers want it to be: *Verification gets the domain model right.*
- Verification is adjoint to validation:
  - ⋆ Both validation and verification are needed.
  - ⋆ Usually verification precedes validation.

- Verification work typically proceeds as follows:
  - ⋆ Desired properties of the domain model — properties that do not transpire immediately from the domain description —
  - ⋆ are formulated, informally or formally.
  - ⋆ Then
    - ⋄ “proofs” by “verbal” arguments,
    - ⋄ or some form of symbolic testing,
    - ⋄ or formal proofs,
    - ⋄ or model checking,
  - ⋆ are performed in order to check that the desired property holds of the domain model.

- So verification, to us, includes, rearranging the terms a bit,
  - ⋆ informal reasoning:
    - ◇ "proofs" by "verbal" arguments and
    - ◇ testing;
  - ⋆ formal reasoning:
    - ◇ formal proofs and
    - ◇ model checking.
  - ⋆ By informal reasoning we shall, however, mean "proofs" by "verbal" arguments.

Informal Reasoning

Characterisation 14.201 By *informal reasoning* we shall understand

- a carefully phrased
- series of arguments,
- which, as a whole,
- convinces an audience of the validity of what is concluded

. ■

- Human beings often reason,
- but are not always careful in doing so.
- Informal reasoning demands great care.

Testing

Characterisation 14.202 By *testing* we shall understand

- that a domain description is
- provided with set values for all relevant arguments (the test data),
- with the description then being evaluated ("executed") for those arguments.
- The test then results in a "final value" of the description for those arguments

. ■

- Such a "final value" may be a complicated quantity.
- Typical final values could be
  - ⋆ an execution sequence, or a trace of description points,
  - ⋆ with a set of variable values for each step in the sequence (i.e., a trace).

- In another way of phrasing it:
  - ⋆ Testing is a systematic search for a counterexample
  - ⋆ to a claim (or proof) of correctness.
- Testing, till recently, has basically been a heuristics-based science.
- An important part of testing is text analysis.
- If domain description parts have been formalised, then theory-based testing technologies have been or can be developed and can be used for testing.

Formal Proofs

Characterisation 14.203 By a *formal proof* we shall understand

- a given domain description,
- a statement (a theorem) to be proved and
- a proof that the domain description satisfies the statement:
  - ⋆ This proof refers to a proof system for the language in which the domain description is expressed (axioms and inference rules),
  - ⋆ and is otherwise a sequence, composed from steps,
  - ⋆ where each step in the sequence is like a theorem (a lemma), a statement, and
  - ⋆ where pairs of steps in the proof sequence are related, i.e., are justified, by the axioms and the inference rules

. ■

Model Checking

Characterisation 14.204 By *model checking* we shall understand

- *a method for formally verifying usually concurrent systems,*
- *whose usually extremely large, practically speaking infinite state systems,*
- *have been reduced to manageable finite-state systems.*

- We augment this characterisation by the following:
  - ⋆ In model checking a somehow executable abstraction of the thing to be checked is programmed.
  - ⋆ That model is then subject to certain forms of executions in which specified properties are checked.
  - ⋆ These executions, for example, check whether the model is able to enter certain states or not

. ■

- Domain descriptions about such finite-state systems are typically expressed as temporal logic formulas.
- Efficient symbolic algorithms are used
  - ⋆ to traverse the (state machine) model defined by the system
  - ⋆ and to check if the domain description holds or not,
  - ⋆ i.e., whether the model execution "enters" appropriate states,
  - ⋆ albeit for a "reduced" set of possible states of systems.
- Extremely large state-spaces can often be traversed in minutes.

Domain Validation

Characterisation 14.205 By *domain validation* we shall understand

- a process, and the resulting (analytic) documents,
- in which some domain descriptive documents are being coinspected by domain stakeholders and domain engineers, and
- in which whatever is being described
  - ⋆ is being positively and/or negatively reviewed
    - ◇ with reference to the elicitation report and
    - ◇ with respect to whatever the stakeholders might now realise about their domain.

- ⋆ This includes pointing out, if necessary,
  - ◇ inconsistencies,
  - ◇ incompletenesses,
  - ◇ conflicts and
  - ◇ errors of description
- ⋆ that may change the elicitation report

. ■

- Domain validation is possibly interwoven with domain verification work — more on this later in the lecture.

OFTWARE ENGINEERING: Domains, Requirements and Software Design Volume 3
4.3.1 The Domain Validation Documents
home/db/volIII/3ch14/3ch14 April 5, 2006, 11:33 Page 1386, Topic: 47, Foil: 20
Department of Computer Science and Engineering
Institute of Informatics and Mathematical Modelling
Technical University of Denmark
Richard Petersens Plads, DK-2800 Kgs.Lyngby, Denmark
DTU

The Domain Validation Documents

- In order to perform domain validations, the validators need the following (input) documents:
  - ⋆ the list of domain stakeholders;
  - ⋆ the domain acquisition documents:
    - ◇ questionnaire,
    - ◇ and the collection of indexed description units;
  - ⋆ the rough-sketch, terminology, narrative, and possibly — if produced — the formalisation documents that constitute the domain description proper;
  - ⋆ and the domain analysis and concept formation documents.
  - ⋆ That is, the validators need access to basically all documents produced (so far) in the domain modelling effort.

TWARE ENGINEERING: Domains, Requirements and Software Design Volume 3
1 The Domain Validation Documents
e/db/volIII/3ch14/3ch14 April 5, 2006, 11:33 Page 1387, Topic: 47, Foil: 21
Department of Computer Science and Engineering
Institute of Informatics and Mathematical Modelling
Technical University of Denmark
Richard Petersens Plads, DK-2800 Kgs.Lyngby, Denmark
DTU

- In order to complete domain validation, the validators produce the following (output) documents:
  - ⋆ a possibly updated domain stakeholder document;
  - ⋆ possibly updated domain acquisition documents;
  - ⋆ possibly updated rough sketches, terminology, narrative, and — if relevant — the formalisation documents;
  - ⋆ possibly updated domain analysis and concept formation documents; and
  - ⋆ a domain validation report.
- We now cover some aspects of the necessarily informal validation process.

OFTWARE ENGINEERING: Domains, Requirements and Software Design Volume 3
4.3.2 The Domain Validation Process
home/db/volIII/3ch14/3ch14 April 5, 2006, 11:33 Page 1388, Topic: 47, Foil: 22
Department of Computer Science and Engineering
Institute of Informatics and Mathematical Modelling
Technical University of Denmark
Richard Petersens Plads, DK-2800 Kgs.Lyngby, Denmark
DTU

The Domain Validation Process

- Domain validation proceeds as follows:
  - ⋆ Domain engineers "sit together" with stakeholders and review, line by line, the domain model,
  - ⋆ holding it up against the previously elicited domain description units,
  - ⋆ while then noting down any discrepancies.

TWARE ENGINEERING: Domains, Requirements and Software Design Volume 3
2 The Domain Validation Process
e/db/volIII/3ch14/3ch14 April 5, 2006, 11:33 Page 1389, Topic: 47, Foil: 23
Department of Computer Science and Engineering
Institute of Informatics and Mathematical Modelling
Technical University of Denmark
Richard Petersens Plads, DK-2800 Kgs.Lyngby, Denmark
DTU

- In doing domain validation, domain stakeholders usually read the informal, yet precise and detailed narrative descriptions.
- No assumption is made as to their ability to read formalisations.
- On the contrary: It is assumed that they cannot read formal specifications.
- For reasonably large-scale projects the customer may hire professional consultants who can also study the formalisations.
- This is just like future ship owners hiring Lloyd's Register of Shipping to check ship designs in preparation for insurance companies to take on insurance risks.

OFTWARE ENGINEERING: Domains, Requirements and Software Design Volume 3
4.3.2 The Domain Validation Process
home/db/volIII/3ch14/3ch14 April 5, 2006, 11:33 Page 1390, Topic: 47, Foil: 24
Department of Computer Science and Engineering
Institute of Informatics and Mathematical Modelling
Technical University of Denmark
Richard Petersens Plads, DK-2800 Kgs.Lyngby, Denmark
DTU

- Domain validation (and verification) ends with a signed domain validation (and verification) report.
  - ⋆ This report either OKs the domain model, or
  - ⋆ points out required corrections
    - ◇ in the elicitation report,
    - ◇ in the domain analysis and concept formation report, and
    - ◇ in the domain model.

TWARE ENGINEERING: Domains, Requirements and Software Design Volume 3
3 Domain Development Iterations
e/db/volII/3ch14/3ch14 April 5, 2006, 11:33 Page 1391, Topic: 47, Foil: 25
Department of Computer Science and Engineering
Institute of Informatics and Mathematical Modelling
Technical University of Denmark
Richard Petersens Plads, DK-2800 Kgs.Lyngby, Denmark
DTU

Domain Development Iterations

- Thus domain validation (and verification) can be an iterative process, alternating possibly with
  - ⋆ further domain verification,
  - ⋆ further elicitation report work,
  - ⋆ further domain analysis and concept formation work,
  - ⋆ and with further domain modelling work.
- The domain validation process may end with further domain validation (and verification) work.

Discussion
General

- We have treated aspects of domain validation and verification — in the same lecture since they relate in many ways.
- And we have used the term verification, primarily to stand for formal proofs, but, secondarily, also for model checks and tests.

TWARE ENGINEERING: Domains, Requirements and Software Design Volume 3
2 Principles, Techniques and Tools
e/db/volII/3ch14/3ch14 April 5, 2006, 11:33 Page 1393, Topic: 47, Foil: 27
Department of Computer Science and Engineering
Institute of Informatics and Mathematical Modelling
Technical University of Denmark
Richard Petersens Plads, DK-2800 Kgs.Lyngby, Denmark
DTU

Principles, Techniques and Tools

- We summarise:

Principle 14.77 *Domain Validation:* To ensure that the domain described is the right domain. ■

Principle 14.78 *Domain Verification:* To uncover a domain theory, i.e., to get the domain descriptions right. ■

Techniques 55 *Domain Validation:* In summary, human, collaborative document inspection. ■

OFTWARE ENGINEERING: Domains, Requirements and Software Design Volume 3
4.4.2 Principles, Techniques and Tools
home/db/volII/3ch14/3ch14 April 5, 2006, 11:33 Page 1394, Topic: 47, Foil: 28
Department of Computer Science and Engineering
Institute of Informatics and Mathematical Modelling
Technical University of Denmark
Richard Petersens Plads, DK-2800 Kgs.Lyngby, Denmark
DTU

Techniques 56 *Domain verification* techniques,

- based on formal descriptions, include those that enable
  - ⋆ formal verification (of posed lemmas and theorems),
  - ⋆ model checking, and
  - ⋆ tests,

while domain verification techniques,

- based on informal descriptions, basically amount to
  - ⋆ informal, concise reasoning

. ■

TWARE ENGINEERING: Domains, Requirements and Software Design Volume 3
2 Principles, Techniques and Tools
e/db/volII/3ch14/3ch14 April 5, 2006, 11:33 Page 1395, Topic: 47, Foil: 29
Department of Computer Science and Engineering
Institute of Informatics and Mathematical Modelling
Technical University of Denmark
Richard Petersens Plads, DK-2800 Kgs.Lyngby, Denmark
DTU

Tools 14.19 Since *domain validation* is basically an informal process, the tools are those that support

- document cross-referencing between domain description units and narrative domain descriptions and domain terminologies,
- and data mining based on such documents

. ■

OFTWARE ENGINEERING: Domains, Requirements and Software Design Volume 3
4.4.2 Principles, Techniques and Tools
home/db/volII/3ch14/3ch14 April 5, 2006, 11:33 Page 1396, Topic: 47, Foil: 30
Department of Computer Science and Engineering
Institute of Informatics and Mathematical Modelling
Technical University of Denmark
Richard Petersens Plads, DK-2800 Kgs.Lyngby, Denmark
DTU

Tools 14.20 *Domain verification*

- based on formal descriptions requires such tools as, for example,
  - ⋆ proof assistants and theorem provers,
  - ⋆ model checkers, and
  - ⋆ test generators and tester monitors;

whereas domain verification

- based on informal descriptions basically requires
  - ⋆ human reasoning

. ■