Specifying; a formality?

ir. Erik Jan Marinissen

On November 11th, a half-day symposium was organized on the occasion of the fifth anniversary of OOTI. The topic of the afternoon was formal specification methods (FSMs). There were about 200 participants, many from OOTI and Eindhoven University, but also a substantial percentage of external visitors.

After a buffet lunch, the afternoon started with a welcome by prof.dr. Stan Ackermans, director of the Eindhoven Institute of Postgraduate Studies (IVO). He underlined the importance of Computing Science by looking at the three key entities in technological design: matter, energy, and information. The role of both matter and energy has been known since the invention of the steam engine. Information, however, was added to this pair only a few decades ago. Computing Science is the science that studies the role of this newly discovered entity in the process of technological design.

Opening

After this welcome, the symposium was formally opened by prof.dr. Wisse Dekker. Although chairman-for-the-day prof. S.J. Doorman M.Sc. emphasized Dekker's professorship at Leiden University in his announcement, Dekker is in the first place known as ex-president and now president commissioner of Philips Electronics. That this has made him a Dutch celebrity was noticeable by the number of photographers active during his presentation.

Dekker's speech was well-prepared and to-the-point; in my opinion it was the best one of the afternoon. Confirming what Ackermans had said earlier, he stated that postgraduate designer courses had started five years ago ordered in response to a need in the industry. Large companies in particular were afraid that students graduating from the first phase (which had just been reduced to four years) would not meet their needs for high-quality, multi-disciplinary technological designers. According to Dekker, Philips and the rest of the industry are quite satisfied with the results of the second-phase courses. This is also apparent in the fact that graduates from these courses have no difficulty in finding employment. Dekker assumed that a lot of small and medium-sized companies are still unfamiliar with this new phenomenon in the Dutch academic education system. This could imply an even larger, but still latent, demand for this kind of graduate.

Dekker during his opening address (Photo: Eindhoven University of Technology, Stafgroep Reproduktie en Fotografie)

At the end of his talk Dekker had some concrete recommendations for OOTI. He made a strong plea for quality rather than quantity in the graduates of OOTI. One of the ways of helping to keep the output quality up would be, in his opinion, to stick to a strict input selection. "The second phase was meant only for the best students and it should stay that way." Based on the needs of the industry, Dekker also stressed the importance of learning to work in (multi-disciplinary) teams. (This is already one of the features of OOTI - EJM) He supported one of the conclusions of the CCTO (Dutch Certification Commission for courses for Technological Designer) that the OOTI programme needs more attention to business economics aspects and cost awareness. Finally Dekker expressed his belief that even if the first phase is expanded back to five years, there will stay a demand for peo-

ple from a postgraduate designers course such as OOTI.

Can everyone specify?

Drs. Frans Remmen, formerly lecturer at the Department of Computing Science at Eindhoven University and until recently director of Remmen & De Brock, was the first technical speaker. He stated that the growing complexity of information systems has created a growing and clearly felt need to specify those systems before implementing them. Opinion is divided on the question of who should make these specifications. Remmen distinguished two mainstreams here. One group of people believe that specifications should be made by the users of the future system. They are the experts in the application domain and have the best knowledge of their own needs and wishes. The other mainstream thinks that specifying is an activity which requires specialists in the specification area, the system experts. Remmen does not agree with either view. The first one leads to *structurally inoperative* systems, whereas the second results in *structurally inappropriate* systems. The solution lies, according to Remmen, in the deployment of ''real professionals''. In his definition these are people who combine a high capacity for abstraction (needed to separate the essential from the inessential) and a strong capacity for mathematical modelling with an ability to communicate well with end users about their requirements and wishes. To acquire these capacities, a thorough education in computing science is a necessity. The education programme should pay attention to both technical and mathematical aspects as well as inter-personal communication.

By chosing this position Remmen answered his own question. ''It is far from begin true that everyone can specify.'' This is work for ''real professionals''. The idea of 'specifying for the masses' does not come closer by using more powerful models (object-oriented approach) or software tools. On the contrary, they require an even higher level of professionalism to keep a critical overview on them. And those professionals are trained by high-quality computer science courses as OOTI.

Do FSMs help to beat the competitors?

The next speaker, ir. Jaap van 't Ooster, was invited as an exponent of Dutch industry. He heads one of the R&D departments of Oce-Van de Grinten. This Venlo-based company is active in the office and drawing office market (copiers, printers, and plotters). Computing science is one of the many disciplines (chemistry, physics, mechanics, electrical engineering) that are involved in the development of their new products.

After a rather long introduction of his company, Van 't Ooster described how computing science in Oce has moved from assembler programming via structured programming in Pascal to structured design with the Yourdan method and Craddle tools. Oce is interested in using formal specification tools in their software design process. The advantages they expect are the following.

- Proofs of correctness for reusable building blocks.
- High-level description language, independent of the implementation.
- Automatic code generation in various programming languages.
- Automatic generation of test specifications.
- Specifications that are more understandable by laymen.

Several groups within Oce have experimented with the use of FSMs. Till now those methods have not found a wide use in the company. According to Van 't Ooster the main reason for this is that FSMs tend to pay off only after a longer period. The project-oriented character of R&D within Oce makes it difficult to wait for those long-term benefits. In order to apply a FSM successfully, a long learning process is required. Sending all project members to a course is not enough. Many methods are not accessible to the average engineer (Van 't Ooster mentioned VDM). Reduction in test time could be a concrete selling point of FSMs, but at many project start-ups, even this is too far away to decide to base the entire project on such a FSM.

For the future, Oce is monitoring developments in the areas of object-oriented analysis and design and formal specification languages. In the ESPRIT framework the language Lotos has been tried in Oce's product development. The conclusion of this work was that Lotos' application area (communication protocols) did not match with Oce's field of interest.

Specification: a scientific activity?

Dr. Mike Spivey of Oxford University has become an internationally known name in the area of formal specification with the publication of his reference manual for the Z notation. The symposium organizers had invited him as key note speaker. From this moment on, the symposium language changed from Dutch into English. In my opinion the half-heartedness of the organizing committee about languages was one of the very few minuses of the day. Either you think that the symposium visitors are not able to understand English (in my opinion not true) and then you do not invite an English speaker, or you think they can understand English and hence the entire symposium can be in English, even if only out of politeness to your key note speaker.

Spivey could have left the question mark out of his title. His speech was centered around the idea that writing a formal specification is like developing a scientific theory. He compared science with engineering. Scientists look for new models of physical reality, whereas engineers use known models in their designs. Formal specification is more like science than like engineering. Spivey: "Tentative fragments of formal specifications play the part of scientific hypotheses, which are open to testing by experiment, by examining them for consistency with the rest of the specification, or by comparing them with known facts about the system being described. Like a good scientific theory, a good specification expresses concise general principles that govern the entire behavior of a system."

Spivey named a handful of properties of a good scientific theory and their equivalents in the field of formal specifications. Throughout his talk he used a parallel between Newtonian mechanics (model of a scientific theory) and a software specification as a *running example* to demonstrate his thesis.

- *Abstraction.*
  The suppression of irrelevant detail. Every scientific theory models only that part of the physical reality relevant to the theory. In Newtonian mechanics, position and velocity of a body are modelled, but not color or temperature. Software specifications abstract from the reality of the implementation by using mathematical structures instead of concrete data structures.

- *Concise expression of general principles.*
  In Newtonian mechanics, an example of a general principle is the law of conservation of momentum. *Invariants* form the counter-

Discussion panel: f.l.t.r. Martin Diepstraten, Frans Remmen, Kees van Hee, S.J. Doorman, Mike Spivey, and Jaap van 't Ooster. (Photo: Eindhoven University of Technology, Stafgroep Reproduktie en Fotografie)

part of such conservation laws in software specifications.

- *Validation by experiment.*
  A scientific theory can be used to predict the behavior of a system in a new situation. The accuracy of such predictions depends on the theory. Mechanics can predict the motion of the planets. Likewise, a software specification can predict what the specified system must do in each situation.

- *Internal consistency.*
  Inconsistencies are a sign of a wrong or incomplete theory or specification.

Although coming from the academic world, Spivey has cooperated extensively with several industrial partners, which enables him to speak with practical experience. Where most people will at first think of specifying new systems, Spivey mentioned an industrial project in which an existing system was specified. This example concerned the CICS transaction processing system of IBM. With the help of the Oxford group, IBM has made the following pattern of work to enhance (parts of) the old and never formally specified implementation of the CICS system. Each time an old module has to be updated, first a formal specification of the module is written. That specification is extended with the new features. The modified specification is then used as the basis of a re-implementation of the entire module. This way of working proved to be successful for updating an old but established software product. What Spivey did not mention is that formally specifying an existing system (i.e., using known means to describe a known system) is already closer to engineering than it is to science.[1]

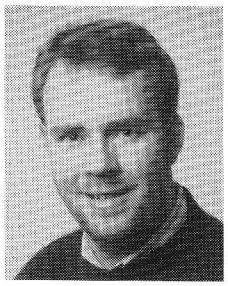
Discussion

After Spivey's presentation there was time for discussion. Under the inspiring guidance of prof. Doorman a panel discussed the use and implications of FSMs among themselves and with the audience. Two persons joined the three speakers in the panel. Prof.dr. Kees van Hee works at the Computing Science department of Eindhoven University, where he heads the group Information Systems. He is one of the driving forces behind ExSpect, a tool for making executable formal specifications. Drs. Martin Diepstraten is OOTI-graduate and currently working for FEL-TNO. His OOTI graduation project comprised the evaluation of several FSMs for the specification of the call processing part of a PABX.

The discussion among the panelists was rather tame, mainly due to the lack of opposite opinions. The questions coming from members of the audience brought in some liveliness, but most credit should be given to chairman Doorman for his often very humorous rephrasing of these questions.

Closure

Prof.dr. Martin Rem, chairman of the OOTI board, closed the symposium by evaluating the entire day. He revealed that the original idea for the theme of this day had not been FSMs, but ''Big Disasters in Computing Science''. A theme that surely would generate a broad interest (based on the idea that everybody loves to hear about other people's failures), but on second thought not appropriate to celebrate the first quinquennium of a course in computing science. One would rather hear about successes on a day like that. And so the second tentative title was found: ''Big Successes in Computing Science''. Rem created an unintended uproar in the audience when he said that this idea was also abandoned, mainly because no one could think of such 'big successes'. Finally, FSMs were chosen as the theme, because FSMs form a main point in the OOTI curriculum. Rem left the question open whether or not he thinks that FSMs fall in either one of the previously chosen titles for the symposium. □



Ir. Erik Jan Marinissen completed the post-masters programme Software Technology in 1992 and is currently working as member of the scientific staff of Philips Research Laboratories in Eindhoven. He is a member of XOOTIC *and co-editor of* XOOTIC MAGAZINE.

[1] More on Spivey's views on formal specifications can be found in an interview with him which starts at page 9 of this edition of XOOTIC Magazine.