

Formal Methods: From Academia to Industrial Practice A Travel Guide

Marieke Huisman

Department of Computer Science (FMT), UT, P.O. Box 217, 7500 AE Enschede, The Netherlands

Dilian Gurov

KTH Royal Institute of Technology, Lindstedtsvägen 3, SE-100 44 Stockholm, Sweden

Alexander Malkis

Department of Informatics (I4), TUM, Boltzmannstr. 3, 85748 Garching, Germany

17 February 2020

Abstract

For many decades, formal methods are considered to be the way forward to help the software industry to make more reliable and trustworthy software. However, despite this strong belief and many individual success stories, no real change in industrial software development seems to be occurring. In fact, the software industry itself is moving forward rapidly, and the gap between what formal methods can achieve and the daily software-development practice does not appear to be getting smaller (and might even be growing).

In the past, many recommendations have already been made on how to develop formal-methods research in order to close this gap. This paper investigates why the gap nevertheless still exists and provides its own recommendations on what can be done by the formal-methods-research community to bridge it. Our recommendations do not focus on open research questions. In fact, formal-methods tools and techniques are already of high quality and can address many non-trivial problems; we do give some technical recommendations on how tools and techniques can be made more accessible. To a greater extent, we focus on the human aspect: how to achieve impact, how to change the way of thinking of the various stakeholders about this issue, and in particular, as a research community, how to alter our behaviour, and instead of competing, collaborate to address this issue.

1 Introduction

Nowadays, software has become an integral part of our daily lives. We can no longer imagine what life would be like if we were not continuously supported by software (and the underlying hardware, of course). As a consequence, there has been an enormous growth in the software industry worldwide, and it is expected that it will continue to increase in the coming years [34, 93]. Moreover, also many other industries such as the service industry (banking, finance [47]) and the automotive industry [83] depend more and more on their software development; they are typically called software-intensive industries and face the same challenges as the software industry.

However, this enormous growth has also made it evident that the software industry is struggling to ensure the reliability of its software [33, 76]. Software failures can have serious economic or societal consequences. For example, recently in Belgium, the ATMs were not usable for a full day after a software update [98], and in the Netherlands, the electronic payment system was intermittently unusable [4, 79]. As a result, banks received damage claims from shop owner organisations, who claimed having a substantial income loss due to software issues. Many other similar examples are available [59, 102], and estimates of the costs of software failures exceed €250,000,000,000 annually worldwide [18, 41, 82]. Moreover, other scientific disciplines also depend increasingly on the reliability of software. For example, a software error recently detected in fMRI software has risked invalidating around 15 to 25 years of brain research including 3500 papers on the subject [29, 30, 71, 72].

For decades, academic researchers have claimed that rigorous use of formal analysis tools can help to increase the quality and reliability of software [22, 104]. A wide range of techniques, with corresponding tool support, have been developed [17]. These techniques differ in the guarantees they provide and in the ease of applicability. There is usually a trade-off: the stronger the guarantees provided by a technique, the more work is typically needed to obtain these guarantees. Despite this variety, all these techniques share a common foundation based on precise mathematical notations (e.g. formal program semantics and program logics), describing the program behaviour and properties [101].

Success stories of formal methods in industrial practice

Formal analysis techniques have been steadily improving over the last years due to the development of powerful automatic solvers and smart combinations of existing technologies, e.g. in SLAM/SLAM2/SDV [7, 57], Astrée [26, 64], or Frama-C [55]. Multiple examples illustrate that the application of formal methods on industrially-relevant examples is becoming possible. We list some interesting examples here, without striving to be exhaustive.

In the aviation industry the use of formal methods has been integrated in the development standards and accepted as a part of the (mandatory) certification procedure [80, 81]. Tools such as Astrée and Frama-C were successfully employed to formally analyse portions of the code for several aircraft models

including the currently largest passenger aircraft A380 [66, 86, 96]. Besides avionics, the Astrée verifier has been routinely applied to the docking software of a cargo space ship, in automotive control, nuclear plant technology, and ventilation [69]. Similarly, in the automotive field formal methods are also gaining increasing attention. Though not strictly enforced by the corresponding automotive standard ISO 26262, some suppliers internally design, check, or verify parts of their software using formal methods [53, 70]; the degree of rigour required by the standard grows along the chain A-B-C-D, from the most relaxed Automotive Safety Integrity Level (ASIL) A to the strictest level D, while formal verification is recommended for C and D [48]. Social networks have no safety-critical software, but they also use formal methods: Facebook internally runs the INFER tool to verify selected properties, such as memory safety errors and other common bugs of their mobile apps, used by over a billion people [21]. The driving force in this case is the huge economic cost of failures. Moreover, in 2011, the AWS division of Amazon started to use TLA+ to meet the requirements stated in their contractual obligations, checking both their present designs and aggressively optimised ones [68]. Amazon believes that formal methods ‘*accelerate* both time-to-market and quality of [their] projects’, and since then, have expanded their efforts, recently also using OpenJML for the analysis of some of their components [25]. Moreover, formal methods have also been successfully used in quite a large number of other areas, for example, to raise the quality of operating system kernels [7, 56], in compilation [60, 65], in telecommunication services [39, 87] to prove or refute properties of cryptography protocols [63], in railway signalling [6, 31], for subway transportation [10, 16], in control systems of the Maeslant storm surge barrier [51, 52, 89] and the Algra bridge [37], for user interfaces [99], in computer-aided design [9], in defence [13], to ensure high quality of cloud services [68], for lighting systems [94], and in a plethora of other areas [5, 27, 77, 78, 104]. Finally, attempts of formal verification of widely used algorithms, protocols, and their implementations sometimes reveal that they are incorrect (e.g. in the case of the Needham-Schroeder protocol [61] or Timsort [28].)

Formal methods as part of daily industrial practice

Despite the high number of success stories describing the use of formal methods in industrial practice, they did not lead to a systematic integration of formal methods in the daily software-development process [97]. We are not the first to observe this: over the last few decades several papers summarised the state-of-the-art in the use of formal methods in industrial practice and made recommendations on how to strengthen this connection [22, 88, 104]. The recommendations that these papers give regarding research directions, tool integration, etc. have been considered by the industry, but still need further elaboration. Moreover, we see that despite this progress, the software industry changes so quickly that every time academic researchers in formal methods make a step to bridge the gap between formal-methods research and the industrial software-development practice, the gap does not become smaller, because industry has again moved

forward, using new technologies and ensuring their market share for the next hype. Furthermore, we think it is important to realise that many of the success stories above depend on an individual academic researcher pushing for it strongly, working hard on building up a relationship with an industrial partner, and adjusting tools to make a specific formal method applicable to the software of this industrial partner.

We believe that to achieve a fundamental change to this situation and to integrate formal methods in the standard software-development process, as a community we have to change the way in which we try to bridge this gap. Instead of individuals pushing forward on their own, we have to act on this together, in a concerted manner. We have to do more than just create individual success stories, but also promote a completely new way of thinking about software development. This paper describes our view on how we, as the formal-methods community, should address this challenge. We will first give an analysis of how we see the current situation, identify what we consider as the bottlenecks, and then present our recommendations. Many of these recommendations are non-technical, but instead, they aim at changing the mentality of the different stakeholders. To structure the analysis and the recommendations, we look at the issue from several perspectives: industry (Section 2), the formal-methods community itself (Section 3), research support structures (Section 4), and education (Section 5). We do realise that our analysis and recommendations may miss out on certain aspects of this complicated issue, but it is our hope that this paper will be a starting point for further discussions on this topic. Ideally, this paper will encourage internal reflection within the formal-methods community, considering how we could become more effective at closing the gap between industrial practice and formal methods.

The analysis and recommendations in this paper are based on numerous discussions we had during workshops and conferences with other researchers and practitioners working in the area of formal methods, who shared their experiences on trying to bridge the gap to industry. We mention, in particular, the discussions held at the workshop ‘Verification of Concurrent and Distributed Software’, held at the Lorentz Center in Leiden, Netherlands on 14–18 September 2015 [38], and at the track *Formal Methods in Industrial Practice – bridging the gap* that we organised during the 8th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA), 7 November 2018 [32].

2 Industry

The term *software industry* is used for a wide range of different companies, ranging from the Googles and Yahoos of this world to single-person companies, developing small mobile phone applications for third-party users. Moreover, many companies in the service industry, such as banks and insurance companies, and even telecommunication companies, are changing into software-intensive companies. This means that the attitude towards software correctness and qual-

ity can vary substantially from one software-producing company to another. Furthermore, companies are profit-driven, and to adopt new technologies and processes for quality assurance and software development, they need to back up and justify such changes by a cost-benefit analysis, or at least by perceived pay-offs. Some factors that can influence such decisions are time-to-market, the development and maintenance costs of software, the retail value of the software product (and thus, the added value), the cost of introducing new technology (cost of tools, cost of training engineers or hiring experts, cost of changing the development process), and external requirements, such as what the competitors do in terms of standards and certification.

So, there obviously cannot be a singular approach to quality assurance in the software industry. But the dilemma of how to ensure that software is developed *efficiently*, and at the same time that it functions *correctly* under all circumstances is widely shared within the whole range of software-industry companies. Unfortunately, many software companies do not really perceive that they have such a dilemma. According to Peter Gabriel Neumann, an expert in computing risks and a principal scientist at SRI International, they ‘throw this [software] together, shrink wrap it and throw it out there. There's no incentive to do it right, and that's pitiful’ [84]. The companies are focused on shipping their software (‘time to market’) and do not realise that afterwards they spend much longer on maintenance than they would have done on improving software quality during development – provided they had the right tools for it.

Experience with the industrial application of formal methods in certain areas shows that it is indeed beneficial: it results in better code that is easier to maintain and contains fewer errors [73, 74, 92]. However, these applications typically succeed in restricted settings, where the reliability or availability requirements are so high that managers are willing to invest time and effort in adopting formal methods. For the ‘mainstream’ industry, the situation is different, and the success of these very specific examples is not guaranteed to have an immediate impact on other, less safety-critical or business-critical domains. Moreover, it is very difficult, if not impossible, to come up with concrete numbers for costs and benefits (including later savings) of the application of formal methods.

Obstacles to the adoption of formal methods

We see several obstacles to the adoption of formal analysis techniques in the software-development process:

- Writing down *software requirements* is often not properly considered as part of the development process; they are left informal, not properly tested, incomplete, etc. However, to use a formal technique, the requirements need to be clarified and formalised, which can only be properly done by programmers with training in requirements engineering. This step incurs fixed costs and takes time: about 30% of the whole time may go into formalisation before any single code line is written, while the remaining phases are shorter [40, Myth 5]. And this step will not be taken, unless

there is a perceived immediate pay-off. Moreover, getting the requirements right is often an iterative process, and while developing the system, one needs to go back to the client frequently to validate that the system is still being developed in the desired direction.

- Companies typically employ an abundance of technology (such as build servers, version management, etc.) that supports an established *software-development process*; changes in the development process mean that companies might have to use different technology or adapt the existing one. It is difficult to convince companies to make such a move, because it will incur a production loss (in the short run, at least), and it is difficult for the decision-makers to believe – let alone accept – that the increased software reliability will outweigh this production loss. After all, there are no satisfactory, sufficiently generic studies that compare the effectiveness of various development processes for reaching the same goal. Even for large companies (e.g., BMW) that already employ various software-development processes for different goals, yet another, new process would require education and a change of mindset, a change that incurs resistance in any case.

In this context, it is important to note that the adoption of formal technologies can vary significantly in the impact it has on the software-development process. Verification is less disruptive to established processes, but there is a trade-off between the effectiveness of the verification and system size: early verification can effectively ascertain that a specification is correctly represented by its slightly larger refinement, whereas post-design verification is less likely to be effective, since it has to deal with a large system already built. For instance, early verification is the contents of the Design Verification phase of the V-Modell XT [3, G.1.1.5], while post-design verification can be used (and is sometimes used) to reduce the testing burden in classical software-development processes following a Top-Down approach [91, Abb. 1.1]. Model-driven design where specification and verification are integrated into an agile development process is more promising, since it is incremental, but requires a new process and may be more difficult to adopt. For example, (formal) specification can be an item on the backlog and a subsequent goal of a Scrum [103] sprint, and verification can be used in the Testing phase of Design Thinking [100] if the properties to be verified are clear. Correctness-by-construction is another promising paradigm, but also requires a substantial change in the way systems are designed. Synthesis is a perfectly valid backlog item in Scrum, of course, assuming that a formal specification exists and the product owner agrees to it.

- Software developers (or their managers) are often simply unaware of the *wide range of tools and techniques* available that could help them to improve their software quality. And even if they are aware, there is never any time to quietly search for available options or to try out some unknown

technology because of the enormous market pressure. Moreover, unfortunately, it is very hard to make a clear and indisputable estimate of the expected cost reduction.

- Existing tools and technologies *never fit one-on-one*. Nowadays, software developers often use very complex development environments, which make extensive use of different frameworks and libraries (which are often developed in different programming languages and can be frequently changing). Time is needed to adapt to the format as required by the formal method at hand. This time is frequently not available, because of the time-to-market pressure, and even when it is, there are always other, more pressing matters that the decision-makers feel the need to address first. Furthermore, the overwhelming majority of the formal-methods tools are typical research prototypes: they do not work under all circumstances, do not cover all cases, and are not professionally maintained. And if they do work well and are maintained, they are often very expensive – probably because of the small market for them. However, in general, formal methods need not be intrinsically costly; they do pay off when applied properly: ‘The fact is that writing a formal specification *decreases* the cost of development’ [40, Myth 5].
- Then, *human psychology* also comes into play: programmers are reluctant to change the way they have always programmed, and managers do not want to adopt novelties they do not understand.
- Finally, we should keep in mind that many programmers have not taken any *appropriate courses* at research universities. In the USA, for instance, 35% of computer programmers had no Bachelor’s or higher degree as of year 2002 [90, p. 98]; according to a worldwide online survey [46], about one fourth of professional developers had no Master’s or higher degree in 2019. Such programmers might have never completed any formal education at all, or they might have attended high school only, or they might have completed some level of professional, non-research education, e.g. a degree at a university of applied sciences¹, etc. At the same time, many programmers that do have a higher education are not necessarily trained in Computer Science.

Enablers for the adoption of formal methods in industry

We should first look more seriously at the current (informal or semi-formal) validation methods being used in industry, such as testing, code inspection, etc. Methods and processes for software testing are being rapidly developed, and software-testing research is a hot topic within software engineering. Testing is now also being increasingly automated and integrated in agile software-development processes with frequent builds. These methods and processes are a

¹As can be found in Germany and the Netherlands, for example.

natural place to gradually introduce formal methods in industry by successively adding automated tool support in the testing and verification process instead of selling formal methods to industry as a ‘standalone’ technique. Another interesting option is to try to combine formal methods and testing to make the full verification process more efficient, e.g. by using formal methods to direct testing efforts to the ‘dark corners’ typically discovered by such methods.

At the same time we feel that eventually something more is needed, namely that *the application of formal methods becomes an integral part of the software-development process*. This can start with small enhancements, such as extending the common usage of static type checking (e.g. automatic warnings if a null-pointer exception or some other run-time error could occur), and should finally lead to full and seamless integration of formal methods in the software-development process. Also tool-combining platforms, which make the reuse of results possible and enable the use of machinery from common development platforms such as Eclipse, are important first steps in this direction [62], but more effort is needed for a smooth integration into the development process.

Then, it is also important to involve the *application expert* directly in the development so that they feel the impact of formal methods themselves [35, 67]. The point here is to find a match to the application expert’s mindset. We cannot expect to educate everybody to become a formal-methods expert; instead, it should be up to us to try to get closer to the customers, domain experts, and users by really trying to understand their way of thinking and getting them to use formal methods.

Eventually, what we as a formal-methods community should continue to aim for is that the people involved in the software industry will become aware that formal methods are useful and will consider the application of formal techniques as a first option to ensure software quality rather than as a last resort. This is a change in attitude taking many years, which can only be achieved by tackling the issue from many different angles, not by simply telling industrial software developers that formal methods will solve all their problems.

Recommendations

1. Invest time in industrially-relevant case studies in order to understand what techniques are actually needed for industrially-relevant applications. Study existing tools and practices and investigate how to integrate frequently used libraries and frameworks in formal verification.
2. Investigate and understand (semi-formal) processes and methods currently used in industry and see how these can be further improved by combining them with formal methods.
3. When designing a formal-methods–supported software-development process, keep the implementers in mind and adapt social deterrents and incentives correspondingly, so that the implementers are motivated to continue to use those techniques.

4. Train engineers and managers in the software industry in good software development and seamlessly integrate formal methods in the process, so that in the long run the engineers and managers will see this as simply a part of the process, not as a special add-on.
5. Investigate simple and lightweight ways to integrate the use of formal methods in the software-development process, ensuring that if a developer tries a formal method for the first time, it will be a pleasant experience, with most likely a high return on investment.
6. Identify areas where formal methods in an industrial setting are most useful and are most easily applied and make sure these are shared among the formal-methods community in order to create a common awareness of good targets.
7. Continuously try to convince your industrial partners of the benefits and opportunities offered from applying formal methods and from hiring staff that has training in such methods, since only in that way the methods will eventually sink in.
8. Share your success stories of applying formal methods in an industrial setting.

3 Formal-methods community

Next, we consider the formal-methods community itself and what we, as academic researchers, can do to bridge the aforementioned gap between formal methods in academia and daily industrial practice. Some of the issues that we identify are related to academia in general, whereas some are more specific to the formal-methods community.

General challenges for academia

An important challenge we have to face here is that academic success is measured by publications, projects, and prizes. This encourages individualism: collaboration and putting effort into making something usable for others does not necessarily advance one's own career. These are the 'rules of the game' that many people play without questioning. As a consequence, we all like our own approach best, and we do not appreciate each other's work, especially if it is not sufficiently 'new'. And if somebody does something that is new, we are mainly interested in how we can beat this person and come up with something that is even better and newer. But is this the best way for society to advance science? As a consequence of the current set-up, academic researchers focus on solving the most difficult and challenging problems and on how to find intricate solutions for those. We then develop a solution that works for this particular challenging aspect of the problem; but we have typically no reason or incentive to adapt this to a complete solution that is applicable in the 'real world'.

What should be done about this? We believe that the existing set-up is still important for us as academic researchers that keep on looking for scientifically challenging problems, and we should keep on striving to find the most elegant solutions; after all, this is what we are good at, and this is our added value. **However**, we should also look at how we can join forces, collaborate, and in this way, produce new results and enlarge the scale of what we can do. We should also be open for the problems that industry faces and help industry solve them by finding the best solution at hand as opposed to simply our own solution. This will require a change of mindset of many researchers, as they need to realise the added value of collaboration, e.g. potentially higher impact. Such a change will also require new kinds of incentives from our academic institutions and the funding structures.

Specific challenges for the formal-methods community

To make this change of mindset possible, we as a community should appreciate the effort that is put into *tool development* more. There are already some conferences that explicitly encourage this (e.g. FMICS, ISoLA, iFM, TACAS, FASE), but we feel that more conferences should have special tool paper categories, where the effort (typically illustrated by an industrial case study) of making a tool widely usable or of integrating different techniques is appreciated. Of particular importance are also journals which are dedicated to the aspect of technology transfer by means of tools and case studies. STTT [23] and *Stories from the Front* in the Journal of Systems and Software [85] are good examples of this, but we think more journals should encourage such submissions. In this way, even if we do not change the overall system of appreciation, we can still make sure that researchers can obtain credits for tool work. Teaming up with software- and requirements-engineering researchers can also be an important way to achieve this: for instance, they have established venues where industrial case studies are welcome and often also have many industrial contacts. Another way to give scientific credits to work on tool development is to organise competitions. There are already several such competitions: VSComp [24], the VerifyThis program-verification competition [44, 45], SV-Comp [11], the RERS competition [49], the SAT competition [8], etc. (see [12] for a more complete overview). A good result in such a competition is considered as a scientific achievement. Moreover, competitions also make tool developers more aware of what can be achieved with other tools, so that they can learn from each other, discuss, and exchange efforts.

Additionally, we as a community should put effort into advertising our tools, e.g. by making YouTube movies, and into providing online platforms to use the tools. It is important that we exchange ideas and help each other to achieve this. We should also make a joint effort to advertise ourselves on the Web (Wikipedia, Facebook, etc.).

Recommendations

1. As a community, collaborate on advertising our tools and how they could be used together in order to create maximal visibility of what we can achieve for the software industry.
2. Put effort in changing the mindset of what is necessary to be a good researcher and make sure that collaboration is encouraged to create the necessary space and time for researchers that work on industrially relevant activities.
3. Make sure sufficient scientific credits can be obtained for the effort put into tool development, industrial case studies, and technology transfer by having more conferences and journals that report on such activities and by teaming up with requirements- and software-engineering researchers.

4 Research support

A major challenge that we see is how to obtain (financial) support for research activities that are aiming at bridging the gap between industry and academia. To achieve this, researchers first of all need to invest time and effort in building up a relationship with potentially interested industrial partners, e.g. by performing a case study to solve some problem the company is interested in. Only once this relationship has been established will companies be open to listen to and understand the innovations proposed by researchers. However, finding time is difficult, since searching for industrial partners is only one of the many activities that researchers have to carry out. Moreover, industrial case studies can be difficult to publish, for they seldom describe new ideas, but tend to apply existing techniques and tools in a particular setting.

Researchers typically get funded to develop new ideas and to publish papers describing these new ideas. For research papers, it is sufficient to develop a prototype, i.e., a proof-of-concept tool that can demonstrate that the ideas work and can be implemented (typically at the *Technology Readiness Levels (TRLs)* [36] 3 to 5). However, such a prototype tool typically cannot be directly transferred to industry. For a tool to be usable in an industrial setting, it needs to be robust and provide full coverage (i.e. at least at TRL 8). For example, for a prototype program-analysis tool it can be sufficient to completely ignore exceptional control flow, but when such a tool is used in a realistic software-development setting, it also needs to handle this aspect.

Extending a tool to make it usable and robust in an industrial setting typically requires much engineering work, for which often a programmer or engineer is better suited than a researcher. In the academic world, however, no credits are normally given for such activities, and *limited funding is available*. If a researcher wishes to undertake this kind of work, usually the only way to do this is to start a spin-off company. However, not all researchers are interested in

setting up companies, and moreover, creating a successful company requires a completely different skill set.

We believe that if funding agencies (and governments) consider that technology transfer from academia to industry is important, they should support this by dedicated funding schemes, which can support work on tool development for a certain period. Importantly, such a funding scheme should not require that the outcome is a tool that can be directly commercialised; the goal should be to develop a tool that is demonstrable to end-users (typically TRL 6–7). It might still lack functionality in some corner cases, but these corner cases should be clearly defined, and there should be a substantial class of applications for which the tool just works without complications. We believe that it is necessary to reach such a state before a company could be convinced to invest time and money in the further development of such a tool.

The development of this end-user–demonstrable tool does not necessarily have to be carried out at the university. For example, many different European countries have created a national ‘eScience center’ [1], which develops software and methods for the scientific community; such an institution can also be a perfect place to extend prototype tools into something that can be demonstrated to industry.

Recommendations

The following recommendations refer to researchers that are in the position to influence the policy makers of the research funding agencies.

1. Develop flexible funding schemes (in-cash or in-kind) to support the engineering work that is necessary to transform a prototype implementation into a demonstrable implementation.
2. Make sure that also researchers that do not want to create a company feel an incentive to transfer their techniques to industry to ensure that the most promising ideas will actually be developed further into prototypes, independent of the affinity with commercial activities of the researcher.
3. Ensure that academic credits can be obtained by transferring results to industry, for example, by giving more priority and weight to conference tracks and journals soliciting tool and demo papers (and making sure that these papers are indeed reviewed as tool-and-demo papers, not as regular research papers). Put emphasis on and reward such activities when recruiting new or promoting existing staff, such that researchers in the formal-methods community feel that activities in this direction will not have a negative impact on their scientific ambitions.

5 Education

Currently, in university education programmes, formal methods are typically taught in a separate course – and often have a reputation of being difficult.

One of the reasons for this is that we as teachers like to teach our most recent developments, giving difficult and challenging verification tasks to the students. We should **not** stop doing this, but we should realise that this only attracts a small percentage of students, and if we want to have impact, we need to broaden the target group of formal-methods-related education.

In particular, we should put additional effort into familiarising **also** the larger percentage of the students with formal techniques and what can be achieved by applying them. Therefore, *formal methods should be woven into software-development and requirements-engineering courses*. This should target not only software-development courses taught at universities, but also software-development courses at other levels (vocational education, training for software developers, etc.). In these courses, we should not force all students to prove full correctness of whatever they develop. Instead, we should give them a good feeling of what can be achieved by using more rigorous and formal techniques to support their requirements-engineering and software-development processes and a good feeling for the wide range of tools and techniques that are available. In particular, they should understand that rigour comes at a cost: the effort to achieve that. It is important that in these courses, lecturers encourage the students to use the tools and techniques that are reasonably well-developed and stable and that will convince the students that the usage of these tools really helps to improve software quality (i.e. they should experience the reduction in development and maintenance time). This means that lecturers should not always use their ‘own’ tool in such courses, but they should put real effort in using tools and techniques that are adequate for the job at hand. It is important that these techniques are taught as something that is simply *part of the process* and not as an optional add-on.

As a concrete case of how this can be achieved, one of the authors has introduced the writing of JML specifications to document the code as part of the first programming course in Java [42]. This forces the students to think about the behaviour of their code and write this in a formal way. In addition, the course provides extra exercises and an optional lecture where the students are challenged to use the run-time checker to validate their specifications. In later years of the programme, this run-time checker can be used as a mandatory step in software development (and static verification is presented as an option). Full verification is taught in a Master’s course, which is mandatory for students in software technology and embedded systems [43]. This course does not focus on the details of how the formal methods are implemented, but rather concentrates on what actually can be achieved with formal techniques. Courses with similar ideas are offered by other universities; concrete examples are [2, 15, 19, 20, 58]. In the literature, this approach to integrate formal methods in the regular software-engineering training has been coined ‘*Secret Ninja Formal Methods*’ [54].

Teaching the use of formal methods as an integral part of the software-development process requires that this idea is rolled out throughout the whole educational programme. Moreover, it also requires that there are some high-quality tools robust enough to be used by students.

An important means to achieve this state of affairs is by exchanging teaching experiences and best practices within the formal-methods community. There are Web pages like Formal Methods Europe [50] and workshops on teaching formal methods such as [14, 75]. Such venues should be much more actively used to distribute these ideas (and provide information for reuse).

Moreover, we should in addition keep our high-level expert formal-methods teaching for the people that really want to understand how things work and, in this way, ensure that the research in formal methods keeps on going strong. For these specialist courses, we should consider how to enlarge the audience by enabling students from other universities to follow such courses as well. One possibility for this is to develop a Massive Open Online Course [95] on such a specialised topic.

Finally, we should keep in mind that only focussing on academic education is not sufficient to make all software developers familiarise themselves with formal methods. As mentioned above, when discussing the situation in industry, many software developers are not trained as academic computer scientists, but learn programming in some other way (e.g. at high school, at a university of applied sciences, or as part of a post-doctoral education). While we do not have the means to educate all these programmers directly in proper software and system development, we should make an effort to educate their teachers and aim for a transfer effect.

Recommendations

1. Teach both a specialised formal-methods course and a course where formal methods are simply part of the process – without emphasising that the second course teaches formal methods – so that future software developers see the use of formal methods as an integral part of the requirements-engineering and software-development process and experience the benefits of formal methods already during training.
2. Ascertain that students get a positive experience working with formal tools and techniques, so that they see the benefits and do not immediately, collectively decide that this is not useful.
3. Do not insist on using only your own tools and techniques, but use well-established and stable tools, again to ensure that students have a positive experience, and do not consider the application of formal methods to be a time-consuming struggle.
4. Make specialised courses available to a large audience to have a maximal dissemination of this specialist knowledge.
5. Offer courses for school teachers and teachers in vocational education and provide them with suitable training materials for their students, so that they can pass on their experiences to more mixed groups of students.

6 Conclusions

In this paper, we have considered the gap between academic research and industrial practice in the area of formal methods. We have looked at this issue from different perspectives: industry, education, research support, and the formal-methods community itself. We believe that from all these points of view, the formal-methods community should be able to take steps towards closing this gap, and we have provided a concrete list of recommendations.

Our conclusions are drawn from a number of *observations*, which can be summarised as follows:

1. Computer Science is a rather new and immature discipline, which, together with certain historical factors, has led to a mutual distrust between industry and academia in that field and to a reluctance to collaborate.
2. Companies are profit-driven, while academic researchers are novelty-driven; this discrepancy has only increased the gap between the two worlds.
3. There are a number of success stories of applying formal methods in industry, but these have largely been the result of individual efforts and not of concerted effort incentivised by funding agencies.
4. At the same time, there are ample opportunities for technology transfer of formal methods to industry that have not been utilised.

Our *recommendations* to the formal-methods community can be summarised as follows:

1. We need to learn how industry works and be willing to do industrially relevant research and industrially useful work.
2. Universities need to find ways to incentivise industrial collaboration by adjusting its system of academic and career credits.
3. The research support and funding agencies need to actively encourage tool development and maintenance beyond prototyping.
4. In academic education, we should ensure that formal tools and techniques become an integral part of software-development teaching; where appropriate, we should also teach how to conduct industrially relevant research.

What we have seen is that there are already some industrial areas that have an interest in software verification, in particular, in the safety-critical software industry. This is good, and we should definitely continue to collaborate with them and have impact there. Furthermore, we should use the successes in these areas as a lever to reach out to other, less safety-critical areas of software development. Only if in the end we manage to convey our theoretical results in formal methods into the daily software-development process of all those small and medium-sized enterprises out there can we conclude that we have finally

closed the gap between academia and industry. To reach this goal, the formal-methods community should change its mentality, actively collaborate, and encourage each other to achieve maximal industrial impact.

Acknowledgements

We are indebted to Christian Prehofer, Bernhard Steffen, and Björn Lisper for giving useful feedback on earlier drafts of this paper. In particular, Björn Lisper pointed out the importance of investigating the techniques currently used in industry and the advantages of teaming up with software-engineering research, while Bernhard Steffen pointed out many relevant initiatives that are working towards the same goal as we intend with our paper. Bernhard Steffen also emphasised the importance of *lightweight* formal methods that make it possible to involve the application expert directly. Finally, Christian Prehofer pointed out that it is impossible to precisely define the costs and benefits of formal methods as well as the importance of taking into account which frameworks and libraries are frequently used in industry and incorporating them in the various academic formal-methods prototypes. We are further indebted to Elizabeth Hamzi-Schmidt for proofreading parts of the paper.

Funding: This work was supported by the NWO 639.023.710 VICI project Mercedes; the ITEA-3 project REVaMP2 [project number 15010]; and the Software- and Systems-Engineering Research Group at the Technical University of Munich, Germany.

References

- [1] Patrick Aerts. *PlanE: The platform of national eScience centers in Europe*. July 2017. URL: <http://plan-europe.eu>.
- [2] Wolfgang Ahrendt. *Software engineering using formal methods*. Course at Chalmers, Sweden. URL: <http://www.cse.chalmers.se/edu/year/2016/course/TDA293/course.html>.
- [3] Daniel Angermeier, Christian Bartelt, Otto Bauer, Gerd Beneken, Klaus Bergner, Ulrich Birowicz, Thomas Bliß, Christian Breitenstrom, Nils Cordes, David Cruz, Patrick Dohrmann, Jan Friedrich, Michael Gnatz, Ulrike Hammerschall, Istvan Hidvegi-Barstorfer, Helmut Hummel, Dirk Israel, Thomas Klingenberg, Klaus Klugseder, Inga Küffer, Marco Kuhrmann, Michael Kranz, Wolfgang Kranz, Hans-Jürgen Meinhardt, Michael Meisinger, Sabine Mittrach, Hans-Joachim Neußer, Dirk Niebuhr, Klaus Plögert, Doris Rauh, Andreas Rausch, Thomas Rittel, Winfried Rösch, Erik Saas, Joachim Schramm, Marc Sihling, Thomas Ternité, Sascha Vogel, Bernd Weber, and Marion Wittmann. *V-Modell XT*. Version 2.3. c/o 4Soft GmbH, Mittererstr. 3, 80336 München, Germany. URL: <http://ftp.tu-clausthal.de/pub/institute/informatik/v-modell-xt/Releases/2.3/V-Modell-XT-Gesamt.pdf>.
- [4] ANP. *Software-update legt weer pinverkeer plat*. 16 Nov. 2011. URL: <http://www.nu.nl/nuzakelijk-overig/2669422/software-update-legt-weer-pinverkeer-plat.html>.
- [5] Stephen Austin and Graeme I. Parkin. *Formal methods: a survey*. Tech. rep. National physical laboratory, Mar. 1993.

- [6] Stefano Bacherini, Alessandro Fantechi, Matteo Tempestini, and Niccolò Zingoni. ‘A story about formal methods adoption by a railway signaling manufacturer’. In: *FM 2006: Formal Methods, 14th International Symposium on Formal Methods, Hamilton, Canada, August 21–27, 2006, Proceedings*. Ed. by Jayadev Misra, Tobias Nipkow, and Emil Sekerinski. Vol. 4085. Lecture Notes in Computer Science. Springer, 2006, pp. 179–189.
- [7] Thomas Ball, Ella Bounimova, Rahul Kumar, and Vladimir Levin. ‘SLAM2: Static driver verification with under 4% false alarms’. In: *Proceedings of 10th International Conference on Formal Methods in Computer-Aided Design, FMCAD 2010, Lugano, Switzerland, October 20–23*. Ed. by Roderick Bloem and Natasha Sharygina. IEEE, 2010, pp. 35–42.
- [8] Tomáš Balyo and Marijn J. H. Heule. ‘Proceedings of SAT competition 2016: solver and benchmark descriptions’. In: B-2016-1 (4 July 2016). Ed. by Matti Juhani Järvisalo. Department of Computer Science Series of Publications B.
- [9] Milica Barjaktarovic and WetStone Technologies, Inc. *The state of the art in formal methods*. Tech. rep. Jan. 1998.
- [10] Patrick Behm, Pierre Desforges, and Jean-Marc Meynadier. ‘MÉTÉOR: an industrial success in formal development’. In: *B’98: recent advances in the development and use of the B method, second international B conference, Montpellier, France, April 22–24, 1998*. Ed. by Didier Bert. Vol. 1393. Lecture Notes in Computer Science. Springer, 1998, p. 26.
- [11] Dirk Beyer. *SV-COMP 2019 – 8th international competition on software verification – results*. 13 Feb. 2019. URL: <http://sv-comp.sosy-lab.org/2019/results/results-verified>.
- [12] Dirk Beyer, Marieke Huisman, Fabrice Kordon, and Bernhard Steffen, eds. *Toolympics, part 3 of the proceedings of TACAS 2019*. Vol. 11429. Lecture Notes in Computer Science. Springer, 2019.
- [13] Robin E. Bloomfield and Dan Craigen. *Formal methods diffusion: prospects*. Sept. 2000.
- [14] Andreas Bollin, Tiziana Margaria, and Isabelle Perseil, eds. *First Formal Methods in SW Engineering Education and Training Workshop*. Vol. 1385. CEUR-WS. URL: <http://ceur-ws.org/Vol1-1385> (visited on 21/06/2015).
- [15] Henning Bordihn, Anna-Lena Lamprecht, and Tiziana Margaria. ‘Foundations of semantics and model checking in a software engineering course’. In: *FMSEET@FM 2015*. 2015, pp. 19–26.
- [16] Jean-Louis Boulanger. *Formal methods. Industrial use from model to the code*. Wiley-ISTE, May 2012.
- [17] Jonathan Bowen. *Formal Methods*. 2014. URL: http://formalmethods.wikia.com/wiki/Formal_methods.
- [18] Tom Britton, Lisa Jeng, Graham Carver, Paul Cheak, and Tomer Katzenellenbogen. *Reversible debugging software: quantify the time and cost saved using reversible debuggers*. Tech. rep. Cambridge Judge Business School, 2013.
- [19] Manfred Broy. *Grundlagen der Programm- und Systementwicklung*. Course at TUM, Germany. Assistance by Alexander Malkis et al. 2014. URL: <http://web.archive.org/web/20161227181301/http://www4.in.tum.de/lehre/vorlesungen/grupsy/WS1314>.
- [20] Manfred Broy. *Modellierung Verteilter Systeme*. Course at TUM, Germany. Assistance by Alexander Malkis et al. 2013. URL: <http://web.archive.org/web/20171105102228/http://www4.in.tum.de/lehre/vorlesungen/mvs/SS2013>.
- [21] Cristiano Calcagno, Dino Distefano, Jérémy Dubreil, Dominik Gabi, Pieter Hooimeijer, Martino Luca, Peter William O’Hearn, Irene Papakonstantinou, Jim Purbrick, and Dulma Rodriguez. ‘Moving fast with software verification’. In: *NASA formal methods – 7th international symposium, NFM 2015, Pasadena, CA, USA, April 27–29, 2015, Proceedings*. Ed. by Klaus Havelund, Gerard Johan Holzmann, and Rajeev Joshi. Vol. 9058. Lecture Notes in Computer Science. Springer, 2015, pp. 3–11.
- [22] Edmund Melson Clarke and Jeannette Marie Wing. ‘Formal methods: state of the art and future directions’. In: *ACM Comput. Surv.* 28.4 (1996), pp. 626–643.

- [23] Walter Rance Cleaveland, Tiziana Margaria, and Bernhard Steffen. ‘Editorial’. In: *STTT* 1.1–2 (Dec. 1997), pp. 1–5.
- [24] Ernie Cohen, Marcelo Frias, Peter Müller, and Natarajan Shankar. *Verified software competition (VSComp)*. Archived: <http://web.archive.org/web/20170614233211/http://vscomp.org>. June 2014. URL: <http://vscomp.org>.
- [25] David R. Cok. ‘Java automated deductive verification in practice: lessons from industrial proof-based projects’. In: *Leveraging Applications of Formal Methods, Verification and Validation. Industrial Practice – 8th International Symposium, ISoLA 2018, Limassol, Cyprus, November 5–9, 2018, Proceedings, Part IV*. Ed. by Tiziana Margaria and Bernhard Steffen. Vol. 11247. Lecture Notes in Computer Science. Springer, 2018, pp. 176–193.
- [26] Patrick Cousot, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, David Monniaux, and Xavier Rival. ‘The ASTRÉE analyzer’. In: *Programming Languages and Systems, 14th European Symposium on Programming, ESOP 2005, held as part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2005, Edinburgh, UK, April 4–8, 2005, Proceedings*. Ed. by Shmuel Sagiv. Vol. 3444. Lecture Notes in Computer Science. Springer, 2005, pp. 21–30.
- [27] Dan Craigen, Susan Lucille Gerhart, and Ted Ralston. ‘An international survey of industrial applications of formal methods’. In: *Z user workshop, London, UK, 14–15 December 1992, Proceedings*. Ed. by Jonathan Peter Bowen and John Edward Nicholls. Workshops in computing. Springer, 1992, pp. 1–5.
- [28] Stijn de Gouw, Jurriaan Rot, Frank S. de Boer, Richard Bubel, and Reiner Hähnle. ‘OpenJDK’s Java.util.Collection.sort() is broken: the good, the bad and the worst case’. In: *Computer Aided Verification – 27th International Conference, CAV 2015, San Francisco, CA, USA, July 18–24, 2015, Proceedings, Part I*. Ed. by Daniel Kroening and Corina S. Păsăreanu. Vol. 9206. Lecture Notes in Computer Science. Springer, 2015, pp. 273–289.
- [29] Anders Eklund, Thomas E. Nichols, and Hans Knutsson. ‘Cluster failure: Why fMRI inferences for spatial extent have inflated false-positive rates’. In: *Proceedings of the National Academy of Sciences of the United States of America*. Vol. 113. 28. 7900–7905. 2016.
- [30] Anders Eklund, Thomas E. Nichols, and Hans Knutsson. ‘Correction for Eklund et al., Cluster failure: Why fMRI inferences for spatial extent have inflated false-positive rates’. In: *Proceedings of the National Academy of Sciences of the United States of America*. Vol. 113. 33. E4929. 2016.
- [31] Alessandro Fantechi, Wan Fokkink, and Angelo Morzenti. ‘Some trends in formal methods application to railway signaling’. In: Stefania Gnesi and Tiziana Margaria. *Formal methods for industrial critical systems: a survey of applications*. John Wiley & Sons, Inc., 2013. Chap. 4.
- [32] Michael Felderer, Dilian Gurov, Marieke Huisman, Björn Lisper, and Rupert Schlick. ‘Formal Methods in Industrial Practice – Bridging the Gap (Track Summary)’. In: *Leveraging Applications of Formal Methods, Verification and Validation. Industrial Practice – 8th International Symposium, ISoLA 2018, Limassol, Cyprus, November 5–9, 2018, Proceedings, Part IV*. Ed. by Tiziana Margaria and Bernhard Steffen. Vol. 11247. Lecture Notes in Computer Science. Springer, 2018, pp. 77–81.
- [33] Archana Ganapathi and David Andrew Patterson. ‘Crash data collection: a Windows case study’. In: *Dependable systems and networks (DSN)*. IEEE Computer Society, 1 Aug. 2005, pp. 280–285.
- [34] Gartner, Inc. *Gartner says global IT spending to grow 3.2 percent in 2019*. 17 Oct. 2018. URL: <http://www.gartner.com/en/newsroom/press-releases/2018-10-17-gartner-says-global-it-spending-to-grow-3-2-percent-in-2019>.
- [35] Frederik Gossen, Tiziana Margaria, Alnis Murtovi, Stefan Naujokat, and Bernhard Steffen. ‘DSLs for decision services: a tutorial introduction to language-driven engineering’. In: *Leveraging Applications of Formal Methods, Verification and Validation. Modeling – 8th International Symposium, ISoLA 2018, Limassol, Cyprus, November 5–9, 2018, Proceedings, Part I*. Ed. by Tiziana Margaria and Bernhard Steffen. Vol. 11244. Lecture Notes in Computer Science. Springer, 2018, pp. 546–564.

- [36] Caroline P. Graettinger, Suzanne Garcia-Miller, Jeannine Siviy, Peter J. Van Syckle, and Robert J. Schenk. *Using the Technology Readiness Levels scale to support technology management in the DoD's ATD/STO environments. A findings and recommendations report conducted for Army CECOM*. CMU/SEI-2002-SR-027. Sept. 2002. URL: http://resources.sei.cmu.edu/asset_files/SpecialReport/2002_003_001_13931.pdf.
- [37] Jan Friso Groote, Jeroen J. A. Keiren, Anson van Rooij, Vikram Saralaya, and Anton J. Wijs. *Verificatie van de correctheid van de PLC-software van de Algerabrug*. Dutch. Tech. rep. for Rijkswaterstaat, confidential. Apr. 2013.
- [38] Dilian Gurov, Marieke Huisman, James J. Hunt, and Arnd Poetzsch-Heffter. *Verification of concurrent and distributed software*. Event report. Sept. 2015. URL: <https://www.lorenzcenter.nl/lc/web/2015/718/report.php3?wsid=718&venue=0ort>.
- [39] Andreas Hagerer, Hardi Hungar, Oliver Niese, and Bernhard Steffen. 'Model generation by moderated regular extrapolation'. In: *FASE*. 2002, pp. 80–95.
- [40] John Anthony Hall. 'Seven myths of formal methods'. In: *IEEE Software* 7.5 (1990), pp. 11–19.
- [41] Les Hatton. 'The chimera of software quality'. In: *IEEE Computer* 40.8 (2007), pp. 104, 102–103.
- [42] Marieke Huisman. *Software systems*. Course at UTwente, The Netherlands. URL: <https://osiris.utwente.nl/student/OnderwijsCatalogusSelect.do?selectie=cursus&cursus=201700117&taal=en&collegejaar=2018>.
- [43] Marieke Huisman. *System validation*. Course at UTwente, The Netherlands. URL: <http://fmt.ewi.utwente.nl/courseinfo/en/2016/192140122>.
- [44] Marieke Huisman, Vladimir Klebanov, Rosemary Monahan, and Michael Tautschnig. 'VerifyThis 2015: a program verification competition'. In: *STTT* (Oct. 2016), pp. 1–9.
- [45] Marieke Huisman, Rosemary Monahan, Peter Müller, Andrei Paskevich, and Gidon Ernst. *VerifyThis 2018: A Program Verification Competition*. Research rep. Inria, 2019.
- [46] Stack Exchange Inc. *2019 developer survey*. 15 Apr. 2019. URL: <http://insights.stackoverflow.com/survey/2019/#education>.
- [47] ING. *The core banking university*. 30 Aug. 2018. URL: <http://www.ing.jobs/Netherlands/Internships/Core-Banking-University.htm>.
- [48] International Organization for Standardization. *Road vehicles – functional safety – part 9: automotive safety integrity level (ASIL)-oriented and safety-oriented analyses*. Geneva, Switzerland, Dec. 2018.
- [49] Marc Jasper, Maximilian Fecke, Bernhard Steffen, Markus Schordan, Jeroen Meijer, Jaco van de Pol, Falk Howar, and Stephen F. Siegel. 'The RERS 2017 challenge and workshop (invited paper)'. In: *Proceedings of the 24th ACM SIGSOFT International SPIN Symposium on Model Checking of Software, Santa Barbara, CA, USA, July 10–14, 2017*. 2017, pp. 11–20.
- [50] Einar Broch Johnsen. *Formal Methods Europe*. 2019. URL: <http://www.fmeurope.org>.
- [51] Pim Kars. 'Formal methods in the design of a storm surge barrier control system'. In: *Lectures on embedded systems, European educational forum, school on embedded systems, Veldhoven, The Netherlands, November 25–29, 1996*. Ed. by Grzegorz Rozenberg and Frits Willem Vaandrager. Vol. 1494. Lecture Notes in Computer Science. Springer, 1996, pp. 353–367.
- [52] Pim Kars. 'The application of Promela and Spin in the BOS project'. In: *The Spin verification system, proceedings of a DIMACS workshop, New Brunswick, New Jersey, USA, August, 1996*. Ed. by Jean-Charles Grégoire, Gerard Johan Holzmann, and Doron A. Peled. Vol. 32. DIMACS series in discrete mathematics and theoretical computer science. DIMACS/AMS, 1996, pp. 51–64.
- [53] David Kelf. *Formal verification assumes starring role in automotive*. 13 June 2017. URL: <http://www.embedded-computing.com/embedded-computing-design/formal-verification-assumes-starring-role-in-automotive>.

- [54] Joseph Roland Kiniry and Daniel M. Zimmerman. ‘Secret ninja formal methods’. In: *FM 2008: 15th international symposium on Formal Methods, Turku, Finland, May 26–30, 2008*. 2008, pp. 214–228.
- [55] Florent Kirchner, Nikolai Kosmatov, Virgile Prevosto, Julien Signoles, and Boris Yakobowski. ‘Frama-C: a software analysis perspective’. In: *Formal Aspects of Computing 27.3* (2015), pp. 573–609.
- [56] Gerwin Klein, June Andronick, Kevin Elphinstone, Gernot Heiser, David Cock, Philip Derin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harvey Tuch, and Simon Winwood. ‘seL4: formal verification of an operating-system kernel’. In: *CACM 53.6* (June 2010), pp. 107–115.
- [57] Rahul Kumar, Thomas Ball, Jakob Lichtenberg, Nate Deisinger, Apoorv Upreti, and Chetan Bansal. ‘CloudSDV enabling Static Driver Verifier using Microsoft Azure’. In: *Integrated Formal Methods – 12th International Conference, IFM 2016, Reykjavik, Iceland, June 1–5, 2016, Proceedings*. Ed. by Erika Ábrahám and Marieke Huisman. Vol. 9681. Lecture Notes in Computer Science. Springer, 2016, pp. 523–536.
- [58] Anna-Lena Lamprecht, Tiziana Margaria, and Clare McInerney. ‘A summer computing camp using ChainReaction and jABC’. In: *COMPSAC Workshops 2016*. 2016, pp. 275–280.
- [59] Leonard Lee. *The day the phones stopped: how people get hurt when computers go wrong*. Donald I. Fine, Inc., 1 Aug. 1992.
- [60] Xavier Leroy, Andrew Wilson Appel, Sandrine Blazy, and Gordon Stewart. *The CompCert memory model, version 2*. Research rep. RR-7987. INRIA, June 2012, p. 26.
- [61] Gavin Lowe. ‘Breaking and fixing the Needham-Schroeder public-key protocol using FDR’. In: *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*. Ed. by Tiziana Margaria and Bernhard Steffen. Berlin, Heidelberg: Springer, 1996, pp. 147–166.
- [62] Tiziana Margaria, Ralf Nagel, and Bernhard Steffen. ‘jETI: a tool for remote tool integration’. In: *Tools and Algorithms for the Construction and Analysis of Systems, 11th international conference, TACAS 2005, held as part of the joint European Conferences on Theory and Practice of Software, ETAPS 2005, Edinburgh, UK, April 4–8, 2005, Proceedings*. 2005, pp. 557–562.
- [63] Catherine Ann Meadows. ‘Emerging issues and trends in formal methods in cryptographic protocol analysis: twelve years later’. In: *Logic, rewriting, and concurrency – essays dedicated to José Meseguer on the occasion of his 65th birthday*. Ed. by Narciso Martí-Oliet, Peter Csaba Ölveczky, and Carolyn L. Talcott. Vol. 9200. Lecture Notes in Computer Science. Springer, 2015, pp. 475–492.
- [64] Antoine Miné. ‘Static analysis of embedded real-time concurrent software with dynamic priorities’. In: *Electr. Notes Theor. Comput. Sci.* 331 (2017), pp. 3–39.
- [65] Michał Moskal, Wolfram Schulte, Ernie Cohen, Mark A. Hillebrand, and Stephan Tobies. *Verifying C programs: a VCC tutorial*. Working draft, version 0.2. 25 Aug. 2012.
- [66] Yannick Moy, Emmanuel Ledinot, Hervé Delseny, Virginie Wiels, and Benjamin Monate. ‘Testing or formal verification: DO-178C alternatives and industrial experience’. In: *IEEE Software* 30.3 (2013), pp. 50–57.
- [67] Stefan Naujokat, Michael Lybecait, Dawid Kopetzki, and Bernhard Steffen. ‘CINCO: a simplicity-driven approach to full generation of domain-specific graphical modeling tools’. In: *Int. Journal on Software Tools for Technology Transfer (STTT)* 20 (3 2018), pp. 327–354.
- [68] Chris Newcombe, Tim Rath, Fan Zhang, Bogdan Munteanu, Marc Brooker, and Michael Deardeuff. *Use of formal methods at Amazon web services*. Tech. rep. Amazon, 2014.
- [69] AbsInt Angewandte Informatik GmbH. *Fast and sound runtime error analysis*. 21 Apr. 2017. URL: <http://www.absint.com/astree/index.htm#vkb2>.
- [70] AbsInt Angewandte Informatik GmbH. *References. Success stories from our customers: Airbus, Daimler, ESA, Honda, and others*. URL: <http://www.absint.com/success.htm> (visited on 12/03/2019).

- [71] Thomas E. Nichols. *Bibliometrics of cluster inference*. 6 July 2016. URL: http://blogs.warwick.ac.uk/nichols/entry/bibliometrics_of_cluster.
- [72] Thomas E. Nichols and Cyril Pernet. *Has a software bug really called decades of brain imaging research into question?* 30 Sept. 2016. URL: <https://www.theguardian.com/science/head-quarters/2016/sep/30/has-a-software-bug-really-called-decades-of-brain-imaging-research-into-question>.
- [73] Ammar Osaiweran, Tom Fransen, Jan Friso Groote, and Bart J. van Rijnsoever. ‘Experience report on designing and developing control components using formal methods’. In: *FM 2012: formal methods – 18th international symposium, Paris, France, August 27–31, 2012. Proceedings*. Ed. by Dimitra Giannakopoulou and Dominique Méry. Vol. 7436. Lecture Notes in Computer Science. Springer, 2012, pp. 341–355.
- [74] Ammar Osaiweran, Mathijs Schuts, Jozef Hooman, Jan Friso Groote, and Bart J. van Rijnsoever. ‘Evaluating the effect of a lightweight formal technique in industry’. In: *STTT 18.1* (2016), pp. 93–108.
- [75] Luigia Petre, Brijesh Dongol, and Graeme Smith. *Formal methods teaching workshop and tutorial (FMTea 2019)*. Event affiliated with FM 2019, 3rd world congress on formal methods. 2019. URL: <http://fmtea.github.io> (visited on 02/01/2019).
- [76] David Pogue. ‘Why we’re all beta testers now’. In: *Scientific American* (1 Nov. 2014). URL: <http://www.scientificamerican.com/article/why-we-re-all-beta-testers-now>.
- [77] Christophe Ponsard et al. *DEPLOY success stories*. Archived: http://web.archive.org/web/20170320232131/http://www.fm4industry.org/index.php/DEPLOY_Success_Stories. 12 June 2012.
- [78] Christophe Ponsard, Jean-Christophe Deprez, and Renaud De Landtsheer. ‘High-level guidance for managers deploying formal methods in their organisation’. In: *Formal methods for industrial critical systems – 18th international workshop, FMICS 2013, Madrid, Spain, September 23–24, 2013. Proceedings*. Ed. by Charles Pecheur and Michael Dierkes. Vol. 8187. Lecture Notes in Computer Science. Springer, 2013, pp. 139–153.
- [79] Guus Ritzen, Amber Kortzorg, and Rosalyn Saab. *Banken beheren miljarden euro’s, maar hebben hun eigen technologie niet op orde*. 7 Apr. 2016. URL: <https://decorrespondent.nl/4290/banken-beheren-miljarden-euros-maar-hebben-hun-eigen-technologie-niet-op-orde/1140066560490-607f3373>.
- [80] RTCA. *DO-178C software considerations in airborne systems and equipment certification*. Committee: SC-205. 2011.
- [81] RTCA. *DO-333 formal methods supplement to DO-178C and DO-278A*. Committee: SC-205. 2011.
- [82] Research Triangle Institute. *The economic impacts of inadequate infrastructure for software testing*. Planning report 02-3 prepared for Gregory Tassej at NIST. Health, Social, and Economics Research, Research Triangle Park, NC 27709, 2002.
- [83] Hagen Schönfeld. *The paradigm shift in the auto industry caused by e-mobility*. 17 July 2018. URL: <http://www.newequipment.com/industry-trends/paradigm-shift-auto-industry-caused-e-mobility>.
- [84] John Schwartz. *Who needs hackers?* interview with Peter Gabriel Neumann. 12 Sept. 2007. URL: <http://www.nytimes.com/2007/09/12/technology/techspecial/12threat.html>.
- [85] David C. Shepherd and Paris Avgeriou. ‘Stories from the front’. In: *Journal of Systems and Software* 146 (16 Nov. 2018). ISSN: 0164-1212. DOI: 10.1016/j.jss.2018.10.018.
- [86] Jean Souyris, Virginie Wiels, David Delmas, and Hervé Delseny. ‘Formal verification of avionics software products’. In: *FM 2009: Formal Methods, Second World Congress, Eindhoven, The Netherlands, November 2–6, 2009. Proceedings*. Ed. by Ana Cavalcanti and Dennis Dams. Vol. 5850. Lecture Notes in Computer Science. Springer, 2009, pp. 532–546.
- [87] Bernhard Steffen and Tiziana Margaria. ‘METAFrame in practice: design of intelligent network service’. In: *Correct System Design*. 1999, pp. 390–415.

- [88] Bernhard Steffen and Tiziana Margaria. ‘Tools get formal methods into practice’. In: *ACM Comput. Surv.* 28.4es (1996), p. 126.
- [89] Jan Tretmans, Klaas Wijbrans, and Michel Roger Vincent Chaudron. ‘Software engineering with formal methods: the development of a storm surge barrier control system’. In: *Formal methods in system design* 19.2 (2001), pp. 195–215.
- [90] U.S. department of labor. *Occupational outlook handbook*. 2004-05 edition. Claitors pub division, Mar. 2004.
- [91] Manfred Broy unter Mitarbeit von Alexander Malkis. *Logische und methodische Grundlagen von Programm- und Systementwicklung. Teil 1*. 2019. ISBN: 978-3-658-26301-0.
- [92] Mark van den Brand and Jan Friso Groote. ‘Software engineering: redundancy is key’. In: *Sci. Comput. Program.* 97 (2015), pp. 75–81.
- [93] Michiel van Genuchten and Les Hatton. ‘Metrics with impact’. In: *IEEE Software* 30.4 (2013), pp. 99–101.
- [94] Jacques Verriet. ‘Model checking indoor lighting systems – how to transfer the result’. Presentation at the Lorentz Center workshop. 15 Sept. 2015.
- [95] Taylor Walsh. *Unlocking the gates: how and why leading universities are opening up access to their courses*. Princeton University Press, 2011.
- [96] Andy Walter and James J. Hunt. ‘Java in safety-critical systems’. Presented at the conference ‘Embedded World’. 2009.
- [97] Hillel Wayne. *Why don't people use formal methods*. 21 Jan. 2019. URL: <http://www.hillelwayne.com/post/why-dont-people-use-formal-methods>.
- [98] Evie Westland. *Pinautomaten België onbruikbaar na software-update*. 3 Jan. 2017. URL: <http://www.metronieuws.nl/nieuws/buitenland/2017/01/pinautomaten-belgie-onbruikbaar-na-software-update>.
- [99] Benjamin Weyers, Judy Bowen, Alan Dix, and Philippe Palanque. *The handbook of formal methods in human-computer interaction*. Springer, 2017.
- [100] Wikipedia. *Design thinking*. 11 Oct. 2019. URL: http://en.wikipedia.org/wiki/Design_thinking.
- [101] Wikipedia. *Formal Methods*. 14 Oct. 2018. URL: http://en.wikipedia.org/wiki/Formal_methods.
- [102] Wikipedia. *List of software bugs*. 23 Dec. 2018. URL: http://en.wikipedia.org/wiki/List_of_software_bugs.
- [103] Wikipedia. *Scrum (software development)*. 11 Oct. 2019. URL: [http://en.wikipedia.org/wiki/Scrum_\(software_development\)](http://en.wikipedia.org/wiki/Scrum_(software_development)).
- [104] Jim Woodcock, Peter Gorm Larsen, Juan Bicarregui, and John Fitzgerald. ‘Formal methods: practice and experience’. In: *ACM Comput. Surv.* 41.4 (Oct. 2009), 19:1–19:36.