Chapter 27
Architecture and Safety for Autonomous Heavy Vehicles: ARCHER

Viktor Kaznov, Johan Svahn, Per Roos, Fredrik Asplund, Sagar Behere, and Martin Törngren

27.1 Summary of the Project

Machines are converging towards autonomy. The transition is driven by safety, efficiency, environmental and traditional ‘robotics automation concerns’ (dirty, dull and dangerous applications). Similar trends are seen in several domains including heavy vehicles, cars and aircraft. This transition is, however, facing multiple challenges including how to gradually evolve from current architectures to autonomous systems, limitations in legislation and safety standards, test and verification methodology and human–machine interaction.

One of the major challenges for developing a fully automated heavy vehicle is to design and develop a system with an acceptable level of system safety. New principles and methods for system architecture, safety analysis and system verification must be developed to reach the necessary safety level.

These challenges are particularly important in case of fully automated heavy vehicles, i.e. no human driver available in the vehicle, considering vehicle weight, size, life span, operational scenarios and the number of produced variants. The business case for commercial vehicles is also very different from passenger cars, whose prime purpose mostly is to transport the driver. Commercial vehicles are a transport tool, where the driver is not part of the cargo, and constitute roughly one-third of the transport cost.

The purpose of the project ‘Architecture and Safety for Autonomous Heavy Vehicles—ARCHER’ is to develop methods and principles for safety analysis of a fully automated commercial heavy vehicle, to create a reference architecture and
to develop methods and principles for test and verification of fully automated heavy vehicles. Also a proof-of-concept realization for overall verification and validation of the reference architecture and developed methods is included.

The project is building upon experiences and knowledge from finished and ongoing research projects partially funded by Swedish government, such as iQDrive (investigates semi-autonomous heavy vehicles where drivers are still in the loop), iQMatic (prototype autonomous transport system consisting of a fully equipped control room and at least one load carrying unit), FUSE (investigates self-driving cars and functional safety aspects) and ESPRESSO (develops and adapts model-based techniques that improve the quality and reduce the cost for development of embedded systems in trucks and especially safety critical systems) [34].

27.2 Background

The Swedish automotive industry makes up a large and significant part of Swedish exports. For Swedish vehicle manufacturers, the domestic market only represents a small proportion of global sales, whereas the majority of research and technical development work take place in Sweden.

A generational shift is now predicted, with vehicles moving from driver control to fully automated control. This shift has already begun—there are already active systems that intervene in extremely critical situations to avoid accidents and increase safety. Semi-automated functions such as ‘Adaptive cruise control’ are also already in place; the adaptive cruise control is an automated system whereby the driver hands over longitudinal control of the vehicle to the vehicle’s autonomous systems. The adaptive cruise control offers considerable potential for development in terms of achieving improved energy and traffic efficiency. It is also well known that the underlying cause of many single-vehicle and workplace accidents involving vehicles is due to tiredness or distraction, in turn often arising from monotonous driving situations. By automating monotonous tasks, accidents of this type can be prevented, thus \textbf{improving traffic safety}.

The current emphasis and shift towards autonomy is enabled by cost-performance and maturity improvements in sensor, actuator, and semiconductor technology. As a result, the Swedish automotive industry has to adapt and change from a mechatronics engineering industry to becoming a full-blown Cyber-Physicals Systems engineering industry with a large and growing element of vehicle automation software operations as well as vehicle communication; see [1].

With regard to skills development in the field of automation, it is extremely important to launch Swedish projects where automated vehicle concepts are developed and tested in their natural environment. With the aid of tangible research projects applied to robust, autonomous research platforms, Sweden ought to be able to retain its position within vehicle automation at the same time as developing the skills required to cope with the generational shift initially facing work vehicles and subsequently commercial and private vehicles.
It is now clear that a number of activities need to be initiated in order to achieve greater breadth and depth regarding the autonomous vehicles skills area. This is partly a reaction to the ongoing development of society and transport systems and partly due to a clear desire on the part of visionary customers. Areas such as ‘sensor fusion’, ‘functional safety’ and ‘perception’ are receiving strong attention by the automotive industry and in academic research, but there are limitations in efforts that explicitly address electrical system architecture, safety and verification—especially in the context of fully automated commercial heavy vehicles. The absence of a human driver creates specific challenges in case of heavy commercial vehicles considering vehicles weight, size, lifespan and complexity of managing a large number of variants. Furthermore, the development of fully automated heavy vehicles is strongly driven by a clear market demand, since, in most applications, there is no need of the human presence in a heavy vehicle, besides the safety aspects. The proposed project, ‘Architecture and Safety for Autonomous Heavy Vehicles—ARCHER’, complements existing Swedish and international projects on automation with its specific focus on (1) architectures for heavy vehicles; (2) full automation, where a human is not available and (3) verification and validation of E/E systems with focus on safety.

27.3 State of the Art

A brief account of state of the art (SOTA) is here given for safety, architecture and verification.

Safety The standard ISO 26262:2011 Road vehicles—Functional Safety [2] describes the prevailing best practices for achieving functional safety of road vehicles. Currently, it is only adopted for passenger cars, but it will likely be applicable for heavy vehicles within the time frame of the project. Adherence with the safety standard is important not only for the comprehensive coverage it provides throughout the product safety lifecycle (from concept to decommissioning) but also because demonstrating compliance with the prevailing best practices is an important factor for exclusion of liability in case of a system malfunction.

The ISO26262 process requires an early hazard analysis of the system, with the subsequent formulation of safety goals and the determination of Automotive Safety and Reliability Levels (ASILs) for each safety goal. However, it is debated whether the standard is immediately applicable to the development of intelligent, autonomous vehicle functions. One reason for this is that it relies on techniques for hazard and risk analysis in which human involvement, usually in the form of the vehicle’s driver, is an important factor in the estimation of risk reduction levels and the subsequent calculation of ASILs for safety requirements [3]. For a truly autonomous vehicle, the involvement of a human being cannot be counted upon, as a mitigating factor in safety-critical operational situations. Thus, either high ASIL levels will have to be accounted for (assuming no human controllability) or the
existing standard needs to be upgraded to include new concepts of controllability, where machine intelligence replaces the human being.

Functional safety considerations within ISO26262 begin with the analysis of risks and identification of hazards for relevant safety-related systems at the vehicle level (items). There exist a number of tools for low-level risk analysis, like Fault Tree Analysis (FTA) [4], Event Tree Analysis (ETA) [5], Failure Mode and Effect Analysis (FMEA) [6], probabilistic FMEA [7], Hazard and operability study (HAZOP) [8] etc. These tools and methods often provide sufficient support for low-level risk or hazard analysis. However, they typically require detailed design specifications and do not take the dynamic behaviour of systems into consideration. Known challenges for autonomous system design include the shifting of more workload to critical or work intensive time periods [9], tighter coupling making autonomous systems react faster [9], insufficient or inappropriate feedback on system modes [10], too much or too little feedback with regard to the specific user [11, 12], reduction of situation awareness [13], reinforcing of decision bias [13], enforcing limitations that are only appropriate in nominal situations also during extreme situations [12] and encouraging of reliance on automation to a degree at which manual skill decreases [13].

Several approaches have been suggested in the literature to address the lack of detailed design specifications at the early design phase. Of these, the Systems Theoretic Process Analysis (STPA) technique [14] has been shown to be promising for recognizing safety requirements and constraints of the system before detailed design [15, 16]. STPA also addresses the dynamic behaviour of a system, and several authors have reported positive outcomes from applying STPA on various systems [14, 17, 18], including automotive functions like forward collision avoidance [19]. This leads us to believe that STPA might be useful for safety analysis of autonomous systems. The application of hazard analysis techniques in the absence of human involvement remains an area that requires further exploration in the field of autonomous heavy vehicles.

On completion of a hazard analysis, the ISO26262 process continues with the generation of safety goals, ASIL classifications inherited from the identified hazards and the formulation of a Functional Safety Concept (FSC). The FSC is then refined into a Technical Safety Concept (TSC) which provides a basis for subsequent formulation of hardware and software safety requirements. At the various Safety Concept levels, aspects like fail-operational characteristics, redundancy, system monitoring and supervisory control enter the picture. A good overview of system monitoring and supervision concepts, especially for autonomous systems, is provided in [20]. The concepts of supervisory control and fail-operational modes are especially relevant for autonomous vehicles, since no generally safe states exist for an operational autonomous road vehicle. Therefore, it is necessary to investigate methods for supervisory control, the distribution of supervisors in the system architecture and their overall effect on safety argumentation for the system. This is where architecting and architecture comes into the picture as an important aspect of design for safety.
Architecture

The traditional approach for electrical system architectures has been
the usage of self-contained hardware platforms, referred to as Electronic Control
Units (ECUs), connected in a communication network. These ECUs exchange
information via coordinated signals, and this scheme, denoted ‘Federated Archi-
tecture’, allows for good separation of concerns and simplified verification of
the integration. However, Federated Architectures face challenges of increasing
functional complexity, non-optimal resource consumption, emergent behaviour and
cost. To address these, both the avionics [21] and recently the automotive domains
are transitioning towards the so-called ‘Integrated Architectures’ where multiple
functions can be supported by one ECU, and one function can be distributed over
multiple ECUs. Functions, subsystems or even library components can be developed
by different organizations or vendors and may use different platform services while
residing in a single ECU and sharing a limited set of communication channels [22].
This direction, however, will not eliminate the distributed nature of vehicle control,
but may imply a new approach for stronger coordination of high-level control.

The transition to integrated architectures necessitates development of new
methods, tools and techniques for the design and analysis of the architectures. This
includes topics related to mixed criticality systems, multi-core and Network-on-
Chip technologies, optimal mapping and allocation of system functionality among
ECUs, assurance of overall system level technical properties like end-to-end timing
and latency as well as extra-functional properties like system safety, reliability etc.
This, in turn, necessitates development of architecture exploration techniques to
evaluate and determine optimum architectures from the excessively large design
space. Techniques like platform based design [23–25] provide early methodologies
for systematic design of functions, architecture, their mapping, and implementation
of the mapped architecture.

The introduction of autonomous functionality necessitates a critical look at
system architectures and the architecting process. This is because autonomy as
a system level property goes well beyond being ‘just another requirement’. The
robotics and artificial intelligence domains have traditionally led the development of
autonomous system architectures. However, transitioning these architectures to the
automotive domain is not a straightforward process, especially due to the automotive
domain’s requirements with respect to being safety-critical, incorporating legacy
designs, differing development process and business cases and the sheer number of
product variants involved. A thorough analysis of system architectures for autonomy
in various domains is presented in [26], which includes a comparison of domain
characteristics, commonalities and differences.

A promising way forward is the development of reference architectures for
autonomous vehicle systems with the use of existing and new design patterns
and principles that facilitate system integration (academically referred to, e.g.
as compositability and correctness by construction). The reference architecture
approach has already been successful for individual autonomous functions like
cooperative driving [27], and it should be possible to generalize it to the vehicle
level, especially when the entire vehicle E/E architecture is controlled by a single
organization. It is of particular interest to develop common reference architectures
for both autonomous and non-autonomous variants of the same vehicle model. The use of novel autonomy patterns and principles are instrumental for reducing the complexity, thus reducing the difficult task of verification.

**Verification Including Testing** Traffic statistics from the United States of America show that the mean time between fatal crashes is about 2 million vehicle hours and the mean time between injury crashes is over 50,000 vehicle hours [28]. For an autonomous vehicle to be acceptable in society, it will need to be proven substantially safer than this baseline. This is a tough challenge when we consider that a fully automated commercial heavy vehicle would be a product that needs to be affordable to current customers, that needs to operate for the life of a heavy vehicle, which by far exceeds the life span of a passenger car, with a minimum of maintenance, and that is confronted with a highly stochastic operating environment, with hazards that need to be identified and mitigated in a fraction of a second. The extensive design redundancy and intensive preventive maintenance regimes that have made commercial aviation safe are not directly economically viable in the automotive sector. Furthermore, hazardous situations on public streets need to be dealt with more quickly than in the air, because of close proximity among other vehicles and pedestrians.

All these factors increase the testing and verification requirements on autonomous road vehicles. Simultaneously, the increasing complexity and exploding state space in autonomous vehicle architectures make it practically impossible to achieve total test coverage of both the vehicle architecture and its behaviour in all possible scenarios. Achieving sufficient test coverage is simply not possible within realistic product development timeframes, using the traditional approach of constructing a system or component prototype and running a sequence of tests on it. ISO26262 essentially says that the higher the risk, the more efforts and rigour should be spent for design and verification, with hints provided to all kinds of techniques, but without guidelines on how different techniques can be beneficially used and combined. There is thus an imperative need to develop a new verification methodology.

There exist a multitude of approaches to verification and testing, from manual reviews to automated testing. We focus here on model-based approaches which show great promise in dealing with verification and which complement the dominating industrial testing practices [29, 30]. We identify three main approaches for verification of complex systems: (1) simulation, (2) formal verification and (3) verification problem formulation and formalization.

The first two approaches involve the creation of models, i.e. formal representations of the system. In the simulation approach, the models are typically constructive whereas in the second case, the models are typically analytic; see, e.g. [29]. The strengths of simulation-based approaches include their use as constructive design models (where parts can be reused, e.g. for code generation and HIL testing), whereas the drawbacks relate to the impossibility to cover the large state space. Corresponding challenges thus include that of finding relevant test cases and understanding what constitutes relevant coverage. In the second approach, a formal
representation is first created (or possibly generated from a constructive model) and is then analy\nsed for the assurance of specific system properties or absence of undesirable properties. Analysis methods include model checking, theorem provers and other formal methods based on discrete mathematics, formal logic or hybrid formalisms. Strengths of formal verification are the possibility to cover complete parts of the state space and that the requirements and constraints are explicitly captured.

Challenges of formal verification include scalability to realistic size problems and their dependence on the formalized models and the tools required to process them. The approach requires specially trained users, even though there nowadays exists tools to facilitate model creation. The sheer effort in constructing models for a complex system has meant that this approach is not very common outside the development of safety-critical systems (practical usage in the automotive industry is so far limited). A hot research topic is to combine simulation and formal verification approaches; see, e.g. MBAT [31].

The third approach refers to how verification problems are formulated and formalized, involving issues such as the choice of the level and type of formalization of requirements capture, and how constraints and assumptions are captured. Safety incidents are known to frequently stem from incomplete understanding of assumptions and mismatches between models [14]. The formulation of requirements, constraints and assumptions is closely connected to verification by simulation, formal analysis and testing, since it will drive the overall approach to verification and validation, and be closely related to test cases. The use of contracts has emerged as a promising approach for the specification of the system and its components in such a way that the incremental assembly of the system is guaranteed to have the desired properties [32, 33]. Contracts enable explicit descriptions of the context in which components can be used and how they can be combined.

A common challenge for the three approaches is that of dealing with model management and integration, a separate research field in its own right, where ARCHER can draw upon results from the FFI ESPRESSO project and the iFEST ARTEMIS project, including dealing with challenges such as consistency management across multiple models [34, 35].

There is no silver bullet for verification of autonomous systems. The ARCHER hypothesis is that a combination of archite\ncing (reducing complexity), combination of verification techniques (automating what is feasible and putting efforts on the critical and hard to formalize aspects), is the right way forward towards cost-effective verification.

### 27.4 Project Content

ARCHER is considered to be a first step as part of a longer term initiative. A continuation of the proposed project is planned to focus on verification and validation of results from ARCHER in demonstrational trucks and to progress
towards higher TRL’s and to work towards establishing an autonomy competence centre in close collaboration with the KTH ITRL lab.¹

ARCHER contains three main focus areas in the context of fully automated heavy commercial vehicles: (1) methods and principles for safety analysis, (2) methods and principles for system architecture and (3) methods and principles for verification.

The first area is focusing on the safety perspective. As stated in the SOTA part of this chapter, the current safety analysis methods are largely based on a physically present human driver who can act as a last resort in the functionality degradation chain. For the automation levels without an operator, new degradation principles as well as new safety analysis methods and principles must be developed. To exemplify, a few relevant questions in this area are presented below.

- Where do available standards and methods for the safety analysis fall short when applied to fully automated heavy vehicles?
- How should available standards and methods for the safety analysis be improved to provide a reliable and effective methodology for development of fully automated heavy vehicles?
- How should the safety requirements be formulated to handle the trade-off between safety and availability?
- How will safety requirements change depending on the planned operational environment of a vehicle?
- How will principles for human independent diagnosis and diagnostic procedures be defined?

The second area is focusing on the system architecture perspective. A reference architecture (or a set of architectures that cover fundamentally different application scenarios and/or subsystems) will be developed, that fulfils the identified safety, test and operational requirements and addresses architectural bottlenecks, while considering realistic constraints on, e.g. infrastructure availability, legacy system integration and cost efficiency. To exemplify, a few relevant questions in this area are presented below.

- Which architectural principles and patterns should be used to provide an acceptable system safety and cost assuming no human driver presence at all?
- Which architectural principles and patterns should be used to be feasible for actual production of commercial vehicles?
- Which architectural principles and patterns should be used to make system feasible for testing and verification considering level of automation?

The third area is focusing on testing and verification. The verification aspect needs to be included already at design time or even at architectural design as a fully automated heavy vehicle cannot be verified by the current test methods. Principles for efficient testing to reach acceptable safety levels will be developed.

¹The KTH and industry Integrated Transport Research Lab: https://www.itrl.kth.se/
A methodology which combines state of the art testing, simulation and formal verification methods will be developed. The methodology will consider and exploit characteristics in terms of faults/failure modes, behavioural and structure aspects (including architectural patterns), types of verification techniques and formalization including abilities for verification automation, as well as the criticality of faults/risks.

### 27.5 Project Targets

The main expected results from the ARCHER project are:

- methods and principles for safety analysis of fully automated heavy vehicles
- methods and principles and a reference system architecture enabling safe, secure and cost-efficient fully automated heavy vehicles
- methods and principles for test and verification and validation of fully automated heavy vehicles
- Three licentiate theses (half-way PhD thesis in the Swedish doctoral education, to be completed as PhDs in the follow-up project)
- Nine master theses
- increased collaboration between industry and academia

The target of the project is to develop a set of requirements, design principles, methodologies and a reference architecture for development of fully automated heavy vehicles. Given that the majority of industrial projects are at relatively low TRL levels, there is a need to consider architecture in order to deal with complexity, safety, availability and business considerations. Architecture, validation, verification and safety are strongly related, and there is thus a benefit in pursuing them simultaneously. With the proposed focus, ARCHER thereby paves the way for progressing towards higher TRLs.

### References

1. CyPhERS deliverable D3.2. Market and Innovation Potential of CPS. Technical Report by the CyPhERS FP7 project, Aug 2014, [http://www.cyphers.eu/sites/default/files/D3.2.pdf](http://www.cyphers.eu/sites/default/files/D3.2.pdf)
2. ISO 26262:2011 Road vehicles—Functional safety (2011)
3. S. Behere et al., Architecture Challenges for Intelligent Autonomous Machines: An Industrial Perspective, in *Proceedings of the 13th International Conference on Intelligent Autonomous Systems (IAS-13)*, Padova, Italy, 2014
4. C.A. Ericson, Fault Tree Analysis–A History, in *Proceedings of 17th International System Safety Conference*, 1999
5. T. Tobioka, R.C. Bertucio, Use of event tree analysis in development of a LOCA test program. Trans. Am. Nucl. Soc. 39, 590–591 (1981)
6. R. McDermott et al., *The Basics of FMEA*, 2nd edn. (Taylor & Francis, Boca Raton, FL, 1996)
7. H. Aljazzar et al., Safety Analysis of an Airbag System Using Probabilistic FMEA and Probabilistic Counterexamples, in 6th International Conference on the Quantitative Evaluation of Systems, Hungary, 2009
8. J. McDermid et al., Experience with the Application of HAZOP to Computer-Based Systems, in Proceedings of 10th Annual Conference on System Integrity, Software Safety and Process Security, COMPASS, 1995
9. D.D. Woods, Decomposing automation: Apparent simplicity, real complexity, in Automation and Human Performance: Theory and Applications, ed. by R. Parasuraman, M. Mouloua (Erlbaum, Mahwah, NJ, 1996), pp. 3–17
10. B.N. Sarter, D.D. Woods, Pilot interaction with cockpit automation: Operational experiences with the flight management system. Int. J. Aviat. Psychol. 2(4), 303–321 (1992)
11. R.D. Sorkin, Why are people turning off our alarms? J. Acoust. Soc. Am. 84(3), 1107–1108 (1988). doi:10.1121/1.397232
12. R. Parasuraman, V. Riley, Humans and automation: Use, misuse, disuse, abuse. Hum. Factors: J. Hum. Factors Ergon. Soc. 39(2), 230–253 (1997). doi:10.1518/001872097778543886. http://hfs.sagepub.com/content/39/2/230.abstract
13. D.A. Norman, The problem of automation: Inappropriate feedback and interaction, not over-automation, in Human Factors in Hazardous Situations, ed. by D.E. Broadbent, J. Reason, A. Baddeley (New York, Oxford University Press, 1990), pp. 585–593
14. N.G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety (MIT Press, Cambridge, MA, 2012)
15. T. Ishimatsu et al., Modeling and Hazard Analysis Using STPA, in Proceedings of the 4th IAASS Conference Making Safety Matter, p. 10, 2010
16. H. Nakao, M. Katabira, Y. Miyamoto, N. Leveson, Safety Guided Design of Crew Return Vehicle in Concept Design Phase Using STAMP/STPA, in Proceedings of the 5th IAASS Conference, pp. 497–501, 2011
17. S.J. Pereira, G. Lee, J. Howard, A System-Theoretic Hazard Analysis Methodology for a Non-advocate Safety Assessment of the Ballistic Missile Defense System, in Proceedings of the AIAA Missile Sciences Conference, Monterey, California, 2006
18. J. Thomas, N.G. Leveson, Performing Hazard Analysis on Complex, Software- and Human-Intensive Systems, in Proceedings of the 29th ISSC Conference About System Safety, 2011
19. S. Sulman et al., Hazard Analysis of Collision Avoidance System Using STPA, in Proceedings of the 11th International ISCRM Conference, University Park, Pennsylvania, USA, May 2014
20. E. Baudin, J. Blanquart, J. Guiochet, D. Powell, Independent Safety Systems for Autonomy: State of the Art and Future Directions, Technical Report LAAS-CNRS No. 07710
21. C.B. Watkins, R. Walter, Transitioning from Federated Avionics Architectures to Integrated Modular Avionics, in 2007 IEEE/AIAA 26th Digital Avionics Systems Conference, IEEE, Oct 2007
22. M. Di Natale, A. Sangiovanni-Vincentelli, Moving from federated to integrated architectures in automotive: The role of standards, methods and tools. IEEE Proc. 98(4), 603–620 (2010)
23. A. Sangiovanni-Vincentelli, G. Martin, Platform-based design and software design methodology for embedded systems. IEEE Des. Test Comput. 18(6), 23–33 (2001)
24. A. Sangiovanni-Vincentelli, A. Ferrari, System Design—Traditional Concepts and New Paradigms, in Proceedings of ICCD, 1999
25. A. Sangiovanni-Vincentelli et al., Alberto Benefits and Challenges for Platform-Based Design, in Proceedings of the 41st Annual Conference on Design Automation—DAC ‘04, pp. 409–414, 2004
26. S. Behere, Architecting Autonomous Automotive Systems: With an Emphasis on Cooperative Driving, Licentiate Thesis, KTH, Stockholm, 2005
27. S. Behere, M. Törngren, D. Chen, A reference architecture for cooperative driving. J. Syst. Archit. 59(10), 1095–1112 (2013). doi:10.1016/j.sysarc.2013.05.014. Part C
28. S. Shladover, An Automated Highway System as the Platform for Defining Fault-Tolerant Automotive Architectures and Design Methods. NSF CPS Workshop Position Paper, 2011
29. M. Törngren et al., Model based development of automotive embedded systems, in *Automotive Embedded Systems Handbook*, ed. by N. Navet, F. Simonot-Lion. Industrial Information Technology Series (Taylor and Francis CRC Press, Boca Raton, FL, 2008). ISBN 9780849380266
30. A. Benveniste et al., *Embedded Systems Design, The ARTIST Roadmap for Research and Development*. Lecture Notes in Computer Science, vol. 3436 (Springer, Berlin, 2005). doi:10.1007/b106761. ISBN 978-3-540-31973-3
31. MBAT ARTEMIS project, [http://www.mbat-artemis.eu/home/](http://www.mbat-artemis.eu/home/)
32. P. Derler, E.A. Lee, M. Torngren, S. Tripakis, Cyber-Physical System Design Contracts, in *ICCPS ’13: ACM/IEEE 4th International Conference on Cyber-Physical Systems*, 10 Apr 2013
33. J. Westman et al., Structuring Safety Requirements Using Contract Theory, in *SAFECOMP—32nd International Conference on Computer Safety, Reliability and Security*, France, 2013
34. ESPRESSO FFI project, [http://www.vinnova.se/sv/Resultat/Projekt/Effekta/ESPRESSO/](http://www.vinnova.se/sv/Resultat/Projekt/Effekta/ESPRESSO/)
35. iFEST ARTEMIS project, [www.artemis-ifest.eu/](http://www.artemis-ifest.eu/)