FFI

Security framework for vehicle communication

VINNOVA

VOLVO

CHALMERS

Author: Henrik Broberg
Date 2016-02-05
Project within enabling technology

Contents

FFI in short

FFI is a partnership between the Swedish government and automotive industry for joint funding of research, innovation and development concentrating on Climate & Environment and Safety. FFI has R&D activities worth approx. €100 million per year, of which half is governmental funding. The background to the investment is that development within road transportation and Swedish automotive industry has big impact for growth. FFI will contribute to the following main goals: Reducing the environmental impact of transport, reducing the number killed and injured in traffic and Strengthening international competitiveness. Currently there are five collaboration programs: **Vehicle Development, Transport Efficiency, Vehicle and Traffic Safety, Energy & Environment and Sustainable Production Technology.**

For more information: www.vinnova.se/ffi

1 Executive summary

Today's modern cars can have more than 100 computers (Electronic Control Units, ECUs) and about 100 million lines of code [1]. The vehicle safety is improved, but by increasing the number of ECUs and amount of code, you are at the same time potentially increasing the number of possible attacks. The feasibility of attacks on vehicles in the field has been demonstrated by researches, [2] (2010), [1] (2011) and a recent demonstration raised broad awareness on the criticality of the topic (2015) [3][4].

In this project, founded by VINNOVA FFI, we have conducted research and advanced engineering in order to understand threats and vulnerabilities that can lead to risks and develop countermeasures to manage those risks.

Academic research has been done by 2 PhD students, at Volvo Cars and Chalmers, to advance the state of the art in the fields of automotive secure electronic diagnostics, electronics architecture and electronic communication. As a result one PhD thesis has been defended successfully and one licentiate thesis is planned within first half of 2016.

The project results have been used to spread awareness and dialog on risks and how to manage them within the research and development at Volvo Cars and suppliers in particular and to other companies and authorities in general. Several of the projects results are already introduced to market, both as direct functions and as components of several of Volvo Cars electrical platforms (including SPA).

2 Background

Today's modern cars can have more than 100 computers (Electronic Control Units, ECUs) and about 100 million lines of code [1]. The vehicle safety is improved, but by increasing the number of ECUs and the amount of code, you are at the same time potentially increasing the number of possible attacks.

Research by Karl Kosher and others [2] (2010) have shown high potential damage and Checkoway et al [1] (2011) provided evidence that remote attacks is very real. Remote attacks, has recently received a lot of media attention because Charlie Miller and Chris Valasek 2015 showed a successful attack on a car via internet and gained control of vital systems [3] [4]. Fiat Chrysler thus has been forced into a costly repair campaign of 1.4 million cars.

Inadequate awareness of security not only result in a significant risk of direct damage and costly repairs, but also the technology and features to be rejected or postponed and thus lost benefits for customers, business and society.

Over the past five years, information and IT security in vehicles has developed from an area of a few individuals globally, to an area that many companies are trying to grow.

2.1 References

[1] Stephen Checkoway, Damon McCoy, Brian Kantor et al, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", USENIX Security, 2011
[2] Karl Koscher, Alexei Czeskis, Franziska Roesner et al "Experimental Security Analysis of a Modern Automobile", University of Washington, 2010
[3] Charlie Miller and Chris Valasek, "Alert (ICS-ALERT-15-203-01)".[Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-15-203-01, 2015
[4] Andy Greenberg, Wired, "Hackers Remotely Kill a Jeep on the Highway—With Me in It".[Online]. Available: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, 2015

3 Purpose, questions and methodology

The project aims to increase the level of maturity of the technology, process and methodology fields of information and IT security in vehicles.

The central issue is about being able to understand risks and manage risks related to the use of electronics for automation combined with increased networking between the electronics inside and outside the vehicles. From the FFI application:

The overall project goal is to develop security in the future of connected cars. This includes securing the internal network and securing intelligent traffic management systems and other applications requiring communication with external systems.
...
develop ways to measure or verify the outcome of the safety activities.

The project has an academic component to advance the state of art technology and know-how and an industrial part which aims to disseminate knowledge and technology on a broader front at Volvo Cars. The project's academic part consisted of one PhD student at Chalmers and one industry PhD student at Volvo Cars. Both have received guidance from the intuition of Computer Science and Engineering at Chalmers. The project's industrial part consisted of 1-3 FTE (variable over time) who developed technologies and methods, with sufficient maturity and implemented them in the vehicle projects where the needs were greatest.

The method to get the industrial application of academic research follows the pattern of Volvo Cars VIPP program where academic research is spread into the organization through the industrial supervisor. The concepts and the technologies identified in academic research have been further developed by Volvo Cars and implemented in vehicle projects (projects that lead to the introduction of a new model on the market).

Academic research applies the scientific method in current industrial problems vehicle projects and pre-development phase. Much of the work in the project is a continuation of the FFI project Sigyn II (which focused on diagnostics), generalizing how to secure the communication inside the vehicle and also the communication between the vehicle and the outside world.

The academic research can be divided into two main tracks. The first is to ensure communication between the vehicle and the outside world: Vehicle to Infrastructure (V2I) and vehicle to vehicle (V2V), collectively known as V2X. In this part, the issues we have focused on are how to secure the V2X communication in the best way and also how to ensure that the diagnosis including software updating can be done without unacceptable risks.

The second track of the research has been to work with the vehicles' internal architecture with the central question of how to find the most appropriate way to ensure stability (predictable state) for systems and networks in the car. We have been using "social networking techniques" to identify patterns of communication in the vehicle and then automatically propose various optimizations of network solutions.

4 Goals

The project's goals as stated in the application is included below (translated);

Short description of the objectives/motives for the project. Create an integrated framework for IT security in vehicles that include:
• Securing of the vehicle internal network
• External communication V2V and V2I
• Security models for other applications that communicate over the Internet

	Start	*Licentiate*	*Doctorate*
Pierre Kleberger	*2009Q3*	*2012Q3*	*2014Q3*
Asrin Javaheri	*2011Q1*	*2013Q4*	*2015Q4*

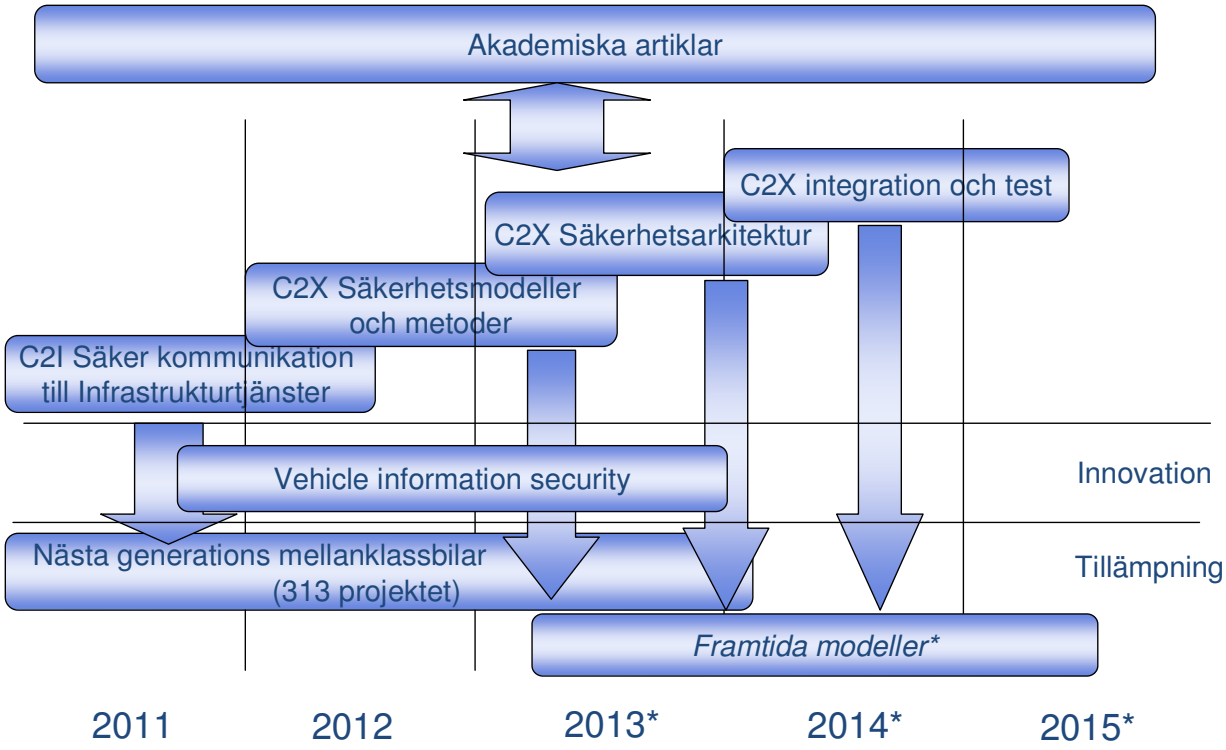

Figure 1, Research strategy and implementation in projects

Work Package secure communications with infrastructure services
Continuing research on how the cars will be able to communicate securely with central IT resources that have been going on up prior to 2012 and the application project implements both for automotive systems and IT systems.

Work Package security models and methods
A working project to develop processes to the next development step in the vehicle platform has begun on the research level to provide input to implementation projects. The strategy is to increase the quality and efficiency of security by taking advantage of the lessons learned from safety in the first work package (secure communication infrastructure services). Results should be implemented in the organization in 2013 in order to be useful as new processes, methods and tools in the work of the next car platform.

Work Package Security Architecture
The next development stage of the car platform has more use cases based on connected services with the need of additional security mechanisms. Further development of the security architecture of the car to be able to handle the increased complexity. New concepts must be provided by the innovation projects at the beginning of 2014.

Work Package C2X communication

Systems for the exchange of information directly between the cars have a different security model than the speed infrastructure services research mainly operated on a regional level (the EU, US, Japan). Target projects are not formulated yet, but Volvo Cars has since the turn of 2011/2012 joined the C2C communication consortium that drives the development and standardization of the area. Participation in research activities at European level provides access to the latest methods, tools and mechanisms of security. The outcome is expected to be the validation and verification (test) methods for certification of the car as part of the network, as well as separation against the other internal network. The work package needs to be delivered in 2014 to be of use in implementing the projects.

Additional information was requested in the quality review of the application:

WP1 - (Research) secure communications with infrastructure services	
Study of state for security in embedded systems in cars and how to evaluate online services in cars. Framework for describing the security features and make the evaluation of embedded systems.	*1. State-of-the art for in-vehicle security.* *2, Guidelines for security evaluation in cars. Article. (Completed before this project. Not part for this FFI-project.)*
Evaluation of wireless diagnosis in a workshop scenario.	*1. Results from study. Report.* *2. Licentiate*
Application of the mechanisms for separation in an in-vehicle network.	*1. Article* *2. Proof of concept*
Robustness tests of the security models of infrastructure services.	*1. Article* *2. Doctorate*
WP2 -4 (Research) Framework for secure communications including C2C communication	
Evaluation of synergies between quality of work "system safety" and "security".	*1. Article methods and adaptation needs of existing quality assurance to address consciously including system failure.* *2. Input to operational development.*
Internal security architecture in the car's embedded systems.	*1. Article on selection of security mechanisms.* *2. Requirement model & threat model as input to projects.*
Case study, design methods and certification for security modules in embedded systems.	*1. Article on application of security mechanisms.* *2,Requirement and threat models for higher assurance levels*
Security test methods for different system levels. Establish a required test set for security concepts.	*1. Article on application of security mechanisms.* *2,test method*

Experimental evaluation of the attack surfaces. Evaluation of the level has improved in the next generation of connected cars compared to the problems raised during 2010.	*1. Article* *2. Proof of concept.* *3. Doctorate*

WP5 - (VCC Advanced Engineering) - Vehicle information security

Develop base technology for authentic software.	*1. Preliminary concept* *2.Bechmark and concept selection* *3.Specification.*
Develop base technology for secure in-vehicle communication	*1. Preliminary concept* *2.Bechmark and concept selection* *3.Specification.*
Develop base technology for authorization enforcement point	*1. Preliminary concept* *2.Bechmark and concept selection* *3.Specification.*
Develop base technology for logging	*1. Preliminary concept* *2.Bechmark and concept selection* *3.Specification.*
Develop base technology for virtualization	*1. Preliminary concept* *2.Bechmark and concept selection* *3.Specification.*
Application of process and methods.	*1. Process model for effective and quality assurance* *2. Analysis template for security assessments* *3. Definitions and educational material.*

WP 6 (VCC industrialization project) Scalable Platform Architecture

Requirement refinement and tailoring to specific EE architecture. *Implementation of authentic software.* *Protocol for communication with VCC infrastructure.* *Verification of functionality*	*1. Requirement specifications* *2. Test specifications* *3. Reports*
Methods for efficient and quality assurance.	*1. Process* *2. Templates and guidelines*
EE architecture development	*1. EE architectural specifications* *2. Integration plan*
Verification of functionality	*1. Test specifications* *2. reports*

Reprioritisation of techniques have been made, but the goals have largely remained the same except for a deviation of the objective of industrial doctoral student. Asrin chose to terminate the doctoral studies and employment after one year. The goal has been adjusted to have an industrial PhD student to defend a licentiate in this project. The project VIS ("Vehicle Information Security", an internal Volvo Cars AE project), has been extended since the application was made, with both updates of concepts and new concepts. Recruitment of a new industrial PhD student caused the plan to be delayed for 6 months and after dialogue with VINNOVA it was decided that the original payment plan would not change. Volvo Cars committed to finance industrial PhD student to June 2016 (i.e. 6 months after the original plan).

5 Results and deliverables

The academic plan for Pierre Kleberger (WP1) has been adjusted in time and for personal reasons the defence of his thesis was delayed to September 2015 (1 year compared to plan). The scope has been adjusted to not include the testing but have focused on the validation of the concept and system phases. See the list of publications for concrete delivery, a brief description of how the deliveries and the ideas explored the contribution to the objectives, here.

Methods used in the telecommunications industry have been the base for Pierre's research in which he proposed a simplified version to justify appropriate protection strategies for connected vehicles. In the industrial application of diagnosis over IP network (Ethernet / Wi-Fi) and remote diagnostics, the method has been used in the development and in vehicle projects to systemize decisions on security level and concept selection. The method has been further simplified in order to be suitable for application to smaller projects and functions to justify protection strategies. The method has been elaborated further in within the frames of the FFI project HeavenS.

Formal verification has been explored at the academic level to verify the protocol design. This method is interesting as a reference, but is too advanced for any broader industrial application currently. Some components (such as protocol design, cryptographic modules, etc.) are already today applicable for formal verification, but then performed by specialists further down the supply chain. For vehicle manufacturers it is a matter of knowing on which elements it is desirable and possible to apply the method.

The reference model that Pierre developed is used as a reference in the system design. Direct adaptation of model-based development at Volvo Cars is a too big a task to be fit in to this project, but it is now used as a reference model by experts when teams need support in their evaluation.

As a direct result, we have been able to influence future ETSI standards in the V2X area and also gained valuable experience in how future standards can and should be used in our own vehicles. The research has also led to the development of a protocol for

accreditation of service equipment in the workshops with the aim of protecting the vehicles from faulty software updates or unauthorized modification of the vehicle's software.

The result of this part of the project has led to an automated tool that, given a desired functionality of the system, suggests an ideal topology, i.e. how all the ECU's in the vehicle are to be connected and finding the most appropriate way to divide the network into a number of smaller network domains. We have been using "social networking techniques" to identify patterns of communication in the vehicle and then automatically proposed different solutions. The proposed solution which is somehow optimised from a security point of view can then be used as a reference model that designers can compare existing solution proposals.

Pierre has explored how the car's network architecture can be optimized to achieve better security attributes and the work was done as a collaboration with Nasser. It is a job that was handed over to the project working with EE system architecture and which is used as an input for the next upgrade of the SPA platform.

The academic plan for the industrial PhD's (wp2-4) was reworked from the bottom when Asrin choose to end her studies and employment after about a year. Nasser Nowdehi was recruited six months later after finishing his master thesis graduation project at Volvo Cars. Today he follows a plan where the licentiate degree will be completed in spring 2016. The review of both Chalmers and Volvo Industrial PhD program was done in 2015 with positive results.

Nasser's first paper is about weaknesses in the cryptographic design of the proposed ETSI standard for secure V2X communication and how these could lead to robustness problems of the system itself. The paper illustrates one aspect of security issues that usually are not as apparent as to circumvent cryptography, to obtain secrets or circumvent access control. In this case it was even the cryptography solution which introduced the attack vector.

Cooperation with Pierre about the optimization of the car's network architecture is already mentioned above.

The Project Vehicle Information Security (VIS) (WP5) have developed technologies to handle threats to a level of maturity suitable for application in vehicle E/E platforms in a number of projects (313 project in the picture above, but also the SPA platform, where the XC90 is the first model) .
All techniques that were planned have not been pursued to base technology, but they have been terminated or passed to the function-owners (and therefore fell outside the scope of the VIS project). With the delivery of the Sensus Cloud (313 project in the picture above) some of the functions were taken over as base technologies.

Collaboration on security has been made with projects on several levels (architecture and in some cases, functions and subsystems) which have resulted in requirements and solutions in different specification levels that are difficult to describe without a going in details on the internal structure of the VCC documentation.

The processes and methods that have been used in the overarching framework for the security work have primarily focused on Volvo Cars existing information and on experience from the IT Security work that has been performed at Volvo Cars. In the framework we have focused on a few "hard points" in the processes to obtain harmonization between IT and R&D. An initiative to develop a development process adapted to the vehicle industry (SAE J3061) has been monitored in order to cherry pick appropriate parts. Work for harmonization of security processes with systems safety processes (ISO 26262) has given practical results. The results are not formalized in the Volvo Cars quality management system, but is part of best practices (e.g. information, contacts and templates on the intranet)

5.1 Delivery to FFI-goals

The program Electronics, Software and Communications (EMC) today following overall objectives (ICFTU, 2014):

Generally
Cooperation programs and projects within the overall theme areas Climate & Environment and Security clearly contribute to:

- *Through increased research and innovation capacity in Sweden safe vehicles industrial competitiveness and jobs in the long and preferably also in the short term.*
- *Develop globally connected and competitive research and innovation environments in which, among others, academy, institute and industry work together.*
- *Promote international research and innovation activities where the conditions for and participation in EU framework programs and other international research and innovation cooperation carefully evaluated.*

EMC-specific
• Raising the technological maturity (by measuring the "technology readiness level," TRL) and more efficient methods in product development to speed up the industrialization of the results and increase customer value.

Comments See Front:

- Capacity building in the area of information security and IT security has increased the competitiveness of individuals Chalmers and companies in the region (not only project participants)

- Today, western Sweden is part of a global research and innovation environment for automotive security.
- Volvo Cars is not part of the EU's framework programs in this area
- The degree of maturity has been increased for many technologies and methodologies and has served as the enabling technology in several projects.

6 Dissemination and publications

6.1 Knowledge and results dissemination

How has / planned project results will be used and disseminated?	Mark with X	Comment
Increase knowledge within area	X	Academic pedigree and breadth (e.g., survey articles) Industrial application specifications via new methods and knowledge to VCC employees in general and decision makers (line managers, project managers, architects, functional owners, designers, test developers) in the VCC in particular.
Passed on to other advanced technological development	X	At research level: HeavenS, HoliSec At industrial level: VIS. Sensus Cloud
Passed on to other product development projects	X	For the development of the VIS project was carried out within the project, provided by the truck project.
Introduction to market	X	Several of the techniques in production in several projects (notably in the SPA platform)
Used in investigations / regulatory / licensing / political decisions	X	Project results have been in dialogue with the authorities, including the US DOT, NHTSA, and European Commission.

The FFI projects HeavenS, the Company and its partners have access to the results and contacts to create synergy. In practice the work has been conducted together even if accounts have been kept separate.

6.2 Publications

Title/author
#1 Security aspects of the in-vehicle network in the connected car P Kleberger, T Olovsson, E Jonsson IEEE Intelligent Vehicles Symposium, Proceedings. Baden-Baden, 5-9 June 2011
#2 An In-Depth Analysis of the Security of the Connected Repair Shop P Kleberger, T Olovsson, E Jonsson The Seventh International Conference on Systems and Networks Communications (ICSNC), Proceedings. Lisbon, 18-23 November, 2012
#3 A Framework for Assessing the Security of the Connected Car Infrastructure P Kleberger, A Javaheri, T Olovsson, E Jonsson The Sixth International Conference on Systems and Networks Communications (ICSNC), Proceedings. Barcelona, 23-29 October 2011
#4 Protecting Vehicles Against Unauthorised Diagnostics Sessions Using Trusted Third Parties P Kleberger, T Olovsson Proceedings of the 32nd International Conference on Computer Safety, Reliability and Security (SAFECOMP). Toulouse, Sept. 2013
#5 A Structured Approach to Securing the Connected Car P Kleberger Licentiate Thesis, Chalmers University of Technology
#6 Security Concerns in Communication with the Connected Car using DoIP P Kleberger, A Javaheri, V Izosimov, H Broberg 15. Internationaler Kongress Elektronik im Kraftfahrzeug; Baden-Baden, Germany. Oct 2011.
#7 Mapping Systems Security Research at Chalmers M Almgren, Z Fu, E Jonsson, P Kleberger, A Larsson, F Moradi, T Olovsson, … Deliverable D2. 3: 1st Project Workshop Proceedings, 66
#8 Formal Verification of an Authorization Protocol for Remote Vehicle Diagnostics P Kleberger, G Moulin IEEE Vehicular Networking Conference (VNC), Proceedings. Boston, 16-18 Dec 2013
#9 Securing Vehicle Diagnostics in Repair Shops P Kleberger, T Olovsson Computer Safety, Reliability, and Security (SAFECOMP), Florence, Sept 2014.
#10 Experiences from implementing the ETSI ITS Secured Message service N. Nowdehi, T. Olovsson **2014 IEEE Intelligent Vehicles Symposium. June 8 - 11, 2014, Dearborn, Michigan, USA**
#11 Towards Designing Secure In-Vehicle Network Architectures Using Community Detection Algorithms

P. Kleberger, N. Nowdehi, T. Olovsson
IEEE Vehicular Networking Conference (VNC), Proceedings. Paderborn, Germany. 3-5 Dec. 2014 (2157-9865). p. 73-80. (2014)

#12 Improving In-Vehicle Network Architectures Using Automated Partitioning Algorithms
Nowdehi, Nasser; Kleberger, Pierre; Olovsson, Tomas
IEEE Vehicular Networking Conference (VNC), Proceedings. December 16-18, 2015, Kyoto, Japan (2015)

#13 Akademisk avhandling för avläggande av doktorsexamen: On Securing the Connected Car - Methods and Protocols for Secure Vehicle Diagnostics
Pierre Kleberger. Institutionen för data- och informationsteknik, Nätverk och system, Chalmers University of Technology, 2015. ISBN: 978-91-7597-241-1.- 197 s.

7 Conclusions and future research

The next step is to increase the level of maturity of existing methods and technology and adding new, so that a reproducible and consistent quality can be maintained in identifying the right measures and to implement and quality assure them effectively.

Our goal is to continue our work to integrate safety and techniques in the development of cars. The focus is not only to be able to find a sufficient level of protection to deal with the risks, but also the efficiency by identifying risks in earlier and earlier stages of development where there is greater scope for redesign or compensatory measures. This means continuing development of methods to analyse threats, vulnerabilities and risks to achieve better scalability, efficiency and reproducibility. Improve harmonization of the methodology to other quality assurance methods (as robustness analysis and testing) for both standard and enhanced quality assurance when personal safety is in question (ISO 26262).

Technically there is a need for further development of techniques to manage risk in a simpler way. Simplicity and integration of the platform in a scalable way are areas that need improvement in order to allow for new ideas to be realized without having information security and IT security becoming an obstacle and to avoid mistakes. Different techniques to increase quality and reduce lead times for information about weaknesses and emerging threats are needed both within and outside the car.

Areas closest to the continued research
• The risks and the countermeasures are similar to and different from other risks in the automotive manufacturing
• How techniques such as cryptography, firewalls, etc. better can be applied in automotive electronics
• Methods to find the right level of protection,
• Quality assurance of safety features and technology
• Quality assurance of features and technology to avoid flaws that can be exploited

• Inclusion of regular quality (productivity)
• Integration with the operating field for deviation (incident preparedness)

8 Participating parties and contact person

CHALMERS

031-77210000

Erland Jonsson (erland.jonsson@chalmers.se);

Tomas Olovsson (tomas.olovsson@chalmers.se);

Pierre Kleberger

VOLVO

031-59 0000

Borg, Jörgen (94140) (jorgen.borg@volvocars.com)

Calais, Kristian (94142) (kristian.calais@volvocars.com)

Nowdehi, Nasser (nasser.nowdehi@volvocars.com)

Broberg, Henrik (henrik.broberg@volvocars.com)