

Remote Shutdown of Heavy Duty Vehicles



Roman Mikulec

Division of Industrial Electrical Engineering and Automation
Faculty of Engineering, Lund University



Södertälje, 7th January 2008

This final thesis for a Master degree in Electrical Engineering was carried out at Scania Fleet Management in Södertälje, Sweden. The aim of the thesis is to study remote vehicle immobilization.

Abstract

Today, vehicles are equipped with advanced electronics and complex alarm systems but still vehicle and cargo theft is a huge problem around the world.

After struggling with this issue for several decades, the government in Brazil finally had enough and voted that all new vehicles manufactured or imported to the country are required to be equipped with an electronic device enabling tracking and immobilization of the vehicle if stolen. Remote immobilization could be a possible solution to prevent vehicle theft and also give the authorities a way to reclaim valuable cargo from stolen vehicles.

Since Scania was already developing a telematic unit with the purpose of tracking vehicles and analyzing vehicle data, this thesis was started to investigate if it was possible to use the unit and the current system for remote immobilization as well. Security of the system would be the key issue since a flaw in security could give unauthorized access to stop vehicles and this would certainly be a disaster.

A prototype system was created to test the reliability and performance of the system.

Contents

1	Background	1	11	Testing	39
2	Introduction	3	11.1	Breaking the silence	39
2.1	Scania Fleet Management	3	11.2	Modifying engine performance	39
2.2	Communicator 200	3	11.3	Testing performance	39
2.3	Remote shutdown	3	12	Results	41
2.4	Project requirements	5	12.1	Test results	41
2.5	Resources	5	12.2	Vehicle immobilization	41
2.6	Limitations	5	12.3	Performance test	41
2.7	Abbreviations	5	12.4	Security	41
2.8	Thesis outline	5	12.5	VOR	41
3	Underlying technologies	7	13	Conclusion and future work	43
3.1	Introduction	7	13.1	Conclusion	43
3.2	GPS	9	13.2	The future of remote shutdown	43
3.3	GSM	11	13.3	Endless possibilities	43
3.4	GPRS	13	14	References	44
3.5	CAN	15	15	Abbreviations	45
4	Existing FMS in Brazil	19	16	Figures	46
4.1	Scania	19	17	Tables	46
4.2	Mercedes	19	18	Appendix A	47
4.3	MAN	19	18.1	Scania thesis proposal (Swedish)	47
4.4	Renault	19	19	Appendix B	48
4.5	Volvo	19	19.1	The accident	48
5	Fleet management services	21	20	Appendix C	49
5.1	Scania fleet management services	21	20.1	Scania CV AB	49
6	FMS hardware	23			
6.1	Scania telematic unit	23			
6.2	Interactor 300 and Interactor 500	23			
6.3	The need for new hardware	23			
7	Communicator 200	25			
7.1	Appearance	25			
7.2	Hardware	25			
7.3	Software	25			
7.4	Testing	25			
7.5	First time configuration	27			
7.6	Current status messages	27			
8	Remote shutdown	29			
8.1	Performing a safe shutdown	29			
8.2	Risk factors	29			
9	Security	31			
9.1	Unauthorized access	31			
9.2	Physical robustness	31			
10	New software	33			
10.1	Creating a prototype	33			
10.2	Remote shutdown GUI version 1.0	33			
10.3	Remote shutdown GUI version 2.0	33			
10.4	Blocking information	35			
10.5	Vehicle information	35			
10.6	Application design considerations	37			
10.7	Remote shutdown application module	37			
10.8	Modifications to existing software	37			

Acknowledgements

I am grateful to many people at Scania Fleet Management for their support with my thesis project, especially my supervisors Mathias Björkman and Mats Axelsson.

I would like to send a special thanks to Magnus Rosenius for all the help to get started and troubleshooting the prototype software.

Thanks to all the readers for comments and opinions about the text and images.

1 Background

We live in a world of continuous expansion, where cities are born every day and people are on the move both day and night. We are now, more than ever dependant on the uninterrupted transportation which supply us with the necessities to cope with everyday living. Bananas from Brazil, wine from South Africa and electronics from China are just a few examples of products that travel thousands of miles to end up in our living rooms.

The transportation industry, the most vulnerable link in this process, has under the last decades struggled with the increasing number of crime and cargo thefts. Figures 1 and 2 show the sad reality for many companies and drivers around the world. Not often do we realize that it is we, the end customers who are left with the bill.

A study made by Scania and Volvo in Brazil showed that almost 13% of transportation prices was a direct consequence of all thefts, damages and other fees which affect the transportation industry [8]. In an attempt to gain control over this negative trend, the government of Brazil proposed a new law which forces the vehicle manufacturers to deal with the problems. The law requires all vehicles to be equipped with an electronic unit which continuously monitors the vehicles position and makes it possible to immobilize the vehicle if necessary [9]. The law, applicable from 1st of August 2009 put great pressure on the vehicle manufacturers since they are unable to sell a single vehicle without an approved security system [9].

1.1.1 Brazilian law summarized

All vehicles produced in Brazil or imported must be equipped with an anti-theft device starting from 1st of August 2009.

The anti-theft device must execute the function of tracking the vehicle and send positioning information to a service monitoring central.

The anti-theft device must be able to execute remote blocking commands from a service central and shut down the vehicle.

Since the Brazilian market is of high importance to Scania and also one of the biggest manufacturing locations for heavy duty vehicles the pressure was high to fulfill the requirements and maintain the production flow.

Development of a new electronic control unit, was quickly ruled out since it would take several years to introduce a new unit and the time available was simply too short. In order to fulfill the new requirement, engineers at Scania began looking at other possible solutions. The preliminary study pointed at two options:

- Upgrade an existing unit with the ability to immobilize the vehicle.
- Introduce a 3rd party unit with very limited insight of their development process.

In January 2008, a thesis was started to investigate if the first option was feasible.

The harsh development in Brazil

During the last twenty years, the crimes against the transportation industry have risen with shocking numbers and cargo theft has become a huge problem all over the world.

Figure 1

Cargo Theft, Number of Incidents

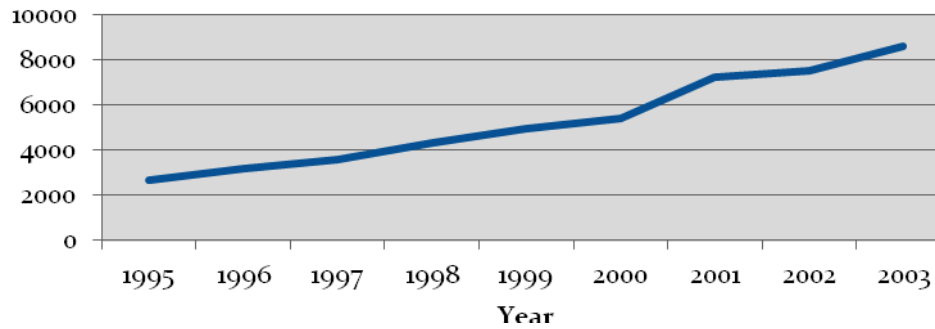


Figure 1 shows the increasing number of incidents over the years in Brazil [8].

Figure 2

Cargo Theft, Total value in Million USD

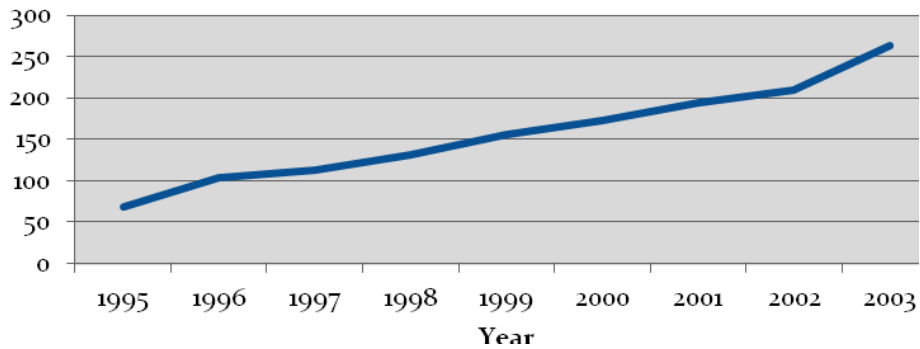


Figure 2 shows the total cost in USD due to crimes against cargo vehicles in Brazil [8].

2 Introduction

2.1 Scania Fleet Management

Scania Fleet Management is a collection of services which gives the customer a comprehensive possibility to follow up the entire fleet [17]. Since Scania has access to all onboard information, the only limitation is set by the developers' imagination. Some examples of how fleet management services can be used can be seen in figures 3 and 4 on the next page.

No matter if the customer is interested in supervising fuel economy of the individual drivers or in need to integrate the vehicles in an advanced order support system, Scania has the solution to satisfy the customers need.

This gives Scania a considerable advantage in the pursuit for new customers. More information about the Scania FMS can be found in the next chapters of this thesis or on the web [18].

2.2 Communicator 200

The Communicator 200 is the result of Scania's decision to expand its product portfolio into the world of Internet services. This small electronic unit with a built in GPS and GSM module is the actual heart of the Fleet Management System. With predetermined time intervals, the unit sends relevant vehicle information to a server where the information is stored, analyzed and presented.

The customer can easily log on to the Scania FMS portal through the Internet, access the information and control the entire fleet around the clock.

The Communicator 200 unit will be explained in more detail later in this thesis.

2.3 Remote shutdown

Remote shutdown of vehicles is associated with a great deal of difficulties where security, by far, is the greatest challenge. The last thing Scania wants is to provide a possibility for unauthorized people, with computer knowledge to turn off vehicles out on our streets. How does one create a solution that provides security today, but also in the future? To find potential flaws in security, the entire chain of communication was analyzed, from the end customer down to the engine. The result of this study will be presented later in this thesis.

At an early stage of this project some restrictions were made. The possibility to immobilize the vehicle would not be offered from the FMS portal, this would only be done by an authorized group of people from Scania Assistance [b]. This due to the risks involved in remote immobilization. You can read about a horrible accident associated with remote immobilization at the end of this thesis.

In order to meet the Brazilian requirements, some changes are needed inside the vehicle. It should not be possible to manipulate the device or remove it without blocking the vehicle. Furthermore, each device must be unique and tied to a single vehicle only. This makes it impossible to steal an immobilized vehicle with a similar device from another vehicle.

These are just a few problems facing the realization of remote shutdown.

Fleet management solutions

There are a number of different 3rd party fleet management solutions which can show information about fleet location. There are even systems which provide estimated driving distances and advanced graphical interfaces. But Scania can offer so much more...

Figure 3

Economy

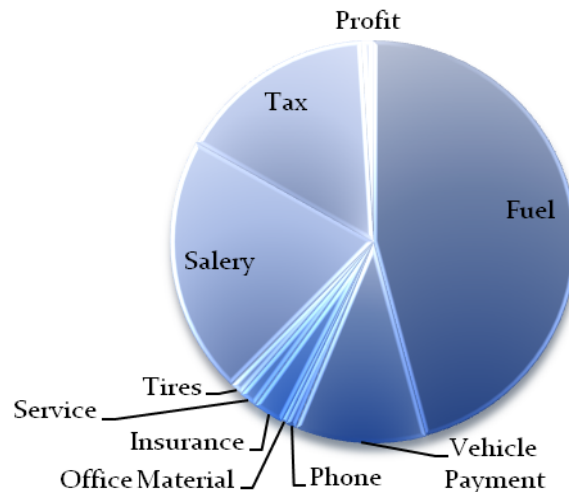


Figure 3 shows an overall summary of a long haulage contractor [k]. By integrating the fleet management system with the order support system, keeping track of economy becomes much easier.

Figure 4

Fuel Consumption

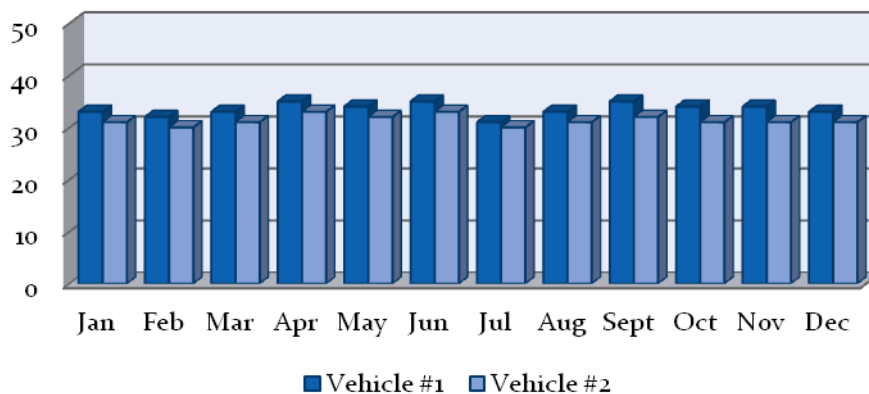


Figure 4 shows an example of how fleet management can be used [k]. The Fleet management system gives the customer the possibility to compare fuel economy of different drivers or different vehicles. The information can then be used to educate specific drivers to a more ecological driving or as support when buying a new vehicle.

2.4 Project requirements

In the first part of this project, security of the existing system was analyzed and potential risks for unauthorized access were evaluated. Part two resulted in a prototype system ready for real-time testing and measurements. The prototype takes requests from an office application and sends data to a server according to the specified protocol.

2.5 Resources

This thesis has a focus on security so the investigating part of the thesis concerns product review and evaluation. Therefore, much of the resources have been internal data sheets and product specifications, rather than scientific articles. Some of the information has been acquired from our co-workers in Brazil and also the National Road Administration in Sweden has been contacted for suggestions and opinions.

2.6 Limitations

This thesis studies the communication and the security inside and between vehicles and the Fleet Management Portal. It will not be a study on vehicle stopping techniques although the topic will be briefly discussed.

2.7 Abbreviations

A list at the end of this thesis contains all abbreviations and a more detailed explanation if none is present directly after they are used.

2.8 Thesis outline

The first two chapters were meant to give the reader a rough assessment of the background to this thesis.

The next chapter describes the communication technologies used inside and outside the vehicle. Readers already familiar with the technologies used can skip this chapter.

The fourth chapter is a short review about other brands and their fleet management services.

Chapter five describes the Fleet Management system in more detail and how it works today.

Chapters six and seven will further study the core of the FMS, the telecommunication device located in the vehicles.

Chapter eight highlights some of the risk factors present when performing a remote shutdown.

Chapter nine covers the different security issues present in the system today and how the system can be approved.

The following chapter describes the development of the new office and vehicle applications.

Chapter eleven describes the prototype testing.

The last two chapters give my conclusions of this thesis and some suggestions on future work.

Throughout the thesis the reader can find short but interesting facts related to the thesis.

Contact information

The following people have been involved in this thesis. If you have any questions feel free to contact us.



Roman Mikulec
Thesis Student
LTH
☎ +46 739232693
✉ roman@bolina.hsb.se



Mathias Björkman
Thesis Supervisor
Scania CV AB
☎ +46 855381000
✉ mathias.bjorkman@scania.com



Mats Axelsson
Thesis Supervisor
Scania CV AB
☎ +46 855381000
✉ mats.axelsson@scania.com



Gunnar Lindstedt
Thesis Supervisor
LTH
☎ +46 462229452
✉ gunnar.lindstedt@iea.lth.se



Ulf Jeppsson
Examiner
LTH
☎ +46 462229287
✉ ulf.jeppsson@iea.lth.se

3 Underlying technologies

3.1 Introduction

This chapter will explain the fundamentals of technologies used by the project prototype. See figures 5 and 6. It is not meant to be a complete description, but rather an orientation to help the reader understand possibilities and limitations of the studied task. The first part of the chapter will describe the technology behind vehicle positioning, the second part the wireless communication with the vehicles and the third and last part the communication used inside the vehicles. Readers already familiar with these technologies can skip this chapter.

3.1.1 Vehicle positioning

The planning and distribution of workload is a hard and time-consuming task [k]. Like a huge puzzle, the dispatcher must optimize each vehicle route in order to maximize the profit. Today, most of the companies keep in touch with the fleet by mobile phones and planning is done completely manual. When new work arrives, the dispatcher must contact several drivers to learn their current positions and give them new instructions. With fleet management systems, vehicle positions are monitored around the clock by GPS receivers in the vehicles which makes planning, route optimization and communication much easier. Read more about the GPS system on page 9.

3.1.2 Communicating with the vehicles

When data needs to be exchanged with moving targets, or from remote locations, wireless communication is desirable. There are a number of techniques available with different focuses regarding range and bandwidth. The current Fleet Management Services, has low demand on bandwidth, but requires countrywide coverage. For this type of applications the GSM network is the most suitable candidate today [c]. Read more about the GSM and GPRS systems on page 11.

3.1.3 Communicating inside the vehicle

The amount of signals sent between different electronic units in the vehicle makes it practically unfeasible to use discrete wires for each signal. In the year 1996, Scania introduced a high speed data bus to distribute the high amount of information needed by the electronic units. Over the years it has been developed into the robust, high quality system used today. Read more about the CAN network on page 15.

Quick Facts

Scania's truck range consists of three series: distribution vehicles, called the P-series, long haulage vehicles, called the R-series and the construction vehicles called the G-series [3].

Underlying technologies

With the click of a button, the manager sends new orders to the driver, luckily unaware of the vast amount of technology involved in passing on each message: Ethernet between computers, fiber optics between servers, wireless communication in the GSM network and CAN messages inside the vehicle. The most fascinating about it is the low latency and high reliability of the whole system.

Figure 5

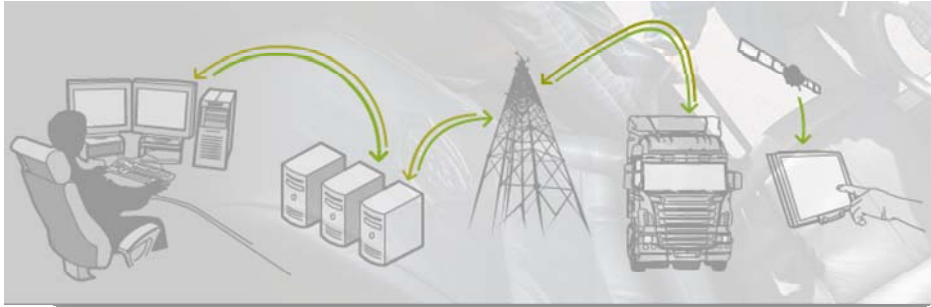


Figure 5 shows the different technologies used by the fleet management system. For the everyday user, technologies like GPS, GSM, GPRS and CAN are well hidden behind the easy-to-use graphical interface of the PC or the onboard computer. The complexity of such systems also make troubleshooting difficult and time consuming since people from each area need to be involved [f].

Figure 6



Figure 6 illustrates the first generation of the Scania on-board computer. The easy-to-use graphical interface gives the driver access to all important information about the current job. Orders, messages and other relevant information are always just a click away.

3.2 GPS

3.2.1 Global positioning system

The Global Positioning System, GPS, was developed by the United States Department of Defense during the seventies and eighties and became operational in 1993 [20]. In the beginning, the system operated in two parallel modes; one with higher precision that was encrypted and reserved for US military, and one with less precision that was free to use by the public. Today, GPS is the most common technique used when determining location, speed, direction, and time in mobile devices. See figure 7.

3.2.2 GPS satellite system

The core of the GPS infrastructure consists of 31 satellites in orbit and a set of satellite tracking stations around the world [20]. See figure 8. The satellites orbit on an altitude of 22.000 km from the earth surface and travel with a speed of 11.265 km/h. The satellites are equipped with considerable batteries and powered entirely by solar energy which keeps them operational around the clock.

3.2.3 Satellite management

The satellite constellation is managed by the US Air Force through a number of tracking stations around the world [20]. In order for the receivers to calculate the position of all satellites, the orbits must be extremely stable. For this reason periodic navigational updates are sent to the satellites and if a satellite is deviating from its orbit it will be taken offline and the orbit will be corrected to keep it on course.

3.2.4 GPS time

Another important variable for calculating position is time. Time is used to measure the distance to all visible satellites by calculating how long it takes for the signal to reach the receiver. Since it is practically impossible to equip every receiver with an expensive and precise atomic clock another solution was implemented. The satellites are equipped with highly precise atomic clocks and transmit the current time in the beginning of every GPS message [20]. This makes it possible to use ordinary quartz crystals in the receivers which are continuously set to current time with every received message. The atomic clocks in all satellites are also corrected by the surveillance central in predefined intervals to ensure all satellites remain synchronized to the GPS time.

3.2.5 GPS accuracy

In the past the accuracy was limited by a random noise applied to the civilian satellite signal by the US Department of Defense to limit non military accuracy. In the year 2000, this random signal was removed and the accuracy today is mostly limited by the multipath propagation [20]. The distance to all visible satellites is calculated by multiplying the time, Δt , it takes for the signal to reach the receiver with the signal propagation speed, the speed of light 299,792,458 m/s. When a reflected signal is received, the path of the signal is longer than in free sight which affects the calculations thus bringing down the accuracy. Buildings and objects often reflect and block the satellite signal, making it hard, sometimes impossible to receive. Clock synchronization is very important for accuracy since one microsecond offset in the receiver causes an error of 300 m in distance. An ordinary civilian GPS receiver has an accuracy of about 15 meters.

3.2.6 GPS signals

A typical GPS receiver calculates its position using the signals from at least four GPS satellites. These transmit precise microwave signals which enables a GPS receiver to calculate its position, speed, heading and precise time. The information is sent in 1500 bit frames with the speed of 50 bit/s using a frequency band in the gigahertz area [20]. Each frame contains the current GPS time, information of the satellite orbit and information of the satellite constellation.

3.2.7 GPS future

With the planned release of the European navigation system Galileo which should be ready for use in 2014, the accuracy could be improved by a factor 10. Since there is no better way of determining the position with unchanged accuracy at the moment, GPS will be in use for the years to come [a].

Quick facts

The first GPS satellite was launched in February 1989 and the most recent launch was in May 2010. The oldest satellite still operational was launched into space in November 1990 [20].

Global positioning system

Today GPS modules are small and cheap which make them perfect for automotive and handheld devices.

Figure 7



Figure 7. GPS is today by far the most common technique used when determining location, direction, speed and time in mobile devices. Devices small enough to fit in your palm can easily contain map information of the entire world.

Figure 8

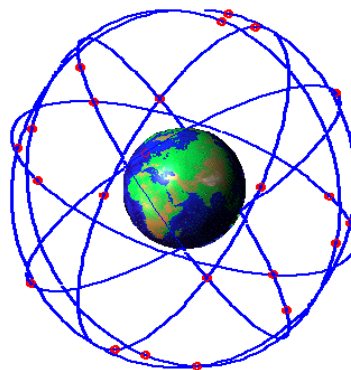


Figure 8 illustrates the satellite constellation of the GPS orbiting 22.000 km above earth with a speed of 11.265 km/h. Data from at least four satellites is needed for the receiver to determine its position.

By using data from a higher number of satellites, accuracy is improved.

3.3 GSM

3.3.1 GSM

The Global System for Mobile telecommunications, GSM, standard was developed in the eighties to address the problem of compatibility between numerous telecommunication systems that had emerged [1]. A first version of the standard was completed in 1990. Since then, the system has been adopted around the world, and new versions of the standard have been released, allowing higher data rates and new features in the networks [13].

3.3.2 The GSM network

The basic GSM network is circuit switched, just like an ordinary land line telephone network. When a call is established between two nodes, the link in-between is busy, regardless if anything is being transmitted or not. To allow many simultaneous calls over the radio link, GSM uses multiple frequency channels around its basic working frequencies. One set of frequencies are used for uplink and one set for downlink. These frequency channels use Time Division Multiple Access, TDMA, to further increase the number of parallel users [1]. TDMA means that a channel is chopped up into a set of repeating time slots, eight to be precise. Each cell phone is given its own frequently recurring time slot in a channel when making a call. When all slots on all channels are occupied no more calls can be added to the network. Figure 9 on the next page illustrates the GSM channels and TDMA.

3.3.3 GSM cells

To increase the total number of simultaneous users in the network and to lower the output power from every cell phone, the GSM network is divided into cells [2]. This approach makes it possible to reuse the available frequencies and depending on the need the cells can be made larger or smaller. Outside the cities the cells can reach 70 km in diameter while in highly populated urban places the cells can be as small as 50 meters [2]. See figure 10.

3.3.4 GSM structure

Each cell has its own Base Station, BS, which contains a radio transceiver. One or multiple base stations are connected to a base station controller, BSC. The controller handles the radio channels, handovers between cells and forwards calls in the cell to a mobile switching centre, MSC, in the network. The switching centre in turn routes the call onwards to the target BS or to another network. The GSM network contains a set of databases:

The visitors location register, VLR, is used to keep track of visiting customers in the cell, also known as roaming.

The home location register, HLR, contain customer specific data such as last known location and billing information.

The authentication center, AUC, has the function to authenticate each SIM card that attempts to connect to the GSM core network. Without the approval from the AUC, the SIM card cannot be used in that network. This is a secure and important database with the main task to avoid SIM cloning.

The equipment identity register, EIR, contains information which cell phones, identified by their IMEI number, need to be banned from the network or monitored. This information is crucial when tracking stolen mobile phones and the information is exchanged between operators worldwide.

Quick facts

Today, GSM is used in 219 countries and available to more than 3.000.000.000 people [12]. By having harmonized the spectrum across most of the globe, GSM users can use the same equipment wherever they travel. GSM terrestrial networks now cover more than 80% of the world's population.

Global system for mobile telecommunications

GSM operates in the ultra high frequency band, UHF. In Sweden the frequencies 890 MHz – 915 MHz are used for uplink and 935 MHz – 960 MHz are used for downlink.

Figure 9

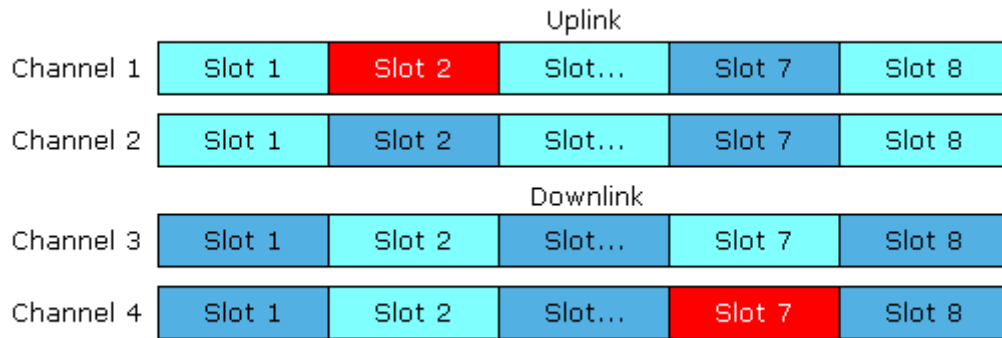


Figure 9 illustrates an example where the base station has reserved the second and the seventh slot for a specific cell phone until the end of the call regardless if anything is said or not.

Figure 10

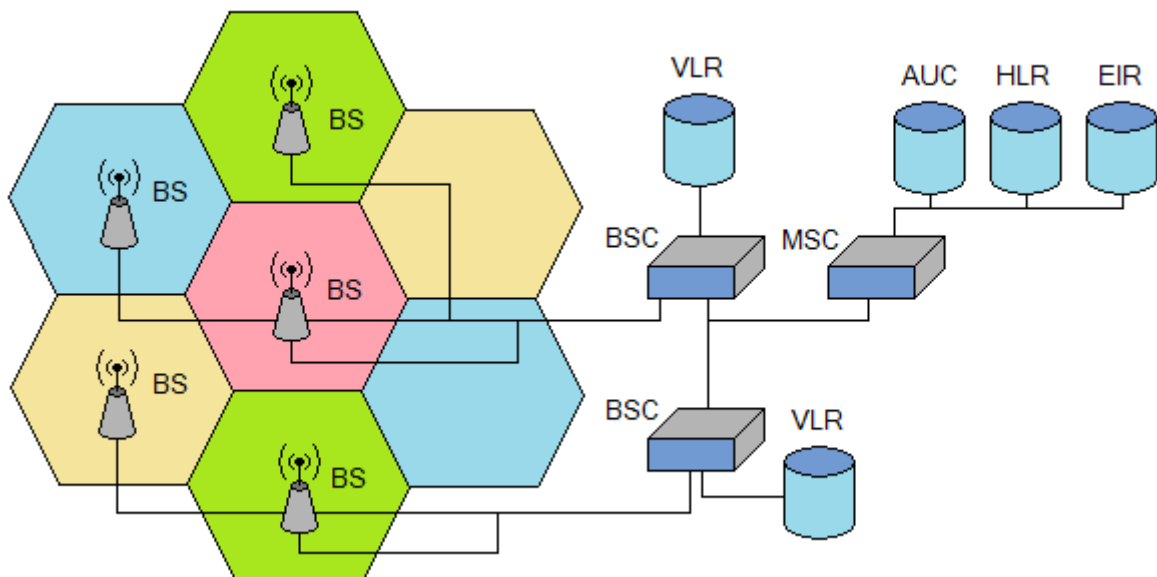


Figure 10 illustrates the structure of a GSM network [2]. Frequencies are reused as shown by the different colored cells. This method increases the number of simultaneous users and also lowers the transmission power hence increasing the battery time of mobile phones inside the cell.

3.4 GPRS

3.4.1 General packet radio service

General Packet Radio Service, GPRS, is an extension of the GSM standard which was released in 1996 [1]. GPRS allows packet based data to be sent in the network and onwards through gateways to the Internet using standard protocols.

3.4.2 The GPRS network

Data to be sent is first divided into small pieces, packets. The individual packets are then sent as soon as there is a time slot available in the network. No repeating time slots are reserved for a specific user as in the basic GSM network [13]. This allows for a more efficient use of the bandwidth. All time slots not reserved, are available to all other users as soon as they have data to transfer. Many users can still be constantly attached to the base station, much like an Internet broadband connection, ready to send or receive [14]. Network operators often employ a tariff scheme where users pay for the data actually sent, not the time period they are connected. The pay-per-byte nature of GPRS makes it ideal to use with remote devices that need to be constantly connected to other devices, or to a central server, but only exchanging small amounts of data spread over long periods of time [1].

3.4.3 GPRS structure

In order to support GPRS some new hardware is needed in the GSM network [1]. The serving GPRS support node, SGSN handles packet routing, mobility management, authentication and charging functions. The gateway GPRS support node, GGSN acts as an interface between the GPRS network and the IP network. It converts the GPRS packets coming from the SGSN into the appropriate format and sends them out on the Internet. In the other direction, IP addresses of incoming data packets are converted to the GPRS address of the destination user.

Figure 11 shows additional components needed to implement GPRS in a GSM network.

3.4.4 Dynamical IP address allocation

Assignment of an IP address to a unit is done dynamically by the network operator, i.e. a unit's IP address will change over time. This means that there is no way for a server that wants to contact a unit to know its IP address for sure. Lately specialized operators utilize a Domain Name System, DNS, to give a unit a static public IP address [2]. The operator then routes incoming requests to the public IP address through the DNS server to the unit's current dynamic IP address.

3.4.5 Alternative communication technologies

One of the requirements of the FMS platform is "real-time" positioning. This condition disqualifies any solution with logging of data for later transfer via e.g. WLAN at a depot. The only alternative today and for years to come, that support packet based transmission country wide, is the third generation, 3G cellular technology. The data rates of 3G are not needed by the FMS platform's current specification and the price of a 3G module is approximately three times that of a GSM module [c]. An advantage of 3G is that network operators tend to have lower prices per megabyte of transferred data.

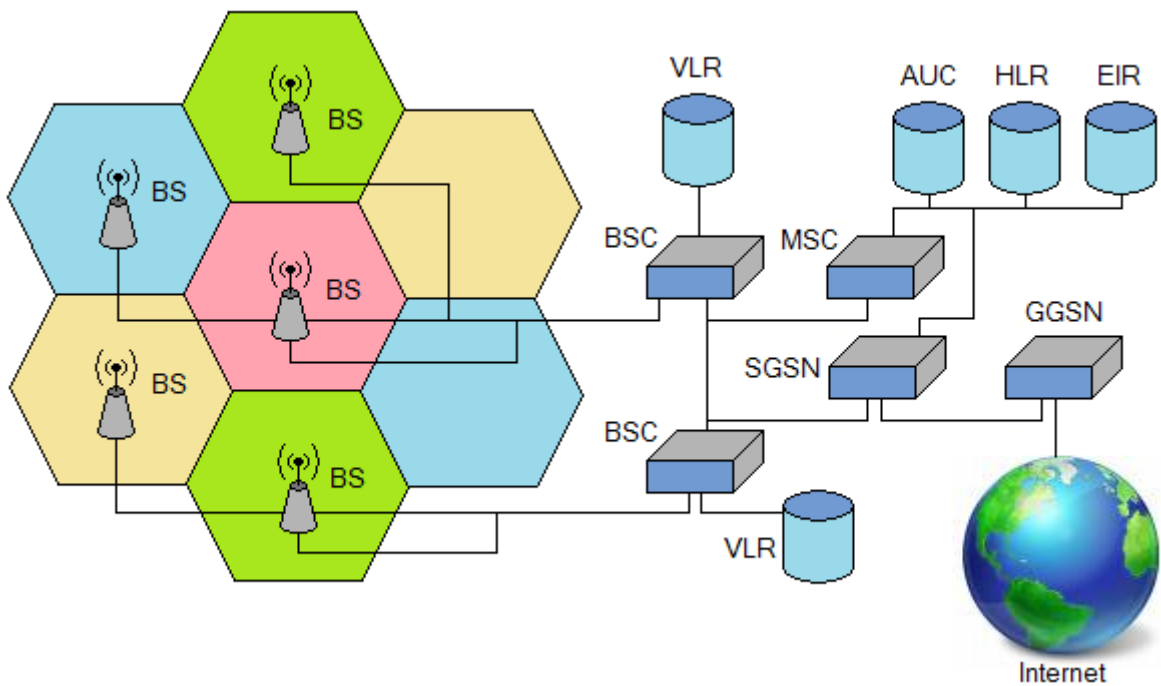
Quick facts

The first phone using the GPRS technology was the Ericsson R520, released in 2001. At first GPRS was used to give Internet access to laptops but today most of the cell phones have large displays and good browsers making them perfect for exploring the world wide web.

General packet radio service

Each slot in the uplink and downlink can transmit 13.4 kbps of user data and since operators limit the amount of GPRS slots to 4, the maximal speed in each direction is limited to 53.6 kbps [14]. This is a relatively low data rate compared to the 3G network where the data rate can reach speeds of 14.4 Mbps.

Figure 11



BS	Base Station
BSC	Base Station Controller
MSC	Mobile Switching Centre
SGSN	Serving GPRS Support Node
GGSN	Gateway GPRS Support Node
VLR	Visitor Location Register
HLR	Home Location Register
AUC	Authentication Centre
EIR	Equipment Identity Register

Figure 11 shows the additional hardware needed in order to implement GPRS in the GSM network [1].

3.5 CAN

3.5.1 Controller area network

The Controller Area Network, CAN, is a communication bus standard designed for the automotive industry. It has focus on robustness and communication with a high message rate but only a few bytes of data per message [15]. This makes it ideal for embedded systems with distributed intelligence, may it be in a truck or an automated production line. The CAN bus's wide use in the automotive industry today was also influenced by the availability of very low cost protocol chips [16].

3.5.2 Physical layer

The CAN standard supports different physical layers for different bus speeds and different levels of fault tolerance, with bitrates up to 1 Mbps. As for the wiring, it is most common to use two balanced wires, called CAN High and CAN Low [15]. The signal level is defined as the voltage difference between the two wires. This setup is more tolerant to electromagnetic disturbances, EMC, than if the signal level would be measured with respect to ground [7].

Non-Return-to-Zero, NRZ, signaling is used where high and low voltages represents binary code with no other neutral rest condition present. If two high bits are transmitted after each other there is no change in voltage between bits.

The standard does not use a central clock; instead each node synchronizes on signal level flanks. To ensure proper synchronization, that is, enough flanks to synchronize on, bit stuffing is used to avoid long trains of equal bits in the NRZ coding scheme. It is important to properly terminate the bus by a resistor at each end to avoid reflections [7].

3.5.3 Protocol layer

The basic data unit is called a message. A message roughly consists of an identifier plus data. All messages are broadcast on the bus and each node reads the identifier of all messages to determine if the data is relevant to it or not. All nodes are obliged to perform error checks and send 'Acknowledge'/'Not acknowledge' on all incoming data, not just on messages that are relevant to the specific node. The extensive error handling is used to attain high robustness and to silent erroneous nodes or make them go off the bus permanently [15].

3.5.4 CAN messages

Four kinds of messages can be sent over the CAN bus.

- Data frames
- Remote frames
- Error frames
- Overload frame

Data is carried by data frames, consisting of identifier and data. The remote frame is used to request data from another node. It consists of an identifier but no data. The node 'owning' the identifier of a remote frame will send a data frame which the requesting node can pick up. If a node detects an error in a message it will send an error frame to notify all the other nodes. The sender of the erroneous message will then try again. The overload frame was needed by the very first CAN-controllers available to signal they need additional time to process the last message [16]. It is rarely used by any CAN devices today due to their better performance.

3.5.5 CAN standards

There are two versions of the CAN standard in use; CAN2.0A and CAN2.0B [16]. The main difference is in the length of the message identifier. 2.0A supports 11 bit identifiers, giving 2000 unique message types, and 2.0B supports 29 bits giving 512 million message types. 2.0B CAN controllers can handle 2.0A identifiers, but not the other way around. CAN 2.0B allows for more complex systems but the price is more data overhead. The different CAN messages can be seen in figure 12.

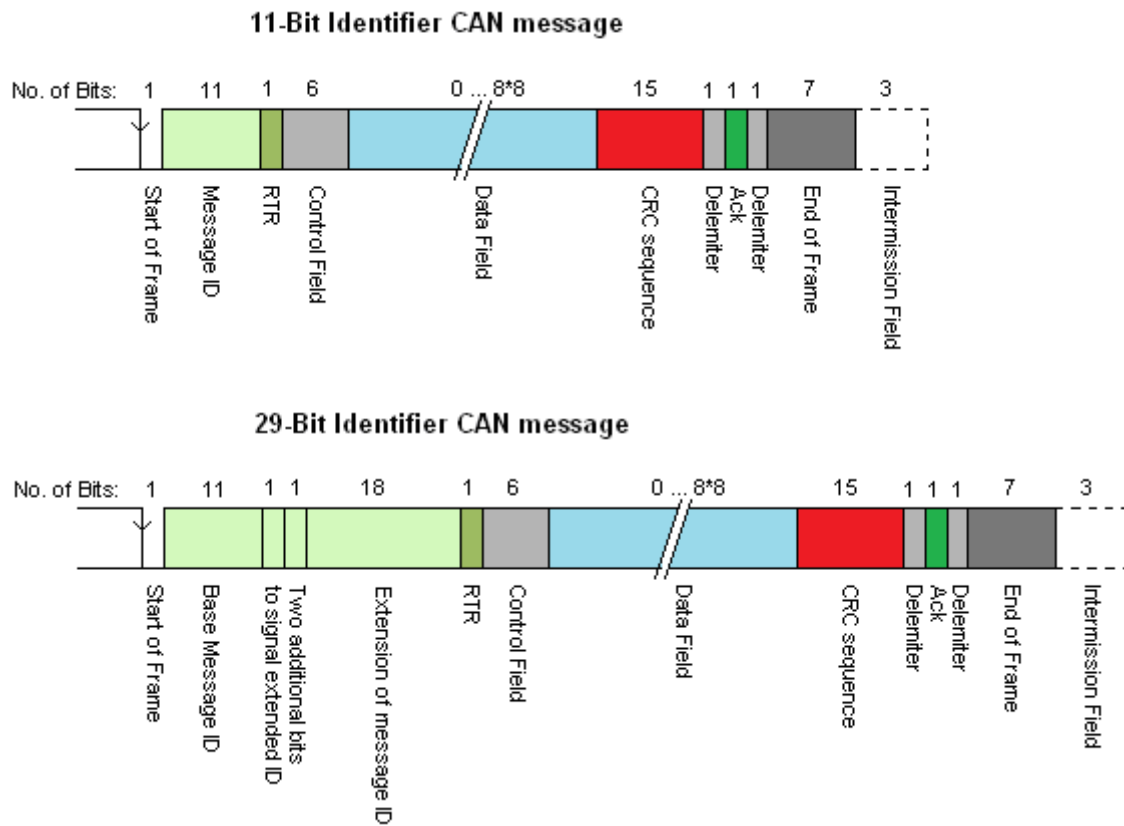
Quick facts

Since the introduction of the high speed CAN bus in the year 1996, new units have been introduced almost every year. Also new sub buses have been introduced [7].

Controller area network

Development of the CAN-bus started originally in 1983 at Robert Bosch GmbH and 4 years later the first CAN controller chips, manufactured by Intel and Philips were available on the market. Up to spring 1997 there have been more than 50 million CAN nodes installed.

Figure 12



Start of frame	Indicates the beginning of a message
Message ID	Unique identifier for each type of message
Remote transmission request	Used to distinguish between remote and data frames
Control field	Contains bits to indicate properties of the message
Data field	Zero to eight bytes containing the actual data
CRC sequence	Contains a checksum of the message
Ack	Indicates that the transmission was successful
End of frame	Indicates end of message
Intermission field	Separates one message from the next

Figure 12 shows the CAN 2.0A and CAN 2.0B messages [15].
Note the 18 bit extended message identifier used in the CAN2.0B standard.

3.5.6 CAN error handling

As mentioned earlier, error handling of the CAN standard is extensive [15]. The standard uses an elaborate scheme which gives points to erroneous sends and receives of a node, and subtracts points when successful. If a node gets more points for erroneous receives than a given value, it will go error passive and not signal any errors it detects. This is to avoid an erroneous node to destroy the bus traffic completely. If the node keeps detecting errors after this it will go off line completely. The same thing will happen to a node which sends too much erroneous data.

3.5.7 CAN signaling and arbitration

The low bit is dominant on the CAN bus and the high is recessive. This means that if two nodes start to transmit at the very same time with one node transmitting high, and one low, the bus value will be low. This is used for bus arbitration. One of the most appealing properties of the CAN standard is the non-destructive bus arbitration [16]. When two nodes want to transmit over the bus at the same time, arbitration determines who gets to send. Each node transmitting on the bus is also listening to it at the same time. Suppose the bus is available. Node A and node B start to transmit their identifiers at the same moment. If node A sends a low bit and node B sends a high, the bus will go low since low is dominant. Node B will sense that the bus value differs from the value it transmits. B will immediately stop transmitting and become a listener. Node A will continue to transmit as if nothing had happened. In this way, no time is wasted. CAN bus arbitration is shown in figure 13.

This arbitration scheme differs from for example the Ethernet network. When a collision is detected in an Ethernet network, all nodes will go silent and then try to retransmit the same frame after an arbitrary period of time [2]. At extremely high load the Ethernet bus will collapse since no data is transmitted due to reoccurring collisions between sending nodes. In the CAN network, only nodes with high priority will be able to communicate at high network load but the network will not collapse.

3.5.8 FMS CAN standard

To promote the use of vehicle performance parameters in fleet management, the major commercial vehicle manufacturers have agreed on a standard set of CAN data that should be made available to third party developers. Parameters made available by the standard include odometer and fuel consumption [7]. The 'FMS Interface' is the hardware part of the FMS standard and is specific to each vehicle brand. It is a gateway between the CAN bus of the vehicle and the third party device [a]. The gateway has two tasks. The first is to transform whatever CAN protocol that the manufacturer might use internally, so that the output complies with the FMS standard. Its second task is to work as a firewall and prevent an external device from sending data on the internal CAN bus network. This could otherwise interfere with the systems of the vehicle and cause fatal accidents. Third party devices may only listen to CAN data, never transmit data. Connecting an external device to the internal CAN bus without a gateway voids the vehicle warranty [18].

3.5.9 SESAMM

Scania Electrical System Anno 2000 is the denomination of the current electrical system used inside the vehicles [7]. The network consists of three major CAN buses, the red, yellow and green bus. The red CAN bus consists of nodes crucial for safety and vehicle operation such as the engine control unit, gear management and the braking system. The yellow CAN bus consists of units which are not critical for vehicle operation but are still of high importance such as the visibility system, the alarm, and the instrument cluster to mention a few of them. Units such as the audio system, the automatic climate control and the navigation system which have no impact on vehicle and traffic safety are connected to the green CAN bus. The three CAN buses are connected to a central ECU called the Coordinator, COO. This unit, the heart of the vehicle, acts as a gateway between the buses and monitors all sent data [j]. Figure 14 illustrates the CAN network in a Scania vehicle.

Quick facts

Due to the increasing amount of data sent between different ECUs many vehicle manufacturers have been searching for a suitable replacement of the CAN bus. FlexRay and Ethernet are two possible and competing technologies [15].

4 Existing FMS in Brazil

4.1 Scania

Some years before the new law was suggested by the Brazilian government, local developers at Scania in Brazil developed a system to monitor and shut down vehicles if stolen [d]. Unfortunately this system is not totally integrated into the electrical system but an optional add-on after the final assembly of the vehicle. The system called IRIS was developed to meet the growing demand of vehicle surveillance systems.

4.1.1 IRIS

Iris uses satellite technology to communicate with vehicles. 48 satellites in orbit and 70 receiver stations around the country assure a good uptime for the communication [10]. In every moment the vehicle has contact with at least 3 satellites which makes IRIS robust, reliable and always ready for use. See figure 15.

A drawback for the system was the high cost of transmitting data over the satellite link.

4.1.2 IRIS Híbrido

To lower the cost but still offer a robust solution IRIS was extended with the ability to use the much cheaper GPRS technology. The updated system was called IRIS Híbrido. IRIS Híbrido uses the relatively cheap GPRS connection as long as possible and falls back on satellite communication when connection to GSM is lost [10].

4.2 Mercedes

No fleet management system at the time of this thesis.

4.3 MAN

No fleet management system at the time of this thesis.

4.4 Renault

No fleet management system at the time of this thesis.

4.5 Volvo

Volvo developed a system called Volvo Link and it is already in use in Brazil. It works similar to Iris Híbrido but has some additional features.

4.5.1 Volvo Link

Volvo Link uses satellite and GSM/GPRS technology to communicate with vehicles [11]. Unlike the IRIS system it is integrated with the rest of the vehicle electronics which makes it hard to disconnect by accident or in other ways manipulate the system. See figure 16.

Volvo Link includes a Driver Panic Button which gives the driver a way to signal that something is wrong. If the driver activates the panic button, Volvo Action Service is contacted and a blocking command is sent to the vehicle. The engine block command limits the speed of the vehicle to 20 km/h for a certain time and then turns the engine off. The engine can still be turned on twice and the vehicle driven for a short distance in case the shutdown occurred in an unsuitable location. After the third shutdown the vehicle cannot be started until a valid unblocking command is received.

Even if the vehicle is in an area where connection with Volvo Action Service is missing the blocking will automatically be executed a short time after the panic button is activated.

Other services available through Volvo Link are:

- Vehicle supervision
- Fuel consumption supervision
- Remote diagnosis of the vehicle
- Remote immobilization
- VAS (Volvo Action Service)

Quick facts

In the year 2007, the production site in Latin America delivered 14.3% of all trucks and 32.4% of all buses produced by Scania [3].

Vehicle Supervision

Already in an early stage of the thesis it was clear that the Swedish heavy vehicle manufacturers were far ahead their foreign competitors. Since Volvo had already deployed their Volvo Link technology the pressure was high on Scania to complete the Fleet Management solution and keep the high market share in South America.

Figure 15



Figure 15 shows a Scania R 440 Topline. Time was running short for Scania to replace the add-on system IRIS and extend the fleet management solution with the modifications needed to fulfill the Brazilian anti-theft-regulation.

Figure 16



Figure 16 illustrating a Volvo tractor model with Volvo Link technology. According to available information about the Volvo Link system [11], the truck manufacturer on the west coast was much closer to satisfying the Brazilian anti-theft-regulation.

5 Fleet management services

5.1 Scania fleet management services

As mentioned in the introduction, the FMS is a way for companies to improve their overall performance and thus become more profitable. As the fuel cost is the greatest expense for a hauler company [k], all methods to lower this cost are extremely valued. Special hardware and subscription is needed to get all the benefits of Fleet Management Services.

The following services can be subscribed through the Scania Fleet Management and viewed on the fleet management portal [17]. See figure17.

5.1.1 Vehicle performance analysis

Vehicle data is presented in a simple format showing all important information about the selected vehicles. Data includes position, speed, odometer, fuel consumption, brake behavior, over revs and overall runtime (drive, idle, Power Take Out).

5.1.2 Driver performance analysis

Driver data is presented in a simple format showing all important information about the selected drivers. Data includes fuel economy, runtime, over speeding, over revs, acceleration and brake behavior and brake applications. From the collected data, driver performance reports can be made. These reports can be used to educate specific drivers to a more ecological driving technique. Another approach is to introduce a bonus system based on fuel economy.

5.1.3 Event reporting

Important events affecting the vehicle are logged and reported on the web portal with data, time and location, allowing immediate action to be taken if necessary or for post-event analysis. For example analysis of harsh braking or over revving.

5.1.4 Reported warnings

Certain parameters can be monitored and a report will be issued when the following events occur: Exceeded distance or time period without service, low tire pressure, serious engine problem, high engine coolant temperature, clutch overload, low engine oil pressure, low urea level, low engine coolant level or seatbelt reminder.

5.1.5 Geofence alarm

It is possible to set a digital boundary to keep the vehicle in or out of a specified geographical area. An alert is issued if a vehicle enters or leaves the specified area allowing immediate action to be taken. The message is displayed on the web portal and can also be sent to a designated email address if preferred by the customer.

5.1.6 Maintenance planning

Customers can create their own maintenance calendar and reminders based on mileage or service dates, to ensure the vehicle is maintained on time. The distance or time to next planned service for each vehicle can be monitored on the web portal.

5.1.7 Positioning and tracking

The FMS enables customers to monitor all vehicle locations by GPS and thus keep track of the entire fleet from the office. This makes planning a whole lot easier, reduces the number of needed telephone checkups, and reduces the impact on the environment while increasing security and reliability of delivering on time. The vehicle position is automatically sent at regular time intervals, as well as whenever the ignition is switched on or off, or when drivers change. It is also possible to request the position from the vehicle at any time.

5.1.8 Wireless download of digital tachograph data

Communicator 200 supports wireless download of both driver card and vehicle tachograph data.

5.1.9 Environmental reporting

Companies with high environmental awareness can receive environmental emission reports which are generated based on actual operating conditions including engine characteristics and fuel consumption.

Quick facts

Since May 2006 all new commercial vehicles must be equipped with a digital tachograph. This is a device which records vehicle speed over time and is used to control driving and resting times of drivers [17].

Fleet Management Portal

The fleet management portal offers a set of tools to analyze vehicle and driver performance. It is also used to keep track of all vehicles in the fleet and set up geographical borders to control fleet movement. Depending on the customer requirements, subscription to the desired services creates a custom FMP satisfying the present needs which can easily be extended in the future by subscription to new services.

Figure 17

Förare	Start	Slut	Streckor (km)	Totalt bränsleförbrukning (litrar)	Genomsnittlig bränsleförbrukning (l/100km)	Medeltakthet (km/h)	Ranking
A. A. A.	2010-12-01	2010-12-31	0	0	0,0	0,0	1
B. B. B.	2010-12-01	2010-12-31	2400	2400	100,0	0,0	2
C. C. C.	2010-12-01	2010-12-31	1000	1000	100,0	0,0	3
D. D. D.	2010-12-01	2010-12-31	124	43	49,6	24,1	4
E. E. E.	2010-12-01	2010-12-31	91	35	42,4	23,3	5
F. F. F.	2010-12-01	2010-12-31	113	49	43,2	23,3	6
G. G. G.	2010-12-01	2010-12-31	149	73	49,2	23,3	7
H. H. H.	2010-12-01	2010-12-31	14	6	70,3	30,2	8
I. I. I.	2010-12-01	2010-12-31	14	6	70,3	30,2	9
J. J. J.	2010-12-01	2010-12-31	11262	2647	23,5	27,9	10
K. K. K.	2010-12-01	2010-12-31	23	9	39,1	17,9	11
L. L. L.	2010-12-01	2010-12-31	46	18	40,2	18,0	12
M. M. M.	2010-12-01	2010-12-31	141	51	36,2	18,0	13
N. N. N.	2010-12-01	2010-12-31	19	6	42,2	18,0	14
O. O. O.	2010-12-01	2010-12-31	19	20	105,3	18,0	15
P. P. P.	2010-12-01	2010-12-31	33	13	39,7	18,0	16
Q. Q. Q.	2010-12-01	2010-12-31	73	27	37,0	18,0	17
Utvärderingsmedel	2010-01-01	2011-01-01	1844	2049	111,5	5,4	
Fordonsparhållningsmedel	2010-01-01	2011-01-01	888	2311	260,3	5,4	

Figure 17 shows the Fleet Management Portal. FMP is a user interface on the Internet where a manager or administrator can easily keep track of all vehicles and their status. From top down: login page, alert monitoring, vehicle tracing and driver analysis.

6 FMS hardware

6.1 Scania telematic unit

To get access to all the benefits provided by the fleet management services, a telematic unit must be fitted in the vehicle. This is usually done when first ordering the vehicle but can also be purchased as an aftermarket add-on to older vehicles.

Since the FMS CAN standard specifies which CAN data must be made available in the vehicle, the customer can use the telematic unit in all vehicles regardless of vehicle brand [17].

The first generation of telematic units, the Interactors were developed in the late 90's to meet the demand for robust vehicle computers with the ability to connect the vehicle to the office but also provide the drivers with a digital navigation system, integrated phone and an entertainment system [a].

6.2 Interactor 300 and Interactor 500

The Scania Interactor 300 and 500 are powerful personal computers with large color screens. See figure 18. The driver can choose to navigate through the menus by using the touch screen or the included keyboard. The Interactor was developed to bridge the gap between the office and the vehicles and give companies with large fleets a way to keep track of all vehicles and minimize the paperwork [a]. Orders are sent from the office, executed by the drivers and invoices sent as soon as the jobs are completed. The delivery progress can be monitored around the clock from the office without making a single phone call to the fleet.

When receiving a new order, the drivers can choose to use the built in navigation system to automatically find the nearest way to the pickup or drop point.

6.3 The need for new hardware

As consumer laptops and navigation equipment got widely available, many companies could not motivate the cost of approximately 50.000 SEK for a new Interactor. With the introduction of cheap dongles which gave laptops internet connectivity, the need for a robust onboard computer was gone.

On the other hand, the interest for fleet management services was continuously high. Is there a way to offer all the benefits from fleet management services in a smaller, cheaper unit?

A new device had to be developed for customers who require all advantages of the FMS but does not need the extra features of the expensive PC [b]. The new device should be as simple as possible with no integrated driver interface. It should be a black box that gathers vehicle information and sends it to the web portal where it can be analyzed and presented.

6.3.1 Communicator 200

A new unit was soon under development, the new heart of the Scania FMS; the Communicator 200. Apart from the mentioned services, this thesis will investigate if the unit offers a way to remotely immobilize vehicles.

Quick Facts

First generation telematic units used the GSM short message system, SMS to transfer data between the vehicle and the office. This made data transfer both inefficient and expensive [c].

Changes to the product portfolio

First generation telematic units were powerful personal computers which not only offered fleet management services; they also offered navigation, integrated cell phone, a messaging and logging system and working hour reminder. Unfortunately the rapid evolution of consumer electronics and the large difference in cost forced Scania to change the product portfolio in order to keep market shares.

Figure 18



Figure 18 shows the touch screen connected to an Interactor 500. The large navigation buttons are perfectly suited for the vehicle environment and the home screen gives the driver a quick overview of all new events, orders and calls. Unfortunately, the high cost and new technology made the Interactor out of date [b].

7 Communicator 200

7.1 Appearance

The Communicator 200, further referred to as C200, is literally a black box with connections for power supply, CAN, digital I/O's and antennas. No visual user interface is present in the C200 but an Ethernet connection is planned for future peripherals. Figure 19 on the next page shows the first C200 unit.

7.2 Hardware

The C200 consists of several hardware modules tied together by a Power PC CPU running Linux OS [c]. A GSM module handles all wireless communication to and from the vehicle. The CAN communication module is able to read and write data from the local CAN bus, thus receiving information about vehicle ID, vehicle speed, error codes and all other vehicle parameters available on the bus [7]. The GPS module receives information about the vehicle position, speed and local time. Digital inputs/outputs are used by the vehicle alarm system and other electrical control units to trigger events and initiate data transfer to the web portal.

7.3 Software

In order to achieve a robust system with high uptime, developers introduced small and simple software modules which run independent of each other. The technique detaches modules from each other making them less vulnerable to failures in other modules [5]. The only connection between modules is made through an internal message based protocol making development, testing, upgrading and maintenance much easier. This approach makes it possible to start with a basic set of functions and later add functionality depending on customer subscription. All modules are event driven, reacting to events initiated by a relevant change in the adjacent modules. This means that no action will be taken unless an external stimulus is received [6]. The only exception to this will be if a module's internal timer triggers an event.

7.3.1 Modules and layers

The modules are divided in three different layers, the hardware layer, the server layer and the application layer depending on the functionality of the module [5].

The hardware layer is the software closest to the hardware, translating electrical signals into logical data.

The server layer consists of modules which collect different data, prepares it and distributes the data to subscribing application modules. Each server module keeps track of subscribing modules.

The application layer consists of modules which interpret and manipulate the data. Each application module starts by subscribing data needed to perform its task. When the subscription is confirmed by the server module the application module will be notified each time new data is available from the specific server. A single application module can subscribe data from several server modules. This will be further described when discussing the Remote Shutdown application module. When a new notification is received the data is processed and sent back to the server or to other application modules for further processing. Figure 20 illustrates the different layers.

7.4 Testing

Each module developer writes extensive test cases in order to test all functionality and correct behavior of the module prior to the release [f]. The test program verifies correct data is sent from the tested module and also that incorrect data is ignored and reported. Each day, all released modules are put together and testing is performed on the entire unit [c]. This assures no mistakes are made in the interface between modules and a robust system is sustained.

Quick Facts

Scania was founded in 1891. Since then Scania has built and delivered more than 1.400.000 vehicles [18].

Simple and robust

The modular architecture makes development of new modules less demanding. By using a module template, a new application module can be set up in minutes. Special test software can be used to test the entire module before integrating it in the complete system which makes troubleshooting easy and effective.

Figure 19



Figure 19 shows the first generation of the new telematic unit called the Communicator. Scania put a whole lot of effort in making this unit small, robust and cheap. Fleet management services are now available to a fraction of the old price.

Figure 20

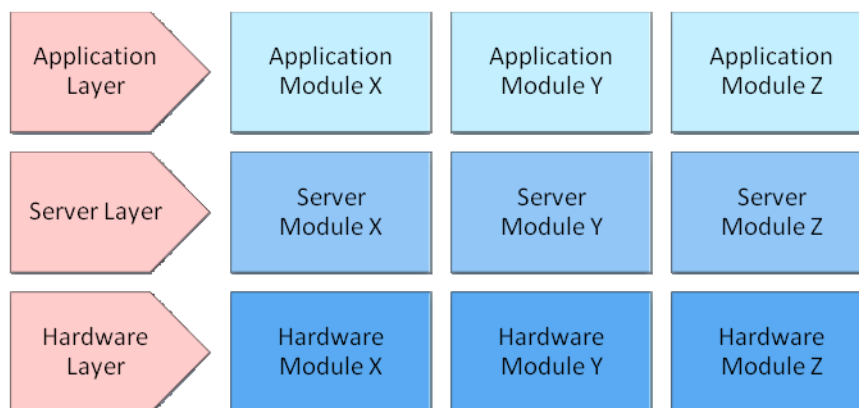


Figure 20 illustrates the software architecture of the Communicator 200. Since each module is independent, modules can be updated one at the time to increase performance or expand the module with new functionality as long as the interface is kept intact [5], [6].

7.5 First time configuration

When the C200 is turned on for the very first time it needs to be configured to be able to send and receive data. The unit will start by sending a configuration request message to a predefined telephone number. The message, containing vehicle identification number, IMSI number, Communicator MAC address and serial number is used to authenticate the vehicle and initiate a transfer of settings required for communicating with the web portal [c].

After a successful authentication, FMP answers with a configuration message containing all information needed to establish a secure communication link between the unit and the portal.

The configuration message contains the URL address to Scania FMP, the time interval for periodic notification messages from the vehicle and most important, the crypto keys used to encrypt/decrypt information sent between the C200 and FMP [c].

Finally the customer specific configuration is sent to the unit before it is ready for use. This is done with a report settings message. The message configures which events will be reported to the FMP. It is also used to activate or deactivate functions such as the remote blocking function. Another parameter that can be configured is the time interval for status messages, which can be set from a couple of minutes to several hours depending on the customer's needs [e].

The C200 is now ready to send and receive data. Each time the ignition is turned on the C200 will notify FMP of its presence and send periodic messages about the vehicle status. The most important message is the "Current Status" message.

7.6 Current status messages

A current status message, CS message, contains all relevant information about the vehicle condition and driver behavior. Each message contains current position, odometer, speed and other relevant vehicle information. This information can then be used to compare vehicles or drivers on the fleet management portal.

A current status is generated and sent to the portal in predefined intervals or triggered by an external event. At the time of this thesis, 19 different triggers were specified. Table 1 on the next page shows an entire CS message.

To keep track of the remote blocking status, a new parameter was added to the CS message. In this way each CS message would contain information about the progress of the remote shutdown. More information about this can be found in the "New Software" chapter on page 35.

Quick facts

In the end of 2008, 2.922 people were working with research and development at Scania and 16.264 were involved with production. In total, Scania employed 34.777 people [18].

Current status messages

The most important message from the C200 is the current status message, the CS message. It contains all important information about the vehicle and the driver. The CS can be triggered by a timer or by different events depending on the configuration.

Table 1

Current Status Message	
Data	Value
Driver ID	16 characters
Trigger Type	1 – 19
Interactor Connected	Disconnected/Connected
Ignition	On/Off
GPS Lat, N/S	N/S
GPS Lat, DD.ddddd	Degrees
GPS Long, E/W	E/W
GPS Long, DDD.ddddd	Degrees
GPS Speed	Knots
GPS Heading	Degrees
Time position, YY	Year
Time position, MM	Month
Time position, DD	Day
Time position, HH	Hour
Time position, MM	Minute
Time snapshot	Minutes
Odometer	Meter
Total time over speeding	Seconds
Total time over revving	Seconds
Total number of harsh brakes	Counter
Total number of brake pedal applications	Counter
Total number of harsh acceleration	Counter
Max Speed	km/h
Fuel Level	0-100%, resolution 0,4%
Service Distance	Km
Warning Distance Without Service Exceeded	Yes/No
Warning Low Tire Pressure	Yes/No
Warning Serious Engine Problem	Yes/No
Warning High Engine Coolant Temperature	Yes/No
Warning Low Engine Oil Pressure	Yes/No
Warning Low Urea Level Lamp	Yes/No
Warning Low Engine Coolant Water Level	Yes/No
Warning Seatbelt Reminder	Yes/No
Error, No GPS Antenna	Yes/No
Error, No GPS Signal	Yes/No
Error, No CAN Connection	Yes/No
Error, Tachograph Tampering	Yes/No
Vehicle Remote Blocking Status	Function Status

Table 1 shows what kind of information is sent to the web portal for analysis. With a CS message every 15 minutes, it is easy to follow the vehicle and driver progress. The Vehicle Remote Blocking Status was added to the CS message during the thesis project.

8 Remote shutdown

8.1 Performing a safe shutdown

A couple of weeks into this thesis project a horrible accident occurred in Brazil probably as a result of an unsuccessful remote blocking [d]. You can read the whole story in the end of this thesis. The accident raised a lot of questions about remote shutdown of vehicles. How can this type of accidents be avoided in the future?

8.2 Risk factors

In order to perform a safe shutdown, a couple of factors must be considered. See also figure 21.

- Vehicle speed
- Vehicle position
- The human factor
- Stopping technique
- Latency
- Other factors

8.2.1 Vehicle speed

The Brazilian law states the vehicle can only be blocked when not in motion. But there are no restrictions about limiting the speed or removing the possibility to accelerate the vehicle if in motion. It is up to every manufacturer to find the best technique to be used.

8.2.2 Vehicle position

Vehicle position must be taken into consideration when performing a remote shutdown. Under no circumstances is the vehicle allowed to become a security risk for other traffic. Shutdown on places like highways and railroad crossings should never be possible.

8.2.3 The human factor

Since it is impossible to anticipate how the driver will react when the vehicle enters the blocking phase, it is wise to conceal the phase all the way to the shutdown point. This procedure decreases the impact of the human factor from the remote shutdown functionality.

8.2.4 Stopping technique

There are many ways of stopping a vehicle but choosing the safest way is easier said than done. If the vehicle is driven extremely reckless, perhaps with the police pursuing the vehicle, it is desired to stop the vehicle as soon as possible to minimize the damage to other vehicles and property. In this case, instant remote shutdown would be a perfect way to stop the vehicle.

In other situations, the remote shutdown can be activated without any notification to the driver until the vehicle comes to a natural stop in traffic. This allows for silent tracking of the vehicle until the blocking is executed.

Maybe the safest way to immobilize the vehicle is to wait for the driver to apply the parking brake and turn the ignition off.

Perhaps one stopping technique is not enough to cover all possible traffic situations when remote shutdown is desirable [b].

8.2.5 Latency

Although the GPRS system is reliable and fast, there is a certain amount of latency which makes real-time surveillance and action difficult. See figure 22 and chapter "Results" on page 41 for further details about latency. Especially when monitoring speed, all latency is undesirable. The only way around this problem is by creating intelligent software acting from inside the vehicle which, once activated, supervises speed and blocks the vehicle when speed reaches the desired value.

8.2.6 Other factors

Other factors which may have impact on the way remote shutdown is executed is the type of load carried by the vehicle. Perhaps different stopping techniques should be used depending if the vehicle is carrying food or gasoline and if the vehicle is located in a town centre or in an unpopulated rural area.

Quick facts

Scania's core values influence the day-to-day work in the entire corporate. Customer first, respect for the individual and quality are the point of departure for all business development [4].

Remote shutdown

There is no doubt that remote shutdown can have fatal consequences if not used with caution. On the other hand, clever implementation of the blocking procedure and a dedicated, educated team handling the blocking can definitively turn the remote shutdown into an effective weapon against cargo and vehicle theft.

Figure 21

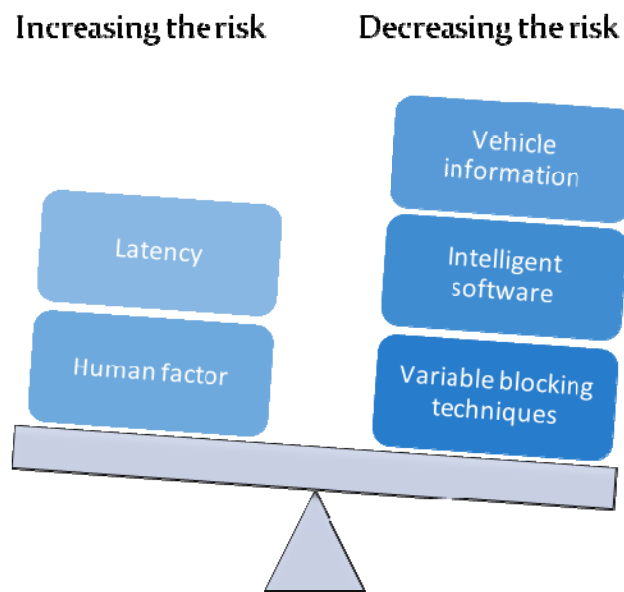


Figure 21 shows factors that increase or decrease the risks during the remote shutdown. The latency can be decreased by optimizing the communication within the entire system thus increasing the real-time performance. The human factor is present but can be minimized through variable blocking techniques and intelligent software. Developers of the final blocking application must consider all possible traffic situations in order to give the operators a feasible way to execute a safe remote shutdown.

Figure 22

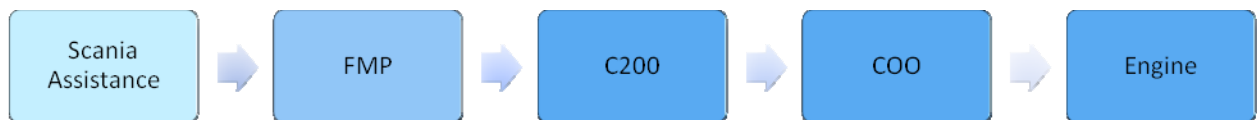


Figure 22 shows an overview of systems involved in the remote shutdown function. Each message or command sent from the office takes on an average 6 seconds to reach the vehicle. The unknown latency makes it difficult to control the remote shutdown in real-time with desired accuracy.

9 Security

9.1 Unauthorized access

An important part of this thesis was to analyze the security of the system. Under no circumstances should it be possible to gain unauthorized access to the remote shutdown functionality. Sufficient measures must be taken and security guaranteed all the way from the office to the vehicle.

Figure 23 on the next page shows the path between the office and the engine. Let us analyze the complete chain, taking into consideration also the customer reporting the theft.

9.1.1 Customer authentication

In order to ensure that the right person is requesting the remote shutdown, some type of customer authentication is required. This can be achieved by using a unique code for each vehicle which is provided together with the purchase of the vehicle. Each time the vehicle changes owner, the code should be changed as well in order to keep the integrity of the code (see figure 23, first lock).

9.1.2 User identification

As mentioned earlier, the remote shutdown will only be executed by a small, dedicated group of people within Scania Assistance. To protect from unauthorized access to the remote shutdown software, some type of user identification can be used. Each authorized member of the group logs on to the software using a unique id and password before executing remote shutdown commands. Another benefit from this approach is the possibility to log and track user actions (see figure 23, second lock).

9.1.3 FMP

In order to send commands to the vehicle, a connection to Scania FMP must be established. This can only be done with computers inside the Scania network making it harder to gain unauthorized access [h].

Once the connection is established, the FMP will handle all communication with the vehicle and also handle the encryption/decryption of each message using the crypto-keys exchanged at first time configuration of the C200 unit (see figure 23, third lock).

9.1.4 Wireless communication

A dedicated line between Scania and the telecommunication operator as well as internal encryption of messages throughout the wireless net ensures sufficient security [h].

9.1.5 C200

Each message received by the C200 is decrypted and compared to the current protocol. Messages with correct structure are processed by different applications while unknown messages are deleted and reported [h].

In order for the blocking to be processed, the remote shutdown application must be installed and the function must be activated.

9.1.6 ECU heartbeat

One way to prevent blocking of the vehicle is to disconnect the telematic unit as soon as the vehicle is stolen. To solve this security issue, a unique heartbeat (a periodic message notifying unit is present) must be added to ensure the unit is connected and running (see figure 23, fourth lock).

9.1.7 CAN eavesdropping

To protect the system from CAN message cloning, messages between C200 and COO must be encrypted. Messages for blocking and unblocking must be different between vehicles in order to prevent unblocking of the engine by using a different C200 unit (see figure 23, fourth lock).

9.2 Physical robustness

Physical parts of the system such as the GSM and GPS antennas must be protected and concealed if possible. If destroyed or disconnected, no messages can be received and no vehicle position reported to FMP. See figure 24.

Quick facts

In 2010, Scania completed its changeover to Euro 5 technology and released the world's most powerful truck - the 730 hp, Scania R 730 [18].

Security

A chain is only as strong as its weakest link. There is no point in spending massive time and effort on different authentication strategies and protecting the internal CAN system if a simple action such as destroying the external antenna voids the remote shutdown function. One must not underestimate the creativity of burglars and vehicle thieves.

Figure 23

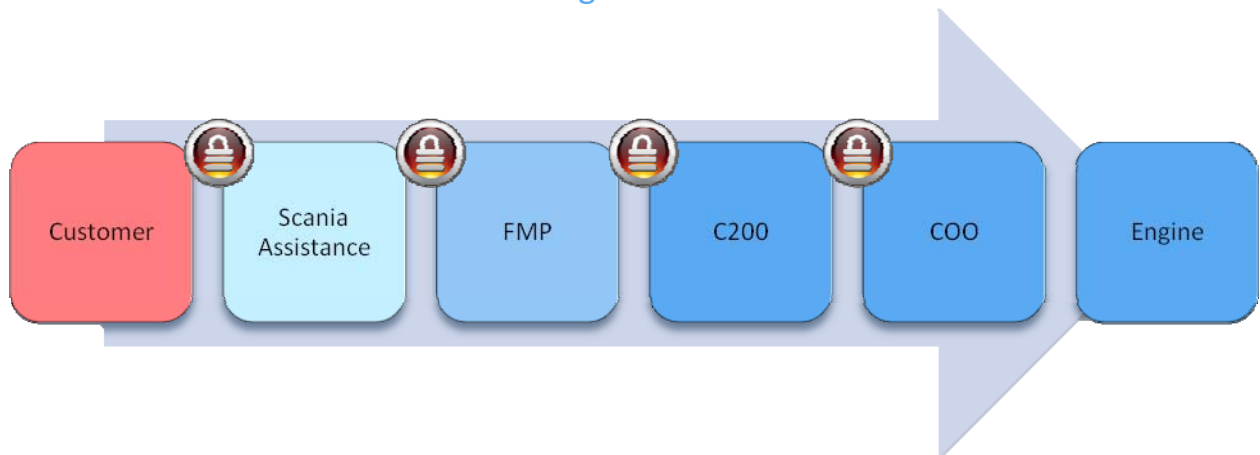


Figure 23 illustrates the complete path for the remote shutdown request. The lock symbols represent different types of security measures.

Figure 24



Figure 24 shows four different types of antennas on the roof of this Scania R730. As the reader can imagine, the antenna is an easy target for someone with criminal intentions.

10 New software

10.1 Creating a prototype

This chapter will describe the development of new software and modifications to existing applications when creating the remote shutdown prototype.

In order to send remote shutdown requests to the vehicle, a new office application was created. The new application was linked to the Scania FMP making it possible to send data to the vehicle and access the database where all vehicle information is stored.

10.1.1 Application design

Before any development could take place, some thought needed to be given to application design.

For security reasons user identification is required to access the remote shutdown application. This is done by checking user id and password.

A large number of vehicle parameters are available in the database and can be of great assistance when executing a remote shutdown. See table 1 for more information. Parameters such as speed, location, ignition and blocking status should be visible in the application and updated periodically to keep track of the vehicle.

In order to test the performance of the system, a variable timer is implemented which provides the possibility to increase the rate of incoming updates. By default, the vehicle sends new information every 15 minutes [e]. This is far from real-time surveillance. It will be interesting to see how low the timeslots can be decreased. Can the system handle periodical updates if the time is lowered to 10 seconds? Or perhaps 2 seconds?

10.2 Remote shutdown GUI version 1.0

The first version of the office software was pretty simple. When the application is started, the user is prompted to input identification and password. The user must also provide the phone number of the vehicle to be immobilized.

If username and password are correct, the user is forwarded to the graphical interface where the remote immobilization can be carried out. Figure 25 illustrates the login and command GUI, Graphical User Interface, in the first version of the application.

As shown in figure 25, three different commands are offered; Status, Limit Speed and Block.

The status command will trigger the vehicle to send periodic CS messages with time intervals selected in the drop down box.

With the speed limit command, it is possible to limit the speed of the vehicle to predefined values of 70, 50 and 30 km/h. This command also triggers periodic CS messages from the vehicle. Default value 15 seconds.

The block command executes remote blocking of the vehicle and triggers periodic CS messages. Default value 15 seconds.

10.3 Remote shutdown GUI version 2.0

Once the first version of the GUI was complete, it became clear the information displayed was hard to grasp. We are used to receive certain information in a graphical way rather than in numbers.

The second version of the GUI uses graphical gauges to display information about speed and ignition. Also new information showing the amount of fuel and vehicle odometer was added to the application as shown in figure 26.

A new progress bar was added to the application showing when new information from the vehicle will be available.

Another new feature in this version was the Map button. When pressed, it launches the standard Internet browser and displays the location of the vehicle using Google Maps.

The Log was modified and shows information about sent and received messages.

Also the login page was modified. Instead of entering the vehicle phone number manually, the available prototypes can be selected in a drop down list.

Quick facts

CEPPSS stands for Continuous Evolution of Properties Planned in Small Steps and is a strategy used by Scania to continuously improve the product without huge changes such as year models [4].

Remote shutdown office application

It was decided at an early stage that the remote blocking function would not be offered to customers through the fleet management portal. It would be a separate application operated by a certain group of people within Scania Assistance.

Figure 25

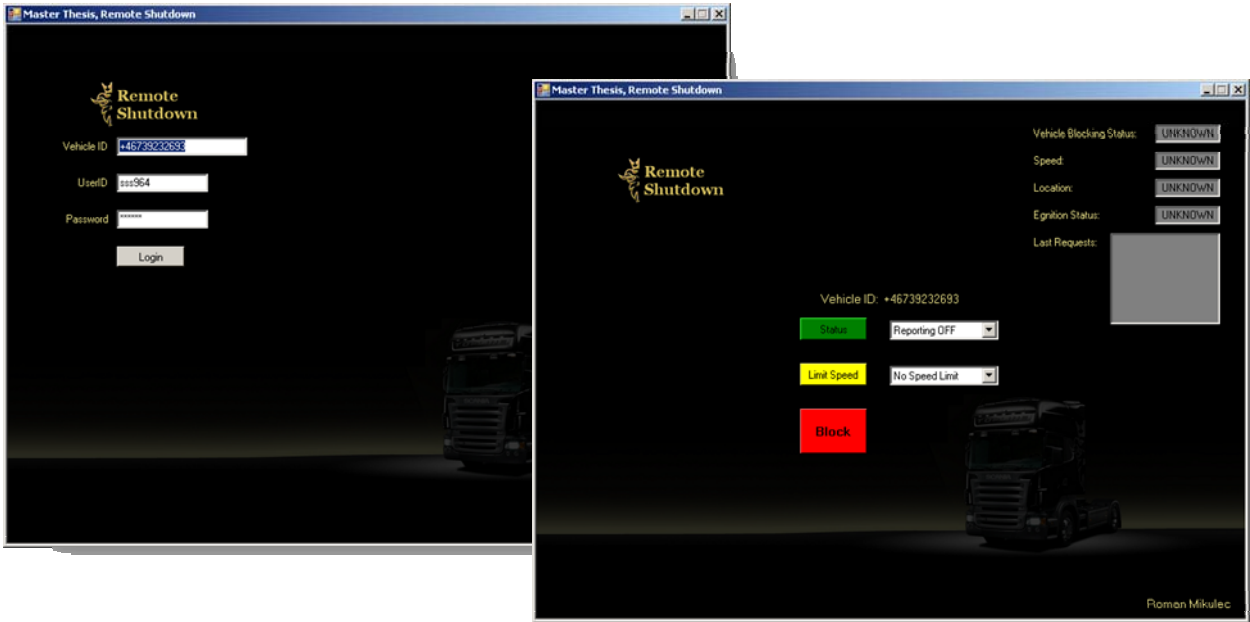


Figure 25, the first version of the office application. This interface really showed how hard it is to shut down a vehicle by only looking at numbers on a screen.

Figure 26



Figure 26, the second version of the office application. In this version, graphical indicators are used to display parameters such as speed, odometer, ignition and fuel level. Pressing the "Map" button displays the current vehicle position using Google Maps.

10.4 Blocking information

To be able to test different stopping techniques and the performance of the prototype, it was essential to find a way to make the system as flexible as possible. To achieve this, a new message type containing all the remote blocking parameters was created. See figure 27.

- Blocking code
- Blocking type
- Time between CS messages
- Speed limit

10.4.1 Blocking code

An 8 bit blocking code was added only to test the performance of the prototype. It was not visible to the user but adds time and complexity to the system.

10.4.2 Blocking type

As discussed in chapter 8 “Remote Shutdown”, one stopping technique is perhaps not enough to cover all possible traffic situations. For that reason different blocking techniques can be executed with the prototype.

10.4.3 Time between CS messages

The 8 bit timer can be used to select the time between each CS message. Ranging from 255 to 1 second, the timer can be used to test overall system performance.

10.4.4 Speed limit

A 16 bit speed limit is used to limit the vehicle speed with extremely high accuracy. Three different limits are implemented in the office GUI but can be easily modified if necessary.

10.5 Vehicle information

When looking at all the information needed to perform a secure blocking of the vehicle, one quickly realizes the current status message contains all relevant data about the vehicle. Instead of creating a new message and extending FMP to handle the new message type, it is much better to extend the current status message with information about the blocking status of the vehicle. See figure 28. All other information is already present, see table 1.

The main advantage of this approach is the ability to track when and what occurred along the way when remote shutdown was executed. Since all information in CS messages is stored in the database the only additional work to be done is displaying the remote blocking status when plotting the vehicle route on the map. In this way it will be possible to track when and where the remote blocking request was received and when it was executed by the vehicle [h].

Quick facts

In order to verify correct function of all ECU's in extreme conditions, each year vehicles are put to the test in the yearly winter and summer tests [4]. Temperatures can reach values from -35 to +50 °C.

Flexible solution

The prototype is developed with flexibility in mind. All values can be varied in order to find the best stopping technique and study system performance.

Figure 27

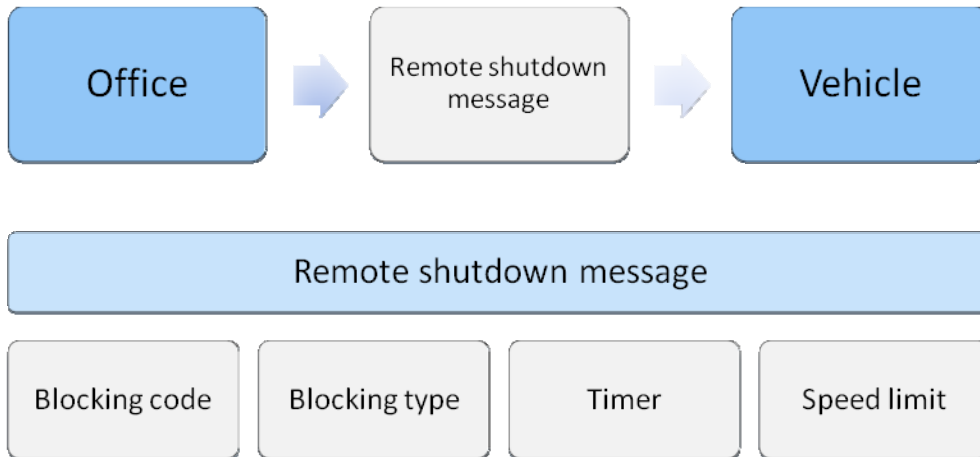


Figure 27 illustrates the new remote shutdown message. The message contains all information needed for the vehicle application to perform a remote shutdown. It is also possible to change all parameters and experiment with different values from the office application during testing.

Figure 28

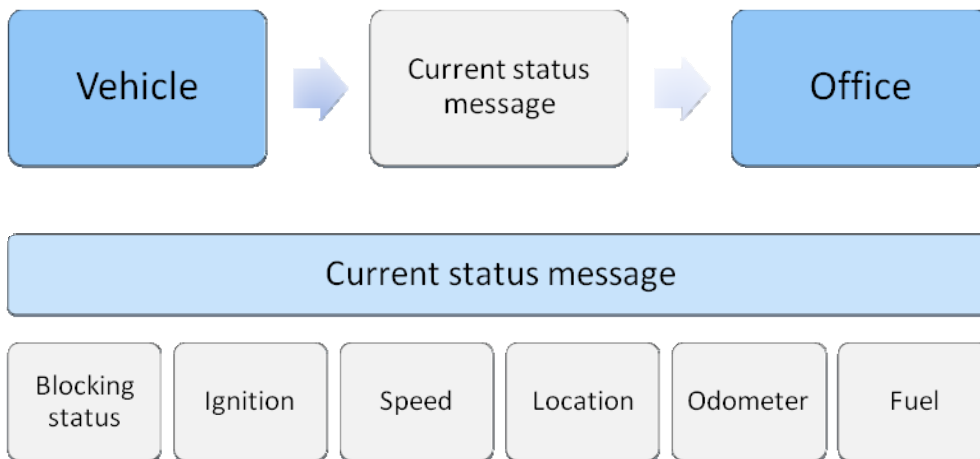


Figure 28 illustrates the flow of information between the vehicle and the office. Although the current office application only monitors the above shown parameters, any parameter in the current status message can be added to the GUI.

10.6 Application design considerations

In order to receive and interpret remote shutdown requests from the office, a new application must be added to the C200 unit and some changes made to the existing software. Before any code was written some consideration must be taken about the application design.

10.6.1 Aborting the remote shutdown

It must be possible to abort the remote shutdown if it is clear that the vehicle is heading to an area where remote blocking is unsuitable. This could be the case if the vehicle is traveling on a highway or in the center of a city.

10.6.2 Enabling/disabling supervision

When enabling the supervision of the vehicle, the application will trigger current status messages to be sent to FMP with time intervals specified in the remote shutdown message. Value zero disables the supervision thus returns C200 to the normal state.

10.6.3 Enabling/disabling speed limit

If speed limit is requested, the application will start by checking the provided blocking code. Once the blocking code is confirmed, the application will activate supervision and speed limit with the values specified in the remote shutdown message. If no timer is specified, the default value of 15 seconds will be used.

10.6.4 Enabling/disabling remote shutdown

When the remote shutdown command is received and the blocking code is confirmed the application will first activate the supervision state with the time specified in the remote shutdown message. If no time is specified, the default value of 15 seconds will be used.

If speed limit value is zero, the application will supervise vehicle speed and execute the shutdown as soon as the speed reaches zero. During this time it is possible to abort the remote shutdown if desired.

If no speed limit is specified the application will start executing the remote shutdown with no regard to vehicle speed. This allows for immediate action if necessary.

10.7 Remote shutdown application module

A new application module was created and the structure of the final application can be seen in figure 29 on the next page.

Once the application is initiated it starts by making a subscription to remote shutdown messages from the communication handler. Each time a new message of this type is received the remote shutdown application will be notified and the contents forwarded to the application.

The internal timer will be set to the value received in the remote shutdown message and for each expired timer, the adjacent application handling current status messages will be triggered into sending data to FMP.

To execute the speed limit or the remote shutdown, the remote shutdown application triggers an adjacent application to send CAN data which affects engine performance. How that is done will be explained in the next chapter.

10.8 Modifications to existing software

The main application handler was modified to start the remote shutdown application and keep it running.

In order for the new application to receive remote shutdown messages, the server application handling incoming messages needed some modification. The new message type described in the previous chapter was added otherwise the data would be recognized as invalid and deleted [g].

Also the server module handling CAN communication was modified. New CAN messages with the possibility to modify engine performance were added.

Quick facts

The vast majority of people working with research and development got their heavy vehicle driving licences when working at Scania and are often out on the test track testing the products during development [4].

Remote shutdown application module

A block diagram or a flow chart is crucial when creating a new application module. Once complete and satisfying, it was time to start programming.

Figure 29

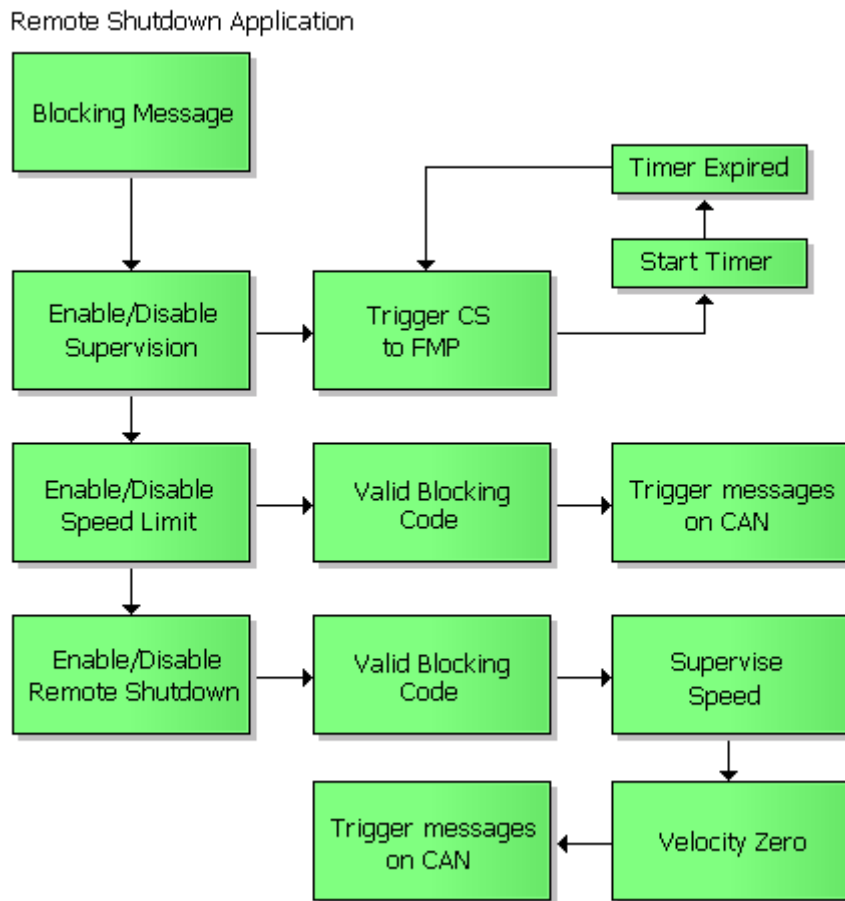


Figure 29, the remote shutdown application shown in a block diagram. When a blocking message is received by C200, the message is forwarded to the remote shutdown application. If the message contains commands for vehicle supervision, the application will periodically trigger CS messages to be sent to FMP. If speed limit is requested, the blocking code will be checked and the vehicle will be limited to the specified speed and supervision activated. Under normal circumstances, if remote shutdown is requested, the blocking code will be verified, the speed monitored and the engine shut down as soon as the speed reaches zero.

11 Testing

11.1 Breaking the silence

Until now the C200 unit had only listened to CAN data, collected specified information and reported the data to the fleet management portal. The only messages sent from the C200 were during vehicle maintenance in order to identify itself in the electrical system and report any DTC's stored in memory [c].

Diagnostic Trouble Code, DTC, readout is a way to check the status of an electronic unit. All units are designed to detect and report certain kind of errors which makes it easier for maintenance personal to find and replace broken parts.

With changes made during development of this prototype, not only will the C200 break the silence, it would also have the ability to change engine performance.

11.2 Modifying engine performance

In order to try out different stopping techniques, there was a need to find a way to modify engine performance with the C200 ECU.

A search through the communication database of the engine ECU presented a feasible solution. A message called "External control message" could be used to limit engine speed or execute a controlled engine stop [j].

The external control message is part of Scania's bodywork system which is an interface used for aftermarket add-ons to the vehicle such as cranes, winches and other systems. Often, these add-on systems are equipped with different security features such as emergency stop buttons or engine performance restrictions.

Since it is beyond the limits of this thesis to implement new functionality in other control modules than C200, this solution would give the desired functionality just by making an easy reconfiguration of the COO unit.

Bodywork System, BWS, is an ECU supplied by Scania to give bodybuilders access to different parameters on the CAN bus and also allow for certain control of vehicle performance.

By activating the BWS functionality in the COO unit, the C200 can be used to limit vehicle speed and execute a controlled engine stop. See figure 30.

11.3 Testing performance

One goal of the prototype was to perform measurements of the overall system performance. That includes time between sent and received messages, delays in the system and application and start up behavior. Four tests were performed on the finished prototype.

- Response time, vehicle turned on
- Response time, vehicle turned off
- Response time until engine reaction
- Message update rate

11.3.1 Response time, vehicle turned on

This test measures the time between a command is sent from the office GUI until it reaches the remote shutdown application module inside the C200 unit. The test was performed using a test bench inside the office.

11.3.2 Response time, vehicle turned off

This test measures the time between a command is sent from the office GUI until the external control message is visible on the CAN bus. The measurements were carried out in office environment.

11.3.3 Response time until engine reaction

This test measures the time between a command is sent from the office GUI until changes to vehicle performance are noticed by the driver. It will be done by sending a speed limit request and the test was performed at Scania's test track in Södertälje.

11.3.4 Message update rate

This test measures the maximum update rate for current status messages. By decreasing the time between each trigger, the unit will increase the message rate until the data rate reaches the limit of GPRS capability. The measurements were carried out in office environment.

Quick facts

Many tests during development are carried out at Scania's very own test track in Södertälje. The 14 km long test track is equipped with vibration zones and slopes with varying inclinations.

Scania ECU's

Depending on the vehicle type and configuration, a modern truck can contain numerous electronic units. At the end of the assembly line, each ECU is configured depending on the current vehicle type and present ECU's. Correct ECU configuration is crucial for right communication between ECU's [a]. For example, if the COO is told there is no BWS present, the external control message will be ignored by the COO thus making engine performance modifications impossible.

Figure 30

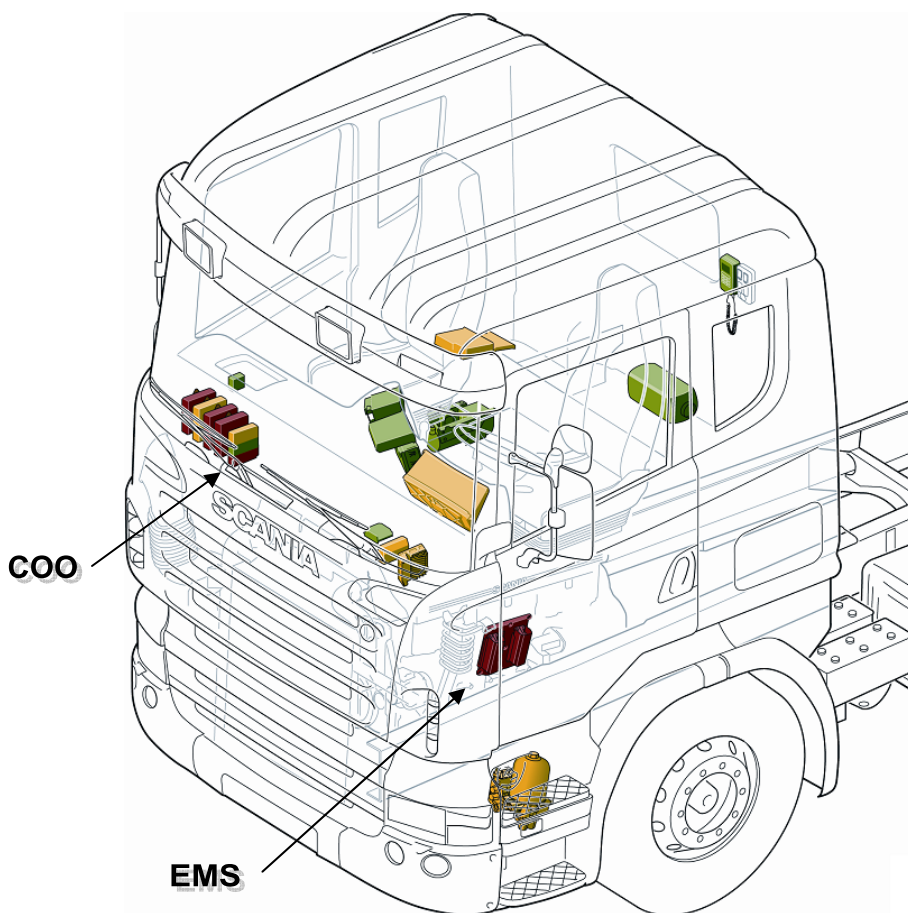


Figure 30 illustrates a left hand driven truck and the numerous ECU's present in the vehicle. The different colors represent which CAN bus the ECU is connected to. Notice the COO placed in the dashboard in front of the passenger seat and the EMS placed directly on the engine.

12 Results

12.1 Test results

Figures 31 to 33 on next page show the results of the first three tests. As mentioned earlier the latency of FMP and GPRS system has quite large variations as can be seen in the first figure. The shortest measured time is 2.2 seconds compared to the longest time of 12.3 seconds. It would not be suitable to use the system for real-time shutdown of vehicles.

When performing the second test a rather disturbing delay in the system was discovered.

Because C200 runs Linux and powers down with the rest of the truck when the ignition is turned off, it also needs some time to start up and establish a connection with FMP when the ignition is turned back on. At this moment (22 April 2008) the C200 needs 55 seconds to boot and another 10 seconds to establish GPRS connection if good coverage is present.

The third test verifies the boot-up time and latency of the system. Once the vehicle ignition is turned on, it takes at least 72 seconds until the remote shutdown message is received, processed and speed limit command sent to the engine.

Before discussing the last test, let us consider the effects of the boot-up time of the C200 unit.

12.2 Vehicle immobilization

The rather long boot-up time introduces a somewhat difficult problem; immobilizing the vehicle when the ignition is turned off and prevent it from driving away. Since it is unrealistic to wait for more than a minute to be able to start the vehicle, a different solution must be adopted.

One possible solution to this problem is to power up the C200 unit with fixed time intervals to receive remote immobilization messages and forward them to the central ECU and immobilizer if immobilization is requested. But this is beyond the limits of this thesis [b].

12.3 Performance test

Once the prototype was up and running a lot of experimenting was done. One of the more interesting tests was the message update rate. It was possible to lower the timer to approximately 5-4 seconds before the triggered messages were put on queue instead of sent to FMP.

It was quite exciting to see the graphical indicators update every 5 seconds. It gives the user a feeling of control when sitting in the office watching the Remote Shutdown GUI. Still, the delay together with the latency shown in figure 31 makes it hard to execute a remote shutdown in real-time.

12.4 Security

The overall security of the system is more than satisfying. The risk of unauthorized access to the remote shutdown functionality is seen as minimal.

In order for someone to immobilize vehicles running on our roads, they must be connected to Scania's Intranet, have the proper software and FMP connection and also have the correct customer authentication code. Furthermore, the remote shutdown can only be executed on vehicles which have the remote shutdown functionality activated.

The greatest challenge is definitely external factors such as antennas and GSM coverage.

12.5 VOR

VOR stands for Vehicle Off Road and reflects the undesired time the vehicle is out of operation due to manufacturing issues. Scania always strives to minimize the number of faults which can cause a VOR [4]. By introducing the C200 unit and making it critical for vehicle operation, we add risk of VOR [b].

Quick facts

All vehicles used for development purposes are given unique names. The vehicle used for testing the remote shutdown function was named Mago.

Prototype testing and results

Tests were performed in the office and on Scania's test track in Södertälje.

Figure 31

Testing the response time when vehicle is turned on

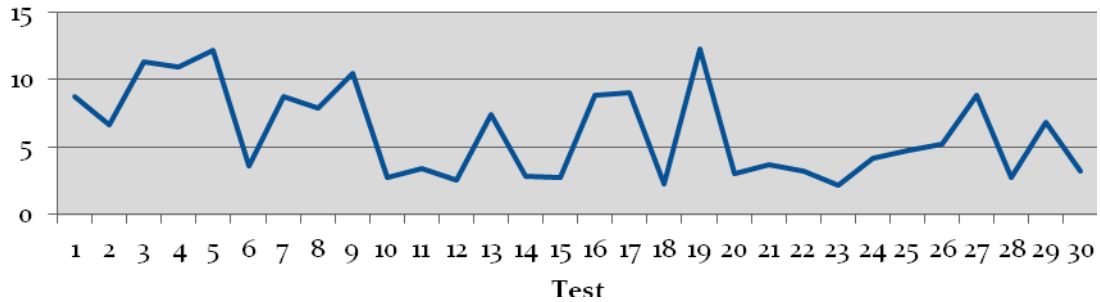


Figure 31 shows the time it takes for a remote shutdown message to reach the C200 unit.

Figure 32

Testing the response time when vehicle is turned off

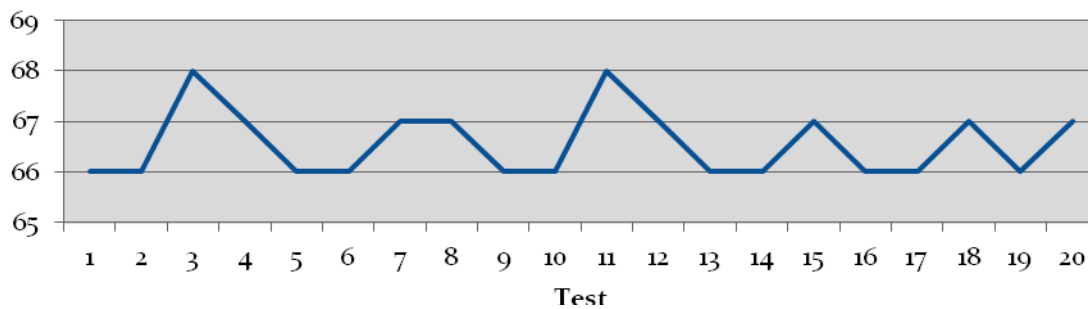


Figure 32 shows the time it takes for the C200 unit to boot up and to receive the first remote shutdown message.

Figure 33

Testing the response time until engine reaction

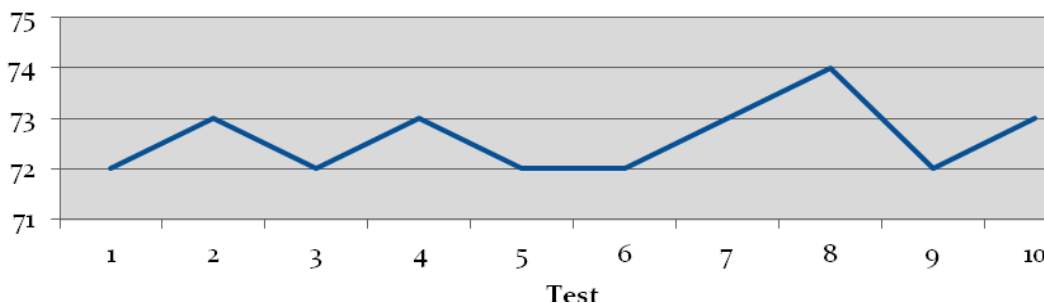


Figure 33 shows the time it takes for the driver to notice the speed limit function from the time he turns the ignition key to on-state.

13 Conclusion and future work

13.1 Conclusion

This thesis project was by far the most interesting but also the most complex project throughout my education. The complete process from design considerations to actually implementing code and testing the final prototype was particularly instructive.

One also comes to realize the importance of all different people involved in this project, not only the developers but also all the people involved in planning and managing the interfaces between all the different systems. One mistake or change done unsynchronized to other systems and you end up with a bunch of unrecognized messages deleted by the C200 or FMP.

As mentioned in the last chapter the risk for unauthorized access to the remote immobilization function is seen as minimal. There are easier ways of stealing vehicles than hacking into Scania's fleet management services.

I personally believe the risk of VOR due to electronics failure or cable harness failure is higher than the risk of unauthorized access to the remote shutdown functionality leading to customer dissatisfaction and frustration. This must be considered during implementation of the final solution.

In the beginning of the thesis a second option to developing and upgrading the existing unit was mentioned, which is the possibility to introduce a third party unit. At the approximately same time as the government in Brazil proposed the required Anti-theft device, a company in Brazil introduced a small device which fulfills all government requirements. A coincidence or a good way of making money?

A huge factor in the final decision will also be the legal aspect [b]. Who is to blame if an accident does happen?

13.2 The future of remote shutdown

There are several challenges facing realization of the remote shutdown function. Hopefully, this thesis project and the finished prototype give some indications on the potential and limitations of the system. The flexible approach of the final prototype makes it possible to put different stopping techniques to the test and also experiment with the message rate to find a balance between data amount and information update.

Apart from the technology challenge itself the introduction of the remote shutdown comes with a huge amount of administrative work as well. New codes to keep track of for the remote shutdown purpose, a dedicated team of people handling the execution of the function and so on.

13.3 Endless possibilities

As the first samples of the Communicator were being developed, Scania decided to make the unit standard equipment on all vehicles. The decision opened for endless possibilities in the future [c].

13.3.1 FMS for everyone

All customers will have the possibility to benefit from the fleet management services.

13.3.2 Remote statistics

Scania would have a new way of collecting vehicle data in order to improve vehicle uptime and performance. With all vehicles reporting all errors, new important statistics would be available [g].

13.3.3 Remote diagnosis and assistance

If an error occurs on the road, it will be possible to read vehicle trouble codes, hence be able to bring proper service parts when assisting the driver.

13.3.4 Remote ECU update

New software could be transmitted to the vehicle and specific ECU's updated without driving the vehicle to a Scania workshop [c].

Quick facts

In the year 2008 Scania delivered 66.516 trucks from which 10.775 was to the Brazilian market. Scania also delivered 7.277 busses and 6.671 engines [18].

14 References

14.1.1 Literature

- [1] Jochen Schiller, Mobile Communications Second Edition, Great Britain, 2003
- [2] Behrouz A. Forouzan, Data Communication and Networking Third Edition, New York, 2004
- [3] Scania CV AB, Liten historiebok om Scania – En stor fordonstillverkare, Södertälje, 2007
- [4] Scania CV AB, R&D Factory, Södertälje, 2010

14.1.2 Specifications

- [5] Modules and Sockets, REIV internal documentation
- [6] Software and Testing, REIV internal documentation
- [7] CAN specification, RESA internal documentation
- [8] Background to the Brazilian Anti Theft Device, Scania and Volvo joint investigation
- [9] Brazilian ATD preliminary proposal 2008

14.1.3 Internet (Last update 2012.04.09)

- [10] <http://www.irisat.com.br>
- [11] <http://www.volvotrucks.com/trucks/brazil-market/pt-br/Pages/home.aspx>
- [12] <http://www.gsma.com/home/>
- [13] <http://en.wikipedia.org/wiki/GSM>
- [14] <http://en.wikipedia.org/wiki/GPRS>
- [15] http://en.wikipedia.org/wiki/Controller_area_network
- [16] <http://www.semiconductors.bosch.de/en/ipmodules/can/whatiscan/whatiscan.asp>
- [17] <http://scania.se/tjanster/fleet-management/>
- [18] <http://www.scania.com>
- [19] <http://imagebank.scania.com/>
- [20] <http://www.gps.gov/>

14.1.4 People

- [a] Mathias Björkman, Fleet Management Cross Functional Coordination, Scania CV AB, Södertälje, Sweden
Supervisor and Fleet Management Services senior staff
- [b] Mats Axelsson, Fleet Management Cross Functional Coordination, Scania CV AB, Södertälje, Sweden
Remote Blocking Function Owner
- [c] Håkan Nilsson, Fleet Management On Board Platform, Södertälje, Scania CV AB, Sweden
C200 software architect
- [d] Daniel Prado, Remote Blocking Systems, Scania CV AB, São Paulo, Brazil
Scania IRIS
- [e] Niklas Thörnqvist, Fleet Management Test and Verification, Scania CV AB, Södertälje, Sweden
Communication between FMP and C200
- [f] Magnus Rosenius, Fleet Management On Board Platform, Scania CV AB, Södertälje, Sweden
C ++ programming, C200 Applications and Software Test
- [g] Anders Björkman, Fleet Management On Board Platform, Scania CV AB, Södertälje, Sweden
C200 Applications and Software Test
- [h] Henrik Hofling, Fleet Management Internet Platform, Scania CV AB, Södertälje, Sweden
Scania Communication Protocol Version 2
- [i] Roland Lindblom, Climate & Safety System, Scania CV AB, Södertälje, Sweden
Remote Blocking Function
- [j] Jan Sterner, Chassis System Design, Scania CV AB, Södertälje, Sweden
COO and Remote Blocking Function
- [k] Miljenko Mikulec, Miljenko Mikulec Åkeri, Malmö, Sweden
Hauler and economy information

15 Abbreviations

3G	Third Generation GSM
AUC	Authentication Centre
BS	Base Station
BSC	Base Station Controller
C200	Communicator 200
CAN	Controller Area Network
COO	Coordinator
CPU	Central Processing Unit
CS	Current Status Message
DNS	Domain Name System
DTC	Diagnostic Trouble Code
ECU	Electronic Control Unit
EIR	Equipment Identity Register
EMS	Engine Management System
EMC	Electromagnetic Compatibility
FMP	Fleet Management Portal
FMS	Fleet Management Services / Fleet Management System
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile telecommunications
GUI	Graphical User Interface
HLR	Home Location Register
I/O	Inputs/Outputs
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
MAC	Media Access Control
MSC	Mobile Switching Centre
NRZ	Non-Return-To-Zero
OS	Operating System
PC	Personal Computer
PTO	Power Take Out
R&D	Research & Development
SCP	Scania Communication Protocol
SESAMM	Scania Electric System Anno 2000
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SMS	Short Message Service
TDMA	Time Division Multiple Access
UHF	Ultra High Frequency
URL	Uniform Resource Locator
VABIS	Vagnfabriken I Södertälje
VLR	Visitor Location Register
VOR	Vehicle Off Road
WLAN	Wireless Local Area Network
YETD	Young European Truck Driver

16 Figures

Figure	Page	
1	2	Number of incidents in Brazil between 1995 and 2003
2	2	Financial losses of transported goods in Brazil between 1995 and 2003
3	4	Showing the cost distribution of a typical transportation company
4	4	Scania FMS can be used to evaluate and educate drivers
5	8	Fleet Management System consist of several technologies
6	8	The first generation telematic unit was called the Interactor
7	10	A handheld GPS navigator
8	10	GPS satellite constellation
9	12	Up and downlink of the GSM network
10	12	GSM network structure
11	14	GSM network structure when extended with GPRS
12	16	CAN message structure
13	18	Arbitration scheme of CAN messaging
14	18	SESAMM, Scania Electric System Anno 2000
15	20	A Scania R440 posing in the sundown
16	20	A Volvo truck made for the American market
17	22	Different screenshots of the Scania Fleet Management Portal
18	24	The Interactor 500 with a 7" touch screen
19	26	Scania Communicator 200 connector view
20	26	Different layers and modules of the C200 software
21	30	Risks involved with remote shutdown put on a scale
22	30	Chart illustrates systems between the office and the vehicle
23	32	Illustration of different security measures
24	32	A Scania R730 testing four different communication antennas
25	34	First version of the Remote Shutdown Office Application
26	34	Final version of the Remote Shutdown Office Application
27	36	The remote shutdown message
28	36	Parameters used by the remote shutdown office application
29	38	Flow chart of the remote shutdown application module
30	40	Placement of different ECU's and CAN bus connection
31	42	Test results from performance test 1
32	42	Test results from performance test 2
33	42	Test results from performance test 3
34	48	Image of the accident in Latin America
35	50	First truck constructed in Södertälje
36	50	Organization Chart

17 Tables

Table	Page	
1	28	The complete current status message

18 Appendix A

18.1 Scania thesis proposal (Swedish)

18.1.1 Bakgrund

Idag har Scania ett traditionellt stöldskyddssystem. Systemet är uppbyggt av en transpondernyckel ansluten till bilens centraldator som kommunicerar med motorstyrenheten via CAN-bussen.

Scania utvecklar även Fleet Management system och larmsystem vilket sammantaget kan ge lägre försäkringspremier, speciellt om man kan erbjuda fjärravstängning av fordon som lämnar den tänkta rutten, eller på annat sätt betar sig konstigt ur transportplanerarens synvinkel.

18.1.2 Mål

Skapa en effektiv och säker telematik-arkitektur för ett nytt system för fjärravstängning baserad på Scantias kommande telematik blackbox, Fleet Management Portal, larmsystem, centraldator och motorstyrssystem.

18.1.3 Uppdragsbeskrivning

- Sätt dig in i hur dagens fleet management-, larm- och immobilizersystem fungerar
- Dokumentera systemarkitektur och funktionalitet
- Kartlägg i vilka fall det är möjligt resp omöjligt att stänga av fordon
- Föreslå en systemarkitektur för telematikdelen (kommunikator och portal) av fjärravstängningsystemet
- Kartlägg hot och möjligheter i samband med trafiksäkerheten resp intrångsrisken i systemet
- Bygg ett demosystem där fordon skall kunna stoppas resp förhindras starta från en kontors-PC

Antal studerande: 1

Startdatum för exjobbet: Dec 2007 eller senare

Beräknad tidsåtgång: 20v

Bakgrund: 180p elektro, fysik, data eller mekatronik.

Kunskaper i Linux, C++ och programmering av webapplikationer är meriterande.

Kontaktperson: Peter Madsen, 08 5538 5922, peter.madsen@scania.com

Handledare: Mathias Björkman, 08 5538 0761, mathias.bjorkman@scania.com

Handledare: Mats Axelsson, 08 5535 2645 , mats.axelsson@scania.com

19 Appendix B

19.1 The accident

Two weeks into the project a horrible accident occurred in Latin America and we were immediately notified by our staff in Brazil. The picture shows the accident and is taken from the local newspaper O Estado de São Paulo on Monday the 21st of January 2008.

Even though the insurance company denies it, the most probable cause for the vehicle stopping in the middle of the street is remote shutdown of some kind. When the hijackers noticed the truck lost speed and things did not go as intended they abandoned the truck in fear of the police in the middle of the road between São Paulo and Rio de Janeiro on Sunday morning.

It all started the night before when the driver made his last pickup of the day, three men forced their way into the truck, hijacking the vehicle, the driver and the load. The load, two cranes approximately worth 165 000 USD a piece, are still missing without a trace along with the hijackers. The driver who was thrown out of the truck on Sunday morning was quickly able to free himself and call the owner of the truck to inform him of the robbery and ask to be picked up 75 km from the capital where he was thrown out.

Figure 34



Sunday, 20th January 2008, an abandoned truck in the middle of the highway was the cause of a major accident where one person died immediately and two others were rushed to the hospital with severe injuries.

After informing the insurance company the owner was off to pick up the abandoned driver. As he was driving down the highway he spotted the stolen truck standing in the middle of the road in the opposite direction. Afraid that the hijackers were still inside the truck he held a distance, parked down the road, called the police and waited for them to show up.

Not long after his call another truck crashed into the motionless vehicle. With a speed close to 80 km/h the damage was terrible. Then another truck crashed into the pile of metal blocking the entire lane. The fourth vehicle involved was a Fiat Siena with two passengers. The 49 year old driver past away immediately while her 23 year old son was taken to the hospital along with the truck driver who crushed them from behind into the wreckage.

Last but not least a tourist bus crashed into the pile of vehicles. The heavy rain and oil on the road made it impossible to stop on time. 6 vehicles were involved on this Sunday morning accident and the owner who is an eyewitness later said "It was horrible and there was nothing I could do".

20 Appendix C

20.1 Scania CV AB

Today Scania is one of the world's leading manufacturers of heavy trucks and buses.

20.1.1 History

Vagnfabriken in Södertälje, VABIS, was founded in the year 1891. It was then producing railroad carts for the Swedish State Railways, SJ, and Stockholm Tramway. In the year 1900 a company called Maskinfabriksaktiebolaget Scania was founded in Malmö. Scania, whose product range included bicycles, had successfully begun small-scale car production. A few years later, in 1911, Scania and Vabis formed a new company called Scania-Vabis to handle the growing demand for cars, trucks and buses on the European market.

The first Swedish private car with a combustion engine was constructed in 1897 by Gustav Erikson at Vabis Södertälje. Five years later Vabis made their first truck (see figure 35 on next page). It had a load capacity of 1.5 tons and a top speed of 12 km/h.

20.1.2 Production

From the start until now Scania has produced more than 1.400.000 vehicles.

20.1.3 Scania's unique module system

Scania's production system can be seen as a huge box of LEGO. By making balanced and carefully chosen performance steps but keeping the interface between the components the same, a huge variety of vehicles can be produced with a limited number of components.

Since each component adds to the storage and production cost there is a huge benefit in lowering the total number of components in production. The modular system enables the same components to be used in both trucks and buses, further lowering the total amount of components. A Scania tourist coach can have up to 85% identical components as a truck.

20.1.4 Scania worldwide

Today Scania's products are sold in more than a 1000 shops in approximately hundred countries worldwide. With more than 1500 maintenance places around the world, you never have to drive far if you are in need of repair or spare parts. The Scania concern employs slightly more than 30.000 people around the world.

20.1.5 Research & Development

Almost all of research and development is carried out at Scania Södertälje. The nearly 2500 engineers are located in different buildings at Scania research and development center. Scania R&D is basically split up in two branches, Powertrain Development and Truck Cab and Bus Chassis Development. The Fleet Management department where this thesis project was carried out is split in four groups; On-Board Platform, Internet Platform, Test and Verification and Cross Functional Coordination. My supervisors were located in the last mentioned group. See figure 36.

20.1.6 YETD

Young European Truck Driver is a competition held each year at Scania in Södertälje. The first competition was held in 2003 as a project to bring awareness to security and fuel economy in close collaboration with EU.

The competition was a huge success and has been held every year since then. Similar competitions are now also held in Latin America, Africa, Asia and Australia. Over the years more than 100.000 young drivers have participated in the competitions.

Competing in seven categories which include security, economic driving and maneuvering the winner leaves Södertälje with pride and a brand new Scania R440!

Scania CV AB

Hundred years of development has made Scania one of the biggest heavy vehicle manufacturers in the world!

Figure 35



Figure 35, the first truck constructed in Södertälje in the year 1902.

Figure 36

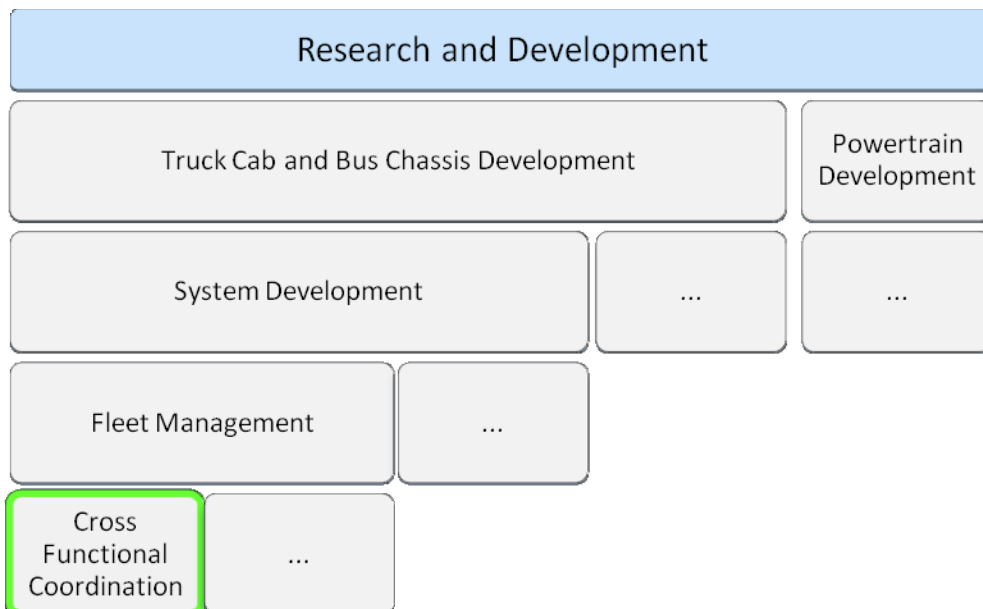


Figure 36 illustrates parts of Scania R&D organization chart. This thesis project was performed at the Cross Functional Coordination group at the Fleet Management department.



Malmö 10 April 2012

This thesis project was carried out at Scania in 2008 but the report presented in 2012. Since there is still no final decision from the government in Brazil, there is no final solution presented from Scania and all data in this report is still applicable.