New immobilizer concept based on Scania’s electrical platform

Navid Varzandeh

2019

Degree project, Advanced level (Master degree, two years), 30 HE
Electronics
Master Programme in Electronics/Automation

Supervisor: Simon Varli
Examiner: José Chilo
Preface

First and foremost, I am grateful to the god for granting me the patience, determination, passion and health to accomplish completing this thesis successfully.

I would like to express my gratitude to Andreas Jerhammar, the head manager of embedded SW & functions department in Scania CV AB for providing me with this opportunity and believing in me and my abilities to succeed in this thesis.

I would also like to acknowledge and appreciate my supervisor, Simon Varli for his time, supervision, support and constructive feedback throughout my work with him.

I wish to thank each and every knowledgeable, caring and supportive member of embedded SW & function department for providing a friendly and productive condition for carrying out my thesis as well as their assist and support.

Finally, I would like to dedicate this thesis to my beloved parents for their unconditional and never-ending supports and sacrifices without which I could not have achieved my goals.
Abstract

Immobilizers are security systems that are set up and installed in modern vehicles in order to prevent thieves from starting the vehicles. The idea is that if any wrong keys are used to start the vehicle, the immobilizer detects the wrong key and start the immobilization procedure to stop the vehicle from turning on.

The vehicle ignition key (key transponder or key fob) is one of the important components in an immobilizer system. An ignition key in an immobilizer system has a Radio Frequency Identification Device (RFID) chip inside it. This RFID chip holds a specific encryption algorithm and particular number of bits (encryption key bits) in itself. Using the encryption algorithm and encryption key bits, RFID chip inside the key authenticates and identifies itself as the right key to the immobilizer system in order to disable the immobilization procedure and start the vehicle.

However, there are two ways thieves can disable the immobilization procedure and start the vehicle. The first approach is by discovering the specific encryption algorithm and key bits in the right key transponder (RFID) and using them to duplicate the correct RFID chip to disable the immobilization procedure and start the vehicle. The second approach is by exploiting the vulnerabilities and weaknesses in vehicle security network (CAN bus) to bypass the immobilizer and manipulate the immobilization procedure to start the vehicle.

Scania vehicles are not using the most secure RFID and immobilization procedures, hence they are vulnerable to two vehicle theft approaches above.

Therefore in this thesis project, I have done research and investigation on Scania vehicles key transponder (RFID) and analyzed their immobilization procedures in order to identify the roots and origins of vulnerabilities in Scania RFID and immobilization procedures.

As the first result of this thesis work, I have found and proposed an RFID chip having one of the strongest encryption algorithms and proper number of encryption key bits for all Scania vehicles. As the second result of this thesis project, I have proposed and introduced two new individual immobilization procedures exclusively for Scania hybrid and electrical vehicles.

Both proposed RFID (encryption algorithm) and immobilization procedures will be implemented in Scania vehicles in near future and will increase the security of Scania immobilizers significantly.
Table of contents

1 Introduction .................................................................................................................. 8
  1.1 Background .............................................................................................................. 8
    1.1.1 RFID recognition .............................................................................................. 8
    1.1.2 Immobilization procedure ............................................................................... 9
  1.2 Thesis objectives & proposed solutions ..................................................................... 10
  1.3 Thesis outline .......................................................................................................... 11
2 Theory .......................................................................................................................... 12
  2.1 Immobilizer RFID chip ............................................................................................ 12
  2.2 RFID validation process technique ......................................................................... 12
    2.2.1 Challenge–response technique ......................................................................... 13
  2.3 Encryption ................................................................................................................ 13
  2.4 Immobilizer description ........................................................................................... 14
  2.5 Immobilizer system architecture ............................................................................... 14
    2.5.1 Central ECU ...................................................................................................... 14
    2.5.2 Random number generator (RNG) .................................................................. 15
    2.5.3 Power ECU ....................................................................................................... 15
    2.5.4 Transceiver ...................................................................................................... 15
    2.5.5 Transponder ..................................................................................................... 15
    2.5.6 Instrument Cluster ........................................................................................... 15
    2.5.7 Starter switch .................................................................................................... 16
  2.6 Immobilizer system functionality .............................................................................. 16
    2.6.1 Key validation ................................................................................................... 16
    2.6.2 Power ECU validation ...................................................................................... 17
  2.7 Controller Area Network (CAN) bus ......................................................................... 18
  2.8 Fundamental components in electrical vehicles ....................................................... 19
    2.8.1 Variable frequency drive (VFD) ....................................................................... 20
    2.8.2 Electrical machine (Electrical motor, Induction motor) .................................... 20
    2.8.3 Fuel cell ........................................................................................................... 20
    2.8.4 Power inverter (inverter) ................................................................................... 20
    2.8.5 Transmission solenoid ...................................................................................... 21
3 Process and results ........................................................................................................ 22
  3.1 Improvement of Scania Immobilizer RFID chip ...................................................... 22
    3.1.1 Vulnerabilities in current Scania immobilizer RFID chip .................................... 23
    3.1.2 AES as new proposed RFID encryption algorithm ............................................ 27
    3.1.3 Overview of current known attacks on AES ....................................................... 31
    3.1.4 AES security measurement criteria .................................................................... 36
    3.1.5 Security analysis of proposed RFID encryption algorithm ............................... 37
    3.1.6 Security comparison of AES, DES, RSA encryption algorithms ....................... 40
  3.2 CAN bus vulnerabilities ............................................................................................. 44
    3.2.1 Lack of segmentation and boundary defense ..................................................... 44
3.2.2 Lack of device authentication .................................................. 44
3.2.3 Unencrypted traffic .................................................................. 45
3.3 Solutions to CAN bus vulnerabilities ............................................. 46
  3.3.1 Encryption ............................................................................ 46
  3.3.2 Device authorization ............................................................... 46
  3.3.3 Defense in depth ................................................................. 47
3.4 Improvement of Scania immobilization procedure ......................... 49
  3.4.1 Current immobilization approach in EV .................................. 49
  3.4.2 Advantages of current EV immobilization approach .................. 50
  3.4.3 Disadvantages of current EV immobilization approach .............. 51
  3.4.4 New proposed immobilization approach for Scania EV ............... 52
  3.4.5 Current immobilization approach in Scania HEV ....................... 54
  3.4.6 Disadvantages of current HEV immobilization approach .......... 55
  3.4.7 New proposed immobilization approach for Scania HEV ............. 56
4 Discussion ..................................................................................... 59
  4.1 Immobilizer RFID chip ............................................................. 59
  4.2 Immobilization procedure ......................................................... 61
5 Conclusions .................................................................................... 63
References ......................................................................................... 67
1 Introduction

Security is an important matter when it comes to the safety and protection of private or public assets and belongings.

1.1 Background

There are many Electronic Control Units (ECUs) set up in a modern vehicle and the task of each ECU is to control the performance of each respective system. Immobilizer is a system in a modern vehicle hence it requires an ECU to control its performance. The ECU which controls the immobilizer system is called Central ECU since it is in the center of all other components and ECUs in an immobilizer system.

Immobilizer main function is to prevent thieves to start the vehicle. This is done by validation processes between different components and ECUs in the immobilizer system of the vehicle. If one of the main components or ECUs is not correctly validated, the vehicle will not start.

The validation processes in an immobilizer are divided into two stages.

1. RFID recognition
2. Immobilization procedure

1.1.1 RFID recognition

The first stage is the validation process between RFID (chip inside the key fob) and Central ECU in an immobilizer system. This stage is also defined as “RFID recognition” stage. In another words, during this stage (validation process) RFID sends an encrypted radio signal of specific length to the Central ECU to authenticate and verify itself as the correct key to start the vehicle. A diagram of RFID recognition stage is shown. See Fig. 1.
RFID recognition

One of the two problems this thesis project aims to solve is that all Scania vehicles, i.e., conventional/hybrid/electrical vehicles use a simple, uncomplicated and insecure RFID which can be cracked, compromised and then duplicated by the thieves and attackers to start the vehicle.

1.1.2 Immobilization procedure

The second stage of validation processes in an immobilizer system is the validation processes between Central ECU and other ECUs in an immobilizer system that control the start of the vehicle, e.g. electrical power and electrical motor in electrical vehicles, fuel and engine in conventional vehicles.

This stage of validation is also referred to as “immobilization procedure”, hence immobilization procedure indicates the second stage of validation processes in an immobilizer system. A diagram indicating immobilization procedure stage is illustrated. See Fig. 2.
The second problem this thesis work aims to solve is the unreliability of immobilization procedure in Scania hybrid/electrical vehicles. Technology with hybrid/electrical propulsion is new. Hybrid/electrical vehicles use electrical machine alongside or instead of the standard internal combustion engine to start the vehicle. The immobilization procedures in Scania hybrid/electrical vehicles have vulnerabilities and weaknesses which introduce potential threats and opportunities associated with intrusion into immobilizer systems and bypassing them to start the vehicle.

1.2 Thesis objectives & proposed solutions

The objective of this thesis project is to propose a more reliable and more secure immobilizer system by:

1. Proposing an immobilizer RFID chip for Scania with significantly stronger encryption algorithm (cipher) that prevents thieves from cracking the RFID tag and duplicating it to start the vehicle.
2. Proposing more secure and efficient immobilization procedures (validation processes) in hybrid/electrical vehicles that prevent thieves from bypassing vehicles immobilizers by manipulating them in case of not having access to the right key.

1.3 Thesis outline

Chapter 2 provides theoretical knowledge about immobilizers as well as fundamental components and networks exploited by immobilizers in modern vehicles.

In Chapter 3 the most critical vulnerabilities and weaknesses in modern vehicle immobilizers are discussed and analyzed. Afterwards, solutions to detected vulnerabilities are proposed, explained and justified using verified security criteria.

Chapter 4 provides discussion associated with proposed solutions, i.e., advantages and disadvantages of proposed approaches and results.

Chapter 5 gives conclusion to this thesis work, i.e., final and major results, solutions and outcomes of this thesis are presented and future works and spin-off projects are briefly brought forward.
2 Theory

This chapter provides fundamental theory on RFID chip, data encryption, immobilizers architecture and functionality, vehicles network (CAN bus network) and key components in electrical vehicles to give knowledge necessary to better understand and comprehend the contents written in this thesis project regarding immobilizers.

2.1 Immobilizer RFID chip

The vehicles that are equipped with immobilizer systems have RFID chips embedded inside the vehicle key fob. The key fobs that have RFID chips inside them are called transponder keys. When the key blade is inserted in the ignition lock, the RFID tag will be asked by the vehicle to verify if the key is authorized. These immobilizer systems are designed to prevent physically coping the key as well as stealing the vehicle by bypassing the lock. Only a key with a previously paired RFID tag would be authorized to start the vehicle. The RFID technology involved typically relies on LF technology (from 120 to 135 KHz) [1].

When the key transponder is inserted inside the ignition lock (starter lock), the vehicle sends an encrypted random message consisted of number of bits called challenge to the RFID chip inside the transponder key. With the power transferred from the vehicle, the RFID wakes up the microcontroller in it, decodes the challenge, computes a response message and replies back on the LF channel. This mode of operation requires close proximity between RFID and the vehicle because the RFID has to harvest energy from the vehicle to function [1].

2.2 RFID validation process technique

There is a validation process between RFID chip and immobilizer control unit (Central ECU) inside the vehicle in order for the vehicle to verify that the correct RFID chip (transponder key) has been utilized to start the vehicle. This validation process is follows the challenge-response technique.
2.2.1 Challenge–response technique

The challenge–response technique is widely used in immobilizer systems [2], [3]. It is also known as identify friend or foe (IFF) [4]. The challenge–response technique utilizes a communication link that operates in both directions (bidirectional). In this technique, both the verifier (vehicle) and the claimant (RFID chip) share a secret encryption key and encryption algorithm. When the user toggles the transponder key inside the starter lock in vehicle, the vehicle sends a random number, i.e., a random challenge to the key fob’s RFID tag. The RFID inside key fob then encrypts the random challenge using its exclusive and individual encryption key and encryption algorithm stored in it. After that, the RFID chip sends the encrypted response to the vehicle. While the vehicle had been waiting for the response of the challenge, it also has encrypted its own challenge using the same encryption key and encryption algorithm that is stored in the RFID of that transponder key.

After receiving the response from the RFID, the vehicle compares it with its own calculated response. If both match, the vehicle validates the RFID chip (transponder key) and performs the necessary operations [5].

2.3 Encryption

Encryption is defined as a procedure and technique by which data, information and messages are encoded. The purpose for encryption is that only individuals who have been granted the permission (secret key) should be able to access the original and authentic content of encrypted message. Thus, individuals that do not have the permission (secret key) cannot decode the encrypted message and access the content of the encrypted message.

Interferences are not prevented by encryption process, however, encryption rejects giving access to actual content of encrypted data for individuals who do not have the secret key to decode the encrypted data. During and encryption process, the original and actual information or message, i.e., the plaintext, is encrypted by using an encryption algorithm, i.e., a cipher, which in result generates cipher text (encrypted text) that can be accessed and read only if decrypted.

Theoretically, it is possible to compromise and break all encryption algorithms. Nevertheless, an encryption algorithm is considered to be computationally secure if it cannot be compromised and broken within a reasonable amount of time respectively with reasonable resources. The term “reasonable” can be interpreted and defined in different ways in this context. However, current reasonable assumptions for attacks against immobilizer systems are:

- The attacker does not spend more than five minutes in the vehicle.
• The correct RFID (key transponder) is not available for more than ten days for analysis.

• The attacker is familiar with techniques to break the encryption algorithm and access the contents of encrypted message.

2.4 Immobilizer description

Immobilizer is a function, realized by several different systems and components. Immobilizer is a software lock with encrypted challenge/response validation between the components of the system. If one of the components is not correctly validated, the Power Electronic Control Unit (Power ECU) responsible for controlling fuel injection and starter motor operation in conventional vehicles with ICE (Internal Combustion Engine), blocks fuel and starter motor circuits not allowing to start the vehicle.

The ECU liable for blocking the required circuits to prevent the start of vehicle is either Engine ECU (Engine Management System) or Electrical machine ECU (Transmission Management System) depending on the vehicle configuration, i.e., conventional vehicle with ICE or electrical vehicles with electrical machine circuit or both of aforementioned combined (Hybrid). However, the validation procedure is the same regardless of ECU exercised. For the sake of simplicity, Power ECU is used when referring to Engine ECU and Electrical machine ECU.

2.5 Immobilizer system architecture

The components and their respective tasks and responsibilities in the immobilizer system are depicted in the following.

2.5.1 Central ECU

The Central ECU holds the main intelligence for the immobilizer system and also functions as diagnostics interface, both for programming and displaying fault codes. The Central ECU is the interface between key fob (transponder) and Engine ECU or Electrical machine ECU.
2.5.2 Random number generator (RNG)

One of the basic components of a random challenge signal message is a random number. A random number can be classified as dependent, partially dependent, or independent of the previously generated numbers. In the one extreme case, the random number can be cyclic. This means that a random number that is generated this time will not be generated again until all numbers within the random number space are generated. On the other extreme case, the random number is independent of the previously generated number, i.e., the probability of getting the same random number in the next time is the same as the probability of getting any other random number from the random number space. We call such a random number the noncyclic random number [5]. Random number generator is implemented as a part of Central ECU.

2.5.3 Power ECU

Power ECU is the controller of power source and required circuits associated with start of vehicle (e.g. starter motor and fuel to the engine in conventional vehicles). If Transponder-Central ECU validation or Central ECU-Power ECU validation fails, Power ECU blocks the starter motor and fuel to immobilize the vehicle.

2.5.4 Transceiver

The immobilizer transceiver is a passive component which excites the transponder via inductive power supply (wireless). It also directs the communication messages from the Central ECU to the transponder chip over LF-Communication, receives the answers from the transponder and direct them back to the Central ECU.

2.5.5 Transponder

The transponder chip is set up into the starter key. It is excited inductively by the transceiver and communicates (Wireless) with the Central ECU through the transceiver.

2.5.6 Instrument Cluster

In an automobile, an electronic instrument cluster, digital instrument panel or digital dash for short, is a set of instrumentation, including the speedometer, that is displayed with a digital readout rather than with the traditional analog gauges. Many refer to it simply as a digital speedometer.

The Instrument Cluster contains the immobilizer status LED, which functions as driver interface for displaying errors and guidance for back up start.
2.5.7 Starter switch

The starter switch is mounted on the starter lock, as is the transceiver. Signal from starter switch used by the Central ECU are B (Key in starter lock), U15 (Ignition) and U50 (Start).

A comprehensive immobilizer function architecture with connections involved between different components and units is illustrated. See Fig. 3.

![Immobilizer system architecture](image)

**Figure 3. Immobilizer system architecture.**

2.6 Immobilizer system functionality

The Immobilizer functionality can be summarized and simplified in two primary stages.

1. Validation between Key transponder and Central ECU
2. Validation between Central ECU and Power ECU (Engine ECU or Electrical machine ECU)

Thus the key transponder and the Power ECU are validated against Central ECU. The key transponder validation is always performed before the Power ECU validation.

2.6.1 Key validation

Central ECU communicates with the transponder key via the immobilizer transceiver. The key validation procedure in immobilizer function observes the following stages.
The validation starts with the Central ECU sending a randomly generated number called challenge message to the transponder, which runs randomly generated number through the encryption algorithm and then sends the encrypted number back to the Central ECU.

When Central ECU receives the encrypted challenge (response) from the transponder, the Central ECU checks the encrypted response. If the encrypted challenge is correct the key is considered to be validated. Otherwise, the transponder key is set to be invalid.

2.6.2 **Power ECU validation**

After and if the transponder key has been validated, the validation between the Central ECU and the Power ECU shall be initiated as follow:

1. The Central ECU requests a challenge from the Power ECU.

2. The Central ECU receives a challenge (random generated number) from the Power ECU.

3. The Central ECU encrypts the random number received from the Power ECU and sends it back to the Power ECU.

4. The Central ECU receives a response from the Power ECU which is an encrypted version of previously encrypted challenge in previous stage. Central ECU then decrypts the encrypted number and compares it to the encrypted number in the previous stage of validation above. If they both matched, Power ECU is addressed as validated. If they do not match Power ECU is considered invalidated.

To help for better visualization, comprehension and understanding of immobilizer functionality, there is a figure prepared. Figure 4 indicates the challenge-response sequences in Transponder-Central ECU and Central ECU-Power ECU validations. Observe Fig. 4.
Immobilizer checks the status of the validation of the key and Power ECU against Central ECU. If any validation step fails, a fault code shall be activated, engine start shall be prohibited. This is done by immobilizer informing the engine handling module to set the signal “Immobilize and the immobilizer lamp shall be lit”.

2.7 **Controller Area Network (CAN) bus**

Controller Area Network (CAN) bus is a single and centralized network bus that connects all of the ECUs and systems in a modern vehicle together. All of the vehicle’s data traffic is transferred on CAN bus.

CAN bus improves the efficiency of data transfer between all ECUs and systems inside a modern vehicle and also reduces the complexity of the network and connections between them while decreasing the wiring costs. Before the development of CAN bus technology, any two ECUs or systems in a vehicle needed to communicate with each other by an individual dedicated point-to-point connection between them [6].

![Figure 4. Sequence diagram of immobilizer challenge-response validations.](image-url)
Figure 5 demonstrates how a CAN network can considerably decrease the amount of wiring required in a vehicle by eliminating the old point-to-point topology in favor of a more efficient, centralized approach which CAN bus provides.

Although the pre-CAN architecture diagram places the ECU at the center of the logical network, the CAN diagram highlights the network bus itself as the focal point, eliminating point-to-point connections between devices and reducing the involvement of the ECU [6].

![Figure 5. CAN networks wiring reduction [6].](image)

What makes CAN bus different from other common network bus topologies is that data is frequently and continuously flowing on the CAN bus whether it is actually requested or not. CAN is a serial bus network for connecting intelligent devices and ECUs which has become a globally accepted standard for in-vehicle networking [6].

CAN is lightweight and robust which permits additional components and ECUs to be added easily to the CAN network without needing to modify existing components and ECUs. The CAN protocol also allows message prioritization and error checking and due to stated qualities and capabilities CAN has become the modern standard for in-vehicle networking [6].

### 2.8 Fundamental components in electrical vehicles

Before investigating and examining how current electrical vehicles (EV) immobilization systems work, it is imperative to be well familiar with functionality and characteristics of the most primary components EV exploited by immobilizers to prevent start of vehicle in case of incorrect key use. The most important components in EV that play crucial role in immobilization of EV have been introduced and defined in this section.
2.8.1 Variable frequency drive (VFD)

A variable frequency drive is a type of adjustable-speed drive used in electro-mechanical drive systems to control AC motor speed and torque by varying motor input frequency and voltage.

2.8.2 Electrical machine (Electrical motor, Induction motor)

An induction motor or asynchronous motor is an AC electric motor in which the electric current needed to produce torque is obtained by electromagnetic induction from the magnetic field of the stator winding. An induction motor can therefore be made without electrical connections to the rotor.

Applications of three phase induction motors in industries are universally extensive since they are strong, dependable and cost-effective. Induction motors are increasingly being utilized with variable-frequency drives (VFDs) in variable-speed service. VFDs offer especially important energy savings opportunities for existing and prospective induction motors.

2.8.3 Fuel cell

Fuel cells turn the chemical energy produced by electrochemical reaction between hydrogen fuel and oxygen or any other oxidizing substance into electricity, hence they are considered to be electrochemical cells.

Fuel cells need the continuous electrochemical reaction between source of hydrogen fuel and oxygen (mostly obtained from the air) in order to maintain the constant chemical reaction which in turn produces a continuous electricity supply to power up the electrical vehicle. In other words, fuel cells can constantly generate electricity as long as the hydrogen fuel and oxygen are supplied and electrochemical reaction is occurring between them.

2.8.4 Power inverter (inverter)

A power inverter or simply inverter, is an electrical component whose task is to turn direct current (DC) into alternating current (AC). The design and structure of the inverter and its circuitry specifies the particular characteristics of the power inverter in terms of input and output voltage, frequency, and overall power handling. It is important to point out that the power supply is provided by DC source, i.e., batteries or fuel cells, therefore inverter does not produce any power.
2.8.5 Transmission solenoid

A transmission solenoid or clinoid is an electro-hydraulic valve that controls fluid flow into and throughout an automatic transmission. Solenoids can be normally open or normally closed. They operate via a voltage or current supplied by the transmission computer or controller. Transmission solenoids are usually installed in a transmission valve body, transmission control unit or transmission control module.

As the vehicle goes down the road, the vehicle’s computer analyzes data being sent by vehicle speed sensors. Based on this information, the Engine Management System (Engine ECU), or the Transmission Management System (Electrical machine ECU), executes the appropriate upshift or downshift by sending a signal to one of several shift solenoids. These transmission solenoids have a spring-loaded plunger inside, which are wrapped with wire. When this coil of wire receives an electrical charge from the Engine ECU or Electrical machine ECU, it causes the plunger to open, allowing transmission fluid to flow into the valve body and pressurize the desired clutches and bands. When this happens, the transmission changes gears and the vehicle continues down the road [7].
3 Process and results

In this chapter, I have investigated and detected critical vulnerabilities and weaknesses in Scania EV/HEV immobilizer systems and I have proposed solutions to each individual vulnerability that I have discovered in order to improve the security of Scania EV/HEV immobilizer systems.

I have divided the vulnerabilities in EV/HEV immobilizer systems into three categories:

1. Immobilizer RFID chip (key transponder) vulnerabilities
2. CAN bus vulnerabilities
3. Immobilization approach vulnerabilities

In this chapter, I have examined the existing vulnerabilities in each category to discover the root cause of those vulnerabilities in order to eliminate them and improve the security in each category.

3.1 Improvement of Scania Immobilizer RFID chip

In order to investigate and realize the vulnerabilities in immobilizer RFID which allow attackers to crack and clone the right immobilizer RFID and consequently compromise the whole immobilizer system and start the vehicle, I have examined and illustrated the process of a successful attack on a very well-known and universal immobilizer RFID tag.

As the result of the investigation of this successful attack, the weaknesses and vulnerabilities in RFID leading to successful compromise of it has been achieved.

Knowing the exact weaknesses and vulnerabilities in examined RFID tag, a more secure and efficient immobilizer RFID has been proposed that does not have those vulnerabilities.

After describing the encryption bits and encryption algorithm of proposed RFID, I have provided arguments and reasonings based on credible research papers to verify and validate my RFID algorithm proposal in this thesis project.

The criteria by which I have justified my proposal are based on:

1. Investigation of known attacks on proposed immobilizer RFID encryption algorithm
2. Security measurement principles
3. Security analysis of proposed RFID encryption algorithm
4. Security comparison of proposed RFID encryption algorithm with other well-known encryption algorithms

3.1.1 Vulnerabilities in current Scania immobilizer RFID chip

In this section I have discovered security vulnerabilities in Scania immobilizer RFID chip and subsequently analyzed and examined them.

When the key transponder is inserted inside the starter lock and just before starting the vehicle, the transceiver in Scania immobilizer system transmits power to the transponder (Scania RFID chip) via electromagnetic pulse. Once powered, Scania RFID can receive and respond to commands from the transceiver, i.e., receiving challenges, reading them, calculating the encrypted response and sending the response back to the transceiver. Scania RFID chip can also execute and perform computations and calculations, including encryption operations.

Scania transceiver transmits commands (challenges) as series of amplitude-modulated (AM) bits. After each power burst (period of high amplitude signal) in an AM challenge transmission, the transceiver signal will drop drastically in amplitude for some period of time which represents the binary zero in AM signal transmission. It is the duration of this “off-time” or in other words, the duration of binary zero in AM challenge transmission that communicates and broadcasts a bit value to Scania transponder. A short off-time (zero value signal transmission) duration indicates a ‘0’ bit, while a longer off-time duration determines a ‘1’ bit. Between each bit transmission, Scania transceiver signal returns to its full amplitude (power burst) in order to create the off-time intervals and continue powering up and charging Scania RFID transponder [8].

After sending a challenge (random AM signal) to Scania transponder, Scania transceiver will transmit a short, additional power burst to Scania RFID chip (transponder) to charge the RFID chip to its maximum capacity. Once Scania RFID chip receives the AM challenge from Scania transceiver, it gets electrically charged. Scania RFID chip then uses its stored electrical charge to process the challenge sent by Scania transceiver, encrypt the challenge and sends back the encrypted challenge (response) to Scania transceiver using frequency modulated-frequency shift keying (FM-FSK) signal transmission. The response by Scania RFID chip to Scania transceiver is transmitted through 16 RF (Radio Frequency) cycles, where ‘0’ or ‘1’ is specified and indicated by transmitting RFID chip response signal at two different and distinct frequencies [8].
There are mainly two various ways and techniques by which an attacker can obtain and collect signals from Scania RFID chip and each technique or mode of attack requires to be performed in its own practical and effective physical range to result in a successful signal acquisition (signal recovery). The first mode of attack is active scanning, where the attackers bring their own transceiver within scanning range of the Scania RFID which is inside Scania key fob that the driver holds. The idea with active scanning is that, the attackers use their own programmed transceivers to charge up Scania key transponder and send a challenge to the key transponder (RFID chip) and therefore receive the response from Scania RFID chip inside Scania key fob.

Scania RFID implemented in Scania key fob is designed for short range communication to a transceiver, i.e., on the order of a few centimeters. Practically however, it is possible for the RFID chip to communicate with transceiver within a larger range that a few centimeters. Scania RFID chip have the ability to process, encrypt and transmit maximum number of eight challenges per second. In other words, Scania RFID chip can transmit two responses to two different challenges in one fourth of a second. However, one limitation with active scanning is that the transceiver needs to be as close as a few centimeters in order to be able to charge up the RFID and transmits challenges to it and receives the encrypted response from RFID. The reason for this range limitation is that Scania RFID chip is equipped with an antenna to receive challenges from transceiver and transmit responses to it and Scania RFID antenna has been designed in a way that it can communicate with transceivers and be charged up only if the transceivers are within a few centimeters distance of Scania RFID antenna, hence it is a limitation from Scania RFID chip antenna [8].

The advantage of active scanning attack is that the attackers can choose the challenges that they want to send to Scania RFID chip (key transponder) in order to acquire responses from Scania RFID chip. In principle, therefore, it would be possible for an attacker with appropriate engineering skills and abilities to build a completely self-contained cloning device of a small size and pass in close proximity to a Scania RFID (key transponder), and this device would obtain and collect two chosen challenge/response sequences and then simulate and duplicate the accurate RFID chip. Constructing such electrical equipment can only cost a few thousand kronor [8].
The other way to obtain and collect signals from Scania RFID chip is to intercept and overhear (eavesdrop) the challenges and responses broadcasted wirelessly between Scania transceiver and RFID chip. This type of attack is called passive eavesdropping attack. In this type of attacks, there is no need for attacker to be within few centimeters of Scania RFID chip to transmit challenges to Scania RFID chip and charge it up since the aim of the attack is to passively and merely listen to the challenge/response sequences that take place between Scania transceiver and RFID chip when the driver inserts the key transponder (RFID chip) inside the starter lock and turns on the Scania vehicle. Therefore, the success in eavesdropping and listening to Scania transceiver-RFID chip challenge/response sequences rely only on the ability and quality of attacker’s receiver antenna in overhearing the challenge/response sequences between Scania transceiver and RFID chip when the driver is starting Scania vehicle. It has been investigated that attackers can eavesdrop and overhear vehicles validations signals within several tens of feet distance from the transmitter at 13.56 MHz [9].

Scania RFID operates at low frequencies and it has been examined and indicated that the lower frequency signals pass through the obstacles in an easier way and this makes signal eavesdropping and overhearing more convenient for lower frequency signals. However, in order to intercept signals at lower frequencies, attackers need to have larger receiver antennas. Careful experimentations with correct and precise assessment of the degree of active scanning and passive eavesdropping suggest that the threats are well within the realm of practical execution [8].

Every immobilizer RFID chip (every transponder key) is equipped with an encryption algorithm that has an individual encryption key bits, i.e., a specific number of bits holding a particular value (zeros and ones). Using its encryption algorithm and encryption key bits Scania RFID encrypts the challenges (messages consisting number of bits) sent by transceiver to RFID and transmit them back to the transceiver.

There are two weaknesses in current Scania immobilizer RFID chip. The first vulnerability is that Scania RFID chip (transponder key) uses a relatively simple and uncomplicated encryption algorithm which makes it less difficult and time consuming for attackers to discover the encryption algorithm using reverse engineering.

After finding Scania RFID encryption algorithm, the only information the attackers need to be able to duplicate the accurate Scania RFID chip is the RFID encryption key bits. The second weakness in current Scania immobilizer RFID chip is inadequate number of encryption key bits that Scania RFID chip has.
It has been shown that having already found and cracked the RFID encryption algorithm, two challenge/response validation sequence between actual RFID chip and immobilizer transceiver is enough for attackers to discover and exhaust RFID encryption key bits in under 21 hours using a single Xilinx XC3S1000 FPGA (Field-programmable gate array) on a commercial evaluation board. However, by having 16 evaluation board and connecting all of them in parallel, it is possible to recover RFID unique encryption key bits in under an hours [8].

The recovery of RFID encryption key bits is done by scanning through all combinations of bits for all number of bits until the actual accurate encryption key bits is discovered. Hence, the more number of bits an immobilizer RFID chip holds the more complicated and time consuming it would be for the attackers to recover the RFID encryption key bits.

Having RFID encryption algorithm and encryption key bits, the attackers can duplicate the exact accurate RFID chip (transponder key) and utilize it to start and steal Scania vehicles.

Figure 6 illustrates the structure of challenge-response validation between immobilizer RFID chip (key transponder) and vehicle Security System (Central ECU) [8].

Based on the two weaknesses and vulnerabilities detected and discovered in Scania immobilizer RFID chip (transponder key), i.e., simple and uncomplicated encryption algorithm and inadequate number of encryption key bits, the solution is straightforward.
Scania current immobilizer RFID chip needs to be replaced by a stronger immobilizer RFID chip whose encryption algorithm is based on a standard, publicly scrutinized encryption algorithm with an adequate encryption key bits length, e.g., Advanced Encryption Standard (AES) encryption algorithm having 128-bit encryption key length [11].

3.1.2 AES as new proposed RFID encryption algorithm

AES, i.e., Advanced Encryption Standard is an encryption algorithm (cipher) that has been authorized and set up by U.S National Institute of Standards and Technology (NIST) since 2001 to be utilized for encryption and encoding of electronic information and data. The initial and original name for AES encryption algorithm is Rijndael.

AES encryption algorithm has the potential to be used with three different encryption key bit lengths, i.e., 128, 192 and 256 bits. Another advantage of AES encryption algorithm is that, its encryption and decryption performance is regarded to be very fast both when AES is implemented in software and hardware. AES encryption algorithm is currently being exploited worldwide. This encryption algorithm has replaced and substituted the previously selected standard encryption algorithm called DES (Data encryption standard) which was published in 1977.

Regardless of which three encryption key bit lengths are utilized in a specific AES encryption algorithms, the same encryption key is exploited for both encryption and decryption of data in that specific AES encryption algorithm. Therefore, AES encryption algorithm is categorized as a symmetric-key algorithm.

In modern cryptography (secure communication), Complex algorithms or functions are used for encryption and decryption. All these encryption algorithms (ciphers) use encryption key bits (encryption keys) of different sizes, i.e., different number of bits, for encryption and decryption. The strength of encryption algorithm depends on the algorithm and encryption key bits used [12].

In inner work of AES, encryption key is expanded into 11, 13 or 15 keys respectively for 10, 12 or 14 rounds. Then the input block is copied into an array called state array which is a 4x4 matrix. Afterwards, the state array is XOR’ed with first round key and this step is known as AddRoundKey. Finally, AES perform 10, 12 or 14 rounds of computation and calculation on state array according to encryption key size, i.e., 128, 192 or 256 bits. Each round has four different steps and last round contains three steps [13]. AES steps are:

1. Key expansion: The encryption keys for all arounds are obtained and expanded from the AES key schedule algorithm.
2. Initial round: AddRoundKey; The state array is XOR’ed with the first round key.

3. Rounds: Each round except last round performs following four steps.
   - SubBytes on state array using S-box
   - A permutation ShiftRows on state array
   - MixColumns on state array
   - AddRoundKey with state array

4. Final round: This round does not contain MixColumns and it performs following three steps.
   - SubBytes on state array using S-box
   - A permutation ShiftRows on state array
   - AddRoundKey with state array

3.1.2.1 Key expansion

When encrypting a message (data), each round consist of same sequence of operations however some parameter such as encryption key or round keys are different from each other. A Key Schedule is an algorithm that produces and creates those round keys for each round [14]. Suppose, each word length, i.e., each column of 4x4 encryption key is \( W_i = 32 \text{ bits (4 bytes)} \). Therefore, AES-128 encryption key consists of 4 words (4 columns, each column 32 bits) (4*32=128 bits) where the initial round key is the original AES-128 encryption key bits. The subsequent words will be calculated as follows:

\[ W_i = W_{i-1} \ XOR \ W_{i-4} \] for all values of \( i \) that are not multiple of 4 (starting from \( i=4 \), since \( W_0, W_1, W_2 \) and \( W_3 \) are AES default encryption key bits) [12]. For the words with indices that are a multiple of 4 (\( W_{4k} \)):

1. RotWord; Bytes of \( W_{4k-1} \) are rotated left shift.
2. SubWord \((r_{sw})\): SubBytes (S-box) function is applied to all four bytes (Diffusion).
3. The result of \((r_{sw})\) is XOR’ed with \( W_{4k-4} \) and round constant \( Rcon \), i.e., \( W_{4k} = r_{sw} \ XOR \ W_{4k-4} \ XOR \ Rcon \) [12].
3.1.2.2  **Sub bytes**

SubBytes means substitution of byte of the state array by searching in lookup table which is named substitution box or S-box. S-box is a 16x16 lookup table and it holds 256 different values. The S-box table has all possible values for 8-bit sequence that means in decimal 0 to 255. Each byte of the state array is the input of this SubBytes step and the input byte is alternated by a corresponding value. Figure 7 demonstrates S-box [12].

Each byte is mapped into a new byte in the following way. The left most 4 bits show the row and right most 4 bits indicate the column of S-box. If the input byte in S-box is b7 (in binary 10110111), then the left most 4 bits means 101 (b) illustrates the row number and 0111 (7) indicates the column number of S-box. So the output value for input b7 is a9 (in binary 10101001) [15].

![16x16 S-box lookup table](image)

**Figure 7. 16x16 S-box look up table [12].**

3.1.2.3  **Shift rows**

ShiftRows step performs shifting of bytes among the columns of a state array. The state array has 4 rows and 4 columns. This step carries out left shift of certain offset in different rows cyclically. For 128-bit and 192-bit data block, ShiftRows rules are given bellow:

- First row of state array is left untouched as it is.
- Second row of state array is moved (shifted) 1 byte in the left direction.
- Third row of state array is moved (shifted) 2 bytes in the left direction.
- Fourth row of state array is moved (shifted) 3 bytes in the left direction.

Generally, row ‘a’ is left shifted cyclically for (a-1) bytes [12]. Following figure shows how ShiftRows step of AES-128 and AES-192 operates. See Fig. 8.

![Figure 8. AES-128 and AES-192 Shift rows [12].](image)

The importance of this step is to prevent the columns being linearly dependent. In decryption, the inverse ShiftRows step performs opposite direction shifting of each of the last three rows [12].

3.1.2.4 Mix columns

MixColumns step provides diffusion in AES encryption like ShiftRows stage. Each column of state array involves in MixColumns step and produces an output column. This step takes a column of state array and performs matrices multiplication with a specified matrix and produces an output column [12].

3.1.2.5 Add round key

AddRoundKey is the first step of encryption and decryption process. It is also the last step in every round of AES encryption algorithm. In AddRoundKey step, the plaintext is XOR'ed with round key, i.e., 16-byte state array XOR’ed with 16-byte (4 words) round key and produces 16-byte (128 bit) output [12]. See Fig. 9.
3.1.3 Overview of current known attacks on AES

In this chapter, I have provided an overview of current attacks on AES encryption algorithm and I have also considered and included the impact of each attacks on the strength of the AES encryption algorithm.

3.1.3.1 Side channel attack

Side-channel attacks do not target the vulnerabilities of encryption algorithms but instead they try to exploit the information and data that leaks from the physical implementation of the encryption system. For example, in timing attacks which is one of the side channel attack types, the attacker can gather timing information from target computer. This information informs the attacker about exactly how many clock cycles the encryption process has taken. By having this information, it is possible to get the encryption key. Solution for this problem is to make all implementations of the AES run in constant time [16]. Some examples of side channel attacks are timing attacks, differential power analysis attacks, simple power analysis attacks and fault injection based attacks [17].

3.1.3.2 Timing attack

Timing attack is a side channel attack in which the attacker tries to compromise an encryption system by analyzing the time taken to execute encryption algorithms. Every logical operation in a computer takes time to execute, and the time can vary based on the input. With precise measurements of the time for each operation (encryption), an attacker can work backwards to the input. Information can leak from a system based on measurement of the time it takes to respond to certain queries. How much this information can help an attacker depends on many variables and factors such as encryption system design, the processor running the encryption system, the encryption algorithms used, combined implementation details, timing attack countermeasures, the accuracy of the timing measurements, etc. The most promising developments in timing attacks on software implementations of AES concentrates on “micro-architectural” features of the hosting platform [17].
3.1.3.3 Power analysis attack

Power analysis attacks take advantage of many of the same vulnerabilities and weaknesses with AES implementations as timing attacks. Power consumption profiles can reveal secret encryption key information leaked by micro-architectural mechanisms [17]. Military encryption systems usually apply and use physical intrusion protection mechanisms. Therefore, one might assume that this would make them secure against power analysis attacks. However, poorly designed equipment may permit other parameters and factors that correlate with current draw to be monitored remotely (e.g. electromagnetic leakage or transmission power). An attacker can also access the power consumption profile of a target encryption system by inserting a monitoring device secretly during the design phase or later in an unprotected area of the equipment (e.g. within the battery pack) [17].

3.1.3.4 Fault injection analysis attack

Although AES has proven to be sensitive to fault analysis, an attacker must be in physical possession of the cryptosystem to carry out and perform this attack and may even require access to the actual encrypting device [18]. Moreover, the attack requires utilization of a “fault model” of the device and a means to reliably inject faults without permanently damaging the unit under attack. The fault model must be available before an attack is planned and can need detailed knowledge of the design and structure of the system. Even though fault injection analysis doesn’t currently pose a practical threat to military communications applications, research in this area is brisk and practical applications have already appeared [17].

In [19], a predictable fault injection is illustrated by under-powering an AES-base smart card to induce and inject time violations. This work indicated that faults can be induced reliably according to an AES fault model and, more importantly, without permanently damaging the unit under attack.
3.1.3.5 Related-key and distinguishing attack

A related-key attack is a version of a chosen plaintext differential attack. The attacker selects multiple pairs of plaintexts, where the difference between the plaintexts in each pair is determined. Using the encryption algorithm as a black box oracle, the attacker encrypts each plaintext with two keys, where the difference between the keys is determined (however the keys themselves are unknown); these are the "related" keys for which this attack is named. From the information obtained, the attacker recovers the unknown keys [17]. A cryptographic hash function is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash) and is designed to be a one-way function, i.e., a function which is impractical to invert. Although related key attacks are improbable to compromise AES encryption algorithm, related key attacks might succeed when an encryption algorithm is used as part of a cryptographic hash function. A successful related-key attack may then compromise and break the hash function [17].

A known-key distinguishing attack is an attack model against symmetric encryption algorithms, i.e., encryption algorithms with the same encryption key bits for encryption and decryption process. In such attacks, attacker who knows the encryption key can find a structural property in cipher, where the transformation from plaintext to encrypted text is not random. There is no trivial formal definition for what such a transformation may be. These attacks do not directly compromise the confidentiality of encryption algorithms, because in a classical scenario, the encryption key is unknown to the attacker. However, they are known to be applicable in some situations where encryption algorithms are converted to hash functions [17]. Gilbert and Peyrin have issued and released a known-key distinguishing attack which compromise and break the 8-round version of AES-128 [14]. Nevertheless, 128-bit AES exercises 10 rounds, so this attack will not be effective and successful against full AES-128, however it can be practical and break and compromise a nearly-full-strength variant of AES [17].

3.1.3.6 Linear and differential attacks

Linear attack exercises linear relationships that exist between inputs and outputs of an encryption algorithm. Linear combinations of plaintext patterns and linear combinations of encrypted text patterns are compared to linear combinations of encryption key bits. The goal is to discover a relationship that is valid either considerably more or less than 50% of the time. This will form a "biased" approximation which can then be utilized to determine encryption key bits [17].
Differential attack uses relationships that exist between differences in the input and output of an encryption algorithm [20]. In the case of an encryption algorithm, plaintext patterns with specified differences are examined. The objective is to discover "characteristics". Characteristics are particular differences in pairs of plaintext patterns that, for a given encryption key, have a high probability of causing specific differences in the encrypted text pairs [17].

A differential attack would consist of applying pairs of plaintext with determined differences, observing the differences in the encrypted text pairs and giving probabilities to different candidate subkeys. The probabilities will be based on the attacker’s knowledge of the encryption algorithm's characteristics. Enough trials are performed such that the accurate encryption key can be determined [17].

3.1.3.7 **Algebraic attack**

An algebraic attack is a method of attack against an encryption algorithm. It involves:

- expressing the encryption algorithm operations as a system of equations
- replacing some of the variables with known data
- solving the equations for the encryption key

What makes this type of attacks infeasible against AES encryption algorithm is a combination of considerable number of equations and nonlinearity in the relations involved [17]. In any algebra, solving a system of linear equations is nearly straightforward provided that there are more equations than variables. Nevertheless, solving nonlinear systems of equations is much harder. Encryption algorithm designers therefore attempt to make their encryption algorithm highly nonlinear [21].

One technique for adding nonlinearity is to combine operations from different algebraic systems, for example using both arithmetic and logical operations within the encryption algorithm so it cannot easily be described with linear equations in either normal or Boolean algebra. Another alternative is to use S-boxes, which are lookup tables containing nonlinear data [21]. An algebraic attack is similar to a brute force attack or a dictionary attack in a sense that it can, in theory, break any encryption algorithm but in practice and reality it is significantly impractical against any reasonable encryption algorithm [21].
3.1.3.8 SAT solver hybrid attack

An encryption algorithm such as AES can be formulated as a very complicated Boolean expression having a number of variables. These variables are the plaintext input bits, the encryption key bits, and the encrypted text output bits. The Boolean expression is considered to be true if and only if the encrypted text bits are equal to the encryption of the plaintext bits using the encryption key bits [17]. One way to attack an encryption algorithm is to set the plaintext and encrypted text variables in the Boolean expression to the values corresponding to a known plaintext-encrypted text pair, and then to find values for the encryption key variables that make the Boolean expression true. This is an instance of the Boolean satisfiability (SAT) problem. A computer program that automatically finds the solution to a SAT problem is called and known as a SAT solver [17].

A more effective strategy is to integrate a SAT solver with another technique to result in a hybrid attack. A research paper reported an integrated side-channel and SAT-solver attack on DES, 3DES, and AES [22]. It is demonstrated that if a side-channel attack can find and recover values for the input and output bits of any one of the ten rounds of AES, a SAT solver can then recover the full 128-bit encryption key. Nonetheless, according to the research paper, the researchers did not actually perform the side-channel attack, nor did they evaluate the difficulty of finding all the inputs and outputs of a round using side-channel techniques, so whether this hybrid attack would work in practice and reality is still unknown [17].

3.1.3.9 Meet in the middle attack

In the meet-in-the-middle (MITM) attack the attacker requires pairs of plaintext and its corresponding encrypted text. The attacker divides the encryption algorithm into two subciphers. One of the subciphers encrypts the plaintext and the other decrypts the corresponding encrypted text. The idea is to make these subciphers “meet in the middle” by finding an accurate key-pair. See Fig. 10. This technique is ineffective and unsuccessful against AES because it has a nonlinear key schedule [23].

![Figure 10. Meet in the middle (MITM) attack [14].]
3.1.4 AES security measurement criteria

Security is the fundamental and key term of Advanced Encryption Standard. Security of AES encryption algorithm means how resistant this encryption algorithm is against active or passive attack. Security of AES-128 is measured and assessed based on three criteria [12].

- Time security
- Avalanche effect
- Strict Avalanche Criterion

3.1.4.1 Time security

It illustrates the amount of resistance of an encryption algorithm with different encryption key sizes against brute force attack and the time it takes to effectively and successfully execute a brute force attack. Brute force attack implies thoroughly checking and scanning all probable encryption key bits combinations until the accurate encryption key bits is recovered. From Table 1, it can be observed that for 128-bit key, brute force attack must check maximum $3.403 \times 10^{38}$ key combinations [12].

<table>
<thead>
<tr>
<th>Key size (bits)</th>
<th>Possible Combinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>$3.403 \times 10^{38}$</td>
</tr>
<tr>
<td>192</td>
<td>$6.278 \times 10^{57}$</td>
</tr>
<tr>
<td>256</td>
<td>$1.158 \times 10^{77}$</td>
</tr>
</tbody>
</table>

Now the brute force attacking time based on processing speed of latest super computers can be measured and evaluated. As shown in Table 2, even with a modern super-fast computer, it would take billions of years to crack and recover the 128-bit AES encryption key using brute force attack [12].

<table>
<thead>
<tr>
<th>Key size (bits)</th>
<th>Years needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>$3.19 \times 10^{14}$ years</td>
</tr>
<tr>
<td>192</td>
<td>$5.88 \times 10^{33}$ years</td>
</tr>
<tr>
<td>256</td>
<td>$1.0844 \times 10^{53}$ years</td>
</tr>
</tbody>
</table>
3.1.4.2 Avalanche effect

Avalanche effect is a property that is very crucial and critical for encryption algorithms. An encryption algorithms is considered to have Avalanche property if for flipping or changing just a single bit in plaintext or in encryption key bits, the encrypted text changes considerably (about half of the encrypted bits). If an encryption algorithm does not show acceptable degree of Avalanche effect, then the attackers can recover the plaintext by analyzing the encrypted text and therefore break the encryption algorithm [12].

3.1.4.3 Strict Avalanche Criterion

Strict Avalanche Criterion is an important property for a secure and strong encryption algorithm. In encryption algorithms, Strict Avalanche Criterion (SAC) is considered to be maintained by algorithms if, one bit complemented either in encryption key or in plaintext brings about a significant change in encrypted text, i.e., about one half of the encrypted text. This SAC completely depends on encryption algorithms confusion and diffusion characteristics. In AES, SubBytes, ShiftRows and MixColumns steps provide a substantial degree of confusion and diffusion [12].

3.1.5 Security analysis of proposed RFID encryption algorithm

There is no way to provide absolutely perfect data security but it is possible to ensure that it is computationally impossible to decrypt an encrypted messages without having the correct encryption key [24]. One of the problems of DES (Data Encryption Standard) as an encryption algorithm is that it only encrypts 32-bits each round although the block size (plaintext size) is 64-bits. AES encrypts the entire 128-bit block of data (plaintext) in every round which is why AES encryption algorithm performs lower number of rounds compared to DES which has 16 rounds [25].

AES-128 encryption algorithm utilizes 128-bit block of plaintext and 128-bit encryption key. With the fastest super computer of this age it will take $3.19 \times 10^{14}$ years to recover the correct encryption key combination by executing brute force attack. So it is impractical and infeasible not only for an attacker but also for a generation to recover and crack an encryption key by checking all encryption key bits combinations [26]. In this section diverse experiment cases are considered to evaluate the security of my proposed RFID encryption algorithm, i.e., AES, based on encryption algorithms security measurement criteria (Avalanche effect and Strict Avalanche Criterion) mentioned in 3.1.4 section.
Case 1: The plaintext changes and differs by 1 bit in every experiment but the encryption key is always constant. Encryption key (16 byte): 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f. Table 3, indicates the Avalanche effect result for case 1.

Table 3. Avalanche effect for fixed key but variable plain text on AES-128 bit [12].

<table>
<thead>
<tr>
<th>No</th>
<th>Plain text (Alphabet)</th>
<th>Cipher text (Hex.)</th>
<th>Bit variance</th>
<th>Avalanche (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ABCDEFGHIJKLmnop</td>
<td>9CDD85DE85B48BED892F02D8A5CBDAcB</td>
<td>63/128</td>
<td>49.22</td>
</tr>
<tr>
<td>2</td>
<td>ABCDEFGHIJKLmnoq</td>
<td>ACE7083761553A6B3A97BCB1740B176A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ABCDEFGHIJKLmnoB</td>
<td>0026D76C52B61B9A76445035FD4D342B</td>
<td>69/128</td>
<td>53.91</td>
</tr>
<tr>
<td>4</td>
<td>ABCDEFGHIJKLmnoC</td>
<td>E930AC10030FA5DB617AF6DFA741ADE4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>ABCDEFGHIJKLmnoS</td>
<td>DA5D2C1E67818646AC2D955E0FAB4C3B</td>
<td>61/128</td>
<td>47.66</td>
</tr>
<tr>
<td>6</td>
<td>ABCDEFGHIJKLmnoR</td>
<td>7A6EEC02FCADA2FB323D67247.66B3D2EF396</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Case 2: The plaintext always remains constant but the encryption key will change by 1 bit in every experiment. Input plaintext (16 bytes): ABCDEFGHIJKLmnop.

Table 4, demonstrates the Avalanche effect for case 2.

Table 4. Avalanche effect for fixed plaintext but variable key on AES-128 [12].

<table>
<thead>
<tr>
<th>No</th>
<th>Key</th>
<th>Cipher text (Hex.)</th>
<th>Bit variance</th>
<th>Avalanche (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f</td>
<td>6DDBB27CAB5B875FEEB3B132AF00113</td>
<td>68/128</td>
<td>53.13</td>
</tr>
</tbody>
</table>
From Table 3 and 4, it can be realized that AES-128 maintains an acceptable degree of confusion and diffusion property and thus a proper degree of bit variance and Avalanche effect [12].

AES-128 also maintains a satisfactory degree of Strict Avalanche Criterion. Table 5, illustrates that among 8112 encryption samples, AES encryption algorithm manages to maintain SAC for 4322 times in average. It means for flipping 1 bit from zero to one or one to zero in input plaintext, AES encryption algorithm results in more or equal than 50% change in encrypted text in 4322 times [12].

Table 5. SAC for AES-128 [12].

<table>
<thead>
<tr>
<th>Case</th>
<th>Number of Samples</th>
<th>Number of Samples satisfy SAC</th>
<th>Number of Samples not satisfy SAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 03</td>
<td>A65749D1BF1444BCEDB68 6837 C18E237</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 00</td>
<td>0054396C46CC2330B334959 5A6529FCB</td>
<td>64/128 50.00</td>
</tr>
<tr>
<td>4</td>
<td>00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 01</td>
<td>6DDDBB27CAB5B875FEEB 3B132AF00113</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 06</td>
<td>D8B5B0EBF6787F53163B64 144393DEC8</td>
<td>66/128 51.56</td>
</tr>
<tr>
<td>6</td>
<td>00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 07</td>
<td>7185F7D1451E8EE0530E676 A2F2D8560</td>
<td></td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Case 1</th>
<th>8112</th>
<th>4321</th>
<th>3791</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 2</td>
<td>8112</td>
<td>4306</td>
<td>3806</td>
</tr>
<tr>
<td>Case 3</td>
<td>8112</td>
<td>4312</td>
<td>3800</td>
</tr>
<tr>
<td>Case 4</td>
<td>8112</td>
<td>4333</td>
<td>3779</td>
</tr>
<tr>
<td>Case 5</td>
<td>8112</td>
<td>4342</td>
<td>3770</td>
</tr>
<tr>
<td>Average</td>
<td>8112</td>
<td>4322</td>
<td>3790</td>
</tr>
</tbody>
</table>

3.1.6 Security comparison of AES, DES, RSA encryption algorithms

DES is an encryption algorithm for the encryption of electronic data. Although DES encryption algorithm is considered to be insecure, it was substantially effective and influential in the development of modern encryption systems.

DES encryption algorithm is unsafe and unreliable and this is primarily due to the 56-bit encryption key size which is considered to be too small and inadequate. The original DES encryption key size of 56 bits was generally adequate and enough when DES encryption algorithm was designed, but the availability of increasing computational power made brute-force attacks practical and possible among other types of attacks against encryption algorithms. Furthermore, DES has been disclaimed and withdrawn as an encryption algorithm standard by the National Institute of Standards and Technology (NIST) and therefore AES encryption algorithm has been selected by NIST to replace and substitute DES encryption algorithm as a standard encryption algorithm.

RSA is one of the first public-key encryption algorithms and is widely utilized for secure data transmission. In public-key encryption algorithms, the encryption key is public and it differs from the decryption key which is kept secret (private). RSA encryption algorithm is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem".

AES encryption algorithm is not only utilized for its strong security but also for its high speed. The performances of both hardware and software implementations of AES encryption algorithm are faster than DES and RSA. AES can also be implemented on various platforms particularly in small devices and it has carefully been tested for numerous security applications [27].

In Table 6, a comparative study between AES, DES and RSA has been presented with respect to sixteen different factors, See Table 6.
<table>
<thead>
<tr>
<th>Factors</th>
<th>AES</th>
<th>DES</th>
<th>RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developed</td>
<td>2000</td>
<td>1977</td>
<td>1978</td>
</tr>
<tr>
<td>Encryption key bit length</td>
<td>128, 192, 256</td>
<td>56</td>
<td>&gt;1024</td>
</tr>
<tr>
<td>Plain text bit length (Block size)</td>
<td>128</td>
<td>64</td>
<td>≥ 512</td>
</tr>
<tr>
<td>Ciphering (encryption) &amp; deciphering (decryption) key</td>
<td>Same (Symmetric-key algorithm)</td>
<td>Same (Symmetric-key algorithm)</td>
<td>Different (Asymmetric-key algorithm)</td>
</tr>
<tr>
<td>Scalability</td>
<td>Not Scalable</td>
<td>It is scalable algorithm due to varying the key size and block size</td>
<td>Not Scalable</td>
</tr>
<tr>
<td>Encryption</td>
<td>Faster</td>
<td>Moderate</td>
<td>Slower</td>
</tr>
<tr>
<td>Decryption</td>
<td>Faster</td>
<td>Moderate</td>
<td>Slower</td>
</tr>
<tr>
<td>Power consumption</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Security</td>
<td>Excellent</td>
<td>Not enough</td>
<td>Least secure</td>
</tr>
<tr>
<td>Deposit of algorithm keys</td>
<td>Needed</td>
<td>Needed</td>
<td>Needed</td>
</tr>
<tr>
<td>Rounds</td>
<td>10/12/14</td>
<td>16</td>
<td>1</td>
</tr>
<tr>
<td>Simulation speed</td>
<td>Fast</td>
<td>Fast</td>
<td>Fast</td>
</tr>
<tr>
<td>HW &amp; SW Implementation</td>
<td>Faster</td>
<td>Better in HW than SW</td>
<td>Not efficient</td>
</tr>
<tr>
<td>Ciphering (encryption) &amp; deciphering (decryption) algorithm</td>
<td>Different</td>
<td>Different</td>
<td>Same</td>
</tr>
</tbody>
</table>
Four text files of different sizes of 153 KB, 196 KB, 312 KB and 868 KB have been utilized to conduct four experiments, where a comparison of three encryption algorithms AES, DES and RSA has been carried out. Performances of encryption algorithms have been evaluated and assessed based on following factors.

1. Encryption Time
2. Decryption Time

The encryption time is considered the time that an encryption algorithm takes to produce an encrypted text from a plain text. Encryption time is computed as the total plaintext in bytes encrypted divided by the encryption time. Decryption time holds the opposite definition of encryption time. Comparisons analyses of the results of the selected different encryption algorithms have been performed [28]. Experimental results for encryption algorithms AES, DES and RSA are shown in Table 7, and their corresponding graphs are demonstrated in Fig. 11 and Fig. 12.

<table>
<thead>
<tr>
<th>Size Number</th>
<th>Algorithm</th>
<th>Packet Size (KB)</th>
<th>Encryption Time (Sec)</th>
<th>Decryption Time (Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AES</td>
<td>153</td>
<td>1.6</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>DES</td>
<td></td>
<td>3.0</td>
<td>1.1</td>
</tr>
<tr>
<td></td>
<td>RSA</td>
<td></td>
<td>7.3</td>
<td>4.9</td>
</tr>
<tr>
<td>2</td>
<td>AES</td>
<td>196</td>
<td>1.7</td>
<td>1.4</td>
</tr>
<tr>
<td></td>
<td>DES</td>
<td></td>
<td>2.0</td>
<td>1.24</td>
</tr>
<tr>
<td></td>
<td>RSA</td>
<td></td>
<td>8.5</td>
<td>5.9</td>
</tr>
<tr>
<td>3</td>
<td>AES</td>
<td>312</td>
<td>1.8</td>
<td>1.6</td>
</tr>
<tr>
<td></td>
<td>DES</td>
<td></td>
<td>3.0</td>
<td>1.3</td>
</tr>
<tr>
<td></td>
<td>RSA</td>
<td></td>
<td>7.8</td>
<td>5.1</td>
</tr>
<tr>
<td>4</td>
<td>AES</td>
<td>868</td>
<td>2.0</td>
<td>1.8</td>
</tr>
<tr>
<td></td>
<td>DES</td>
<td></td>
<td>4.0</td>
<td>1.2</td>
</tr>
</tbody>
</table>
Figure 11. Comparison of encryption time between AES, DES and RSA [27].

Figure 12. Comparison of decryption time between AES, DES and RSA [27].
By analyzing Table 7, Fig. 11 and Fig. 12 which show time taken for encryption and decryption on various sizes of files by three algorithms, it can be observed that RSA algorithm takes much longer encryption and decryption time compared to time taken by AES and DES algorithms. Furthermore, AES and DES algorithms indicate very minor and insignificant differences in time taken for decryption process.

Based on the text files utilized and the experimental results illustrated, it can be realized that AES encryption algorithm spends the least encryption time and RSA takes the longest encryption time. Moreover, it is inferred that decryption time of AES algorithm is very close to DES and significantly better than RSA algorithm. Therefore, from the simulation results, it is evaluated that AES algorithm is superior than DES and RSA algorithm in terms of encryption and decryption time [27].

3.2 CAN bus vulnerabilities

The CAN bus is approximately a 30-year old architecture that was designed and established for various legitimate reasons, however security certainly was not one of them. The CAN architecture was developed to be lightweight and robust, therefore CAN accomplishes those qualities very well. Nevertheless, CAN bus has several vulnerabilities that are intrinsic and internal in its design. In the following section, the most critical CAN vulnerabilities have been discussed.

3.2.1 Lack of segmentation and boundary defense

Network segmentation is an essential part of secure system design. If a network is not segmented, a trivial vulnerability in a non-sensitive system component or ECU can be exercised and exploited to grant access to the rest of the network, including its most crucial and sensitive parts. Protecting each segment with a proxy and a firewall will significantly decrease an intruder’s access to the other parts of the network. Unfortunately, the CAN bus architecture fails to address this vital network security feature [29].

3.2.2 Lack of device authentication

Another way in which the CAN bus is inherently and internally vulnerable and exposed to attackers is the lack of device authentication on the network. The Controller Area Network, as the name implies, is a network through which various controllers, components and ECUs are connected and communicate. Each controller performs a different function. Some controllers are utilized to transmit data onto the bus. Once messages and data are transmitted onto the bus, they become available to all other vehicular components and ECUs on the CAN bus whether they need that information or not. Other controllers on the CAN bus continuously and frequently listen for specific messages.
CAN bus architecture, under normal situations and conditions, operates very well. Nonetheless, the system does nothing to prevent unauthorized and illegitimate devices and controllers from joining the CAN bus and transferring messages out to any listening controllers or listening to transmitted messages sent by other controllers.

CAN bus manipulation and exploit can be done by listening passively to the CAN bus broadcasted messages and record the different messages for various vehicle functions which is trivial in its level of difficulty. Once an attacker understands the valid and legitimate message format for the given vehicle, he can design and create his own CAN messages to manipulate the vehicle. There are many third-party solutions available today which enable even an amateur attacker to sniff traffic on the CAN bus. An example of such product is CANdo from Netronics [30].

### 3.2.3 Unencrypted traffic

Another dangerous weakness and defect in the design of the CAN bus is the complete lack of encryption. CAN is an unencrypted network bus by design [31]. The consequences and ramification of unencrypted CAN messages are twofold. First, a major flaw and deficiency of unencrypted CAN traffic is that it can be sniffed and listened to. With the appropriate hardware which is already available at a low price an attacker can connect to the CAN bus and passively sniff the broadcasted data and messages.

In the second stage, lack of encryption, again, allows for actual modification and manipulation of CAN messages or the injection of completely new ones. Without some form of encryption, there is no way to ensure message integrity or message validity and authenticity. Therefore, the vehicle will continue processing manipulated CAN messages as if they were legitimate. Once an attacker is inside the CAN bus network, one of the best strategies to prevent him from sniffing or manipulating the messages and data is with data encryption [31].
3.3 Solutions to CAN bus vulnerabilities

3.3.1 Encryption

A major limitation facing CAN encryption is the CAN protocol’s maximum message field size of 8 bytes. It is widely accepted that a strong encryption algorithm needs a 128-bit or 256-bit block size, i.e., a strong encryption algorithm requires at least 128-bit plain text to encrypt. One promising encryption solution for encryption of CAN messages is SecureCAN from Trillium which is a small Japanese company. The Trillium encryption system found in SecureCAN utilizes three different algorithms. A message first undergoes substitution, the resulting encrypted text then passes through a transposition algorithm and eventually, time-multiplexing is applied before the encrypted text is broadcasted on CAN bus [31].

Trillium claims the entire process of encryption, transmission, and decryption can be executed in less than one millisecond, which falls within the time threshold needed for real-time automotive CAN bus applications and utilities. Additionally, SecureCAN can change the encrypted text at random intervals, potentially multiple times per second, utilizing frequency channel hopping. Therefore, it will be close to impossible for attackers to intercept and manipulate CAN messages if SecureCAN encryption solution is implemented [31].

3.3.2 Device authorization

Another key element in preventing an attacker from being able to transmit harmful and malicious messages on the CAN bus is to require authentication or authorization of devices that connect to the CAN bus. To prevent unauthorized ECUs or rogue CAN controllers from transferring CAN messages, the receiving CAN controller needs to be able to validate and verify that the message comes from an authentic source.

CAN device authentication and authorization can be achieved and attained by preprogramming CAN controllers with a whitelist of CAN identifiers that represent the devices, ECUs and controllers that have been verified as eligible and harmless devices. Of course, this creates the opportunity for the attackers to fabricate and change CAN messages and make them appear as if they are being sent from one of the legitimate CAN controllers. Therefore, in order for device authorization to work efficiently and successfully, the CAN identifier field should be encrypted.
One of the solutions to encryption of identifier filed is to utilize a unique and individual encryption code saved in each of the authorized CAN bus ECUs, so that unauthorized CAN bus controller or device cannot communicate with the authorized devices. This is problematic because any modification of identifier field of CAN data frame will result in the recipient CAN controllers and ECUs ignoring the message, as they no longer recognize and identify the source. Therefore, encryption of the CAN identifier needs using of a hardware-based encryption solution placed between the sending and receiving CAN controllers [32].

Richards’ solution demands use of a pair of KEELOQ peripheral devices to serves as encryption and decryption devices between transmitting and receiving CAN ECUs. KEELOQ is a proprietary hardware-based encryption algorithm that is owned by Microchip Technology Incorporated. There are some potential downsides to this solution, as it would add additional processing time to CAN message transmissions, further expense and cost for automakers, and more weight to the vehicle. Therefore, the implementation and execution of any security solution will always come with some trade-offs [32].

3.3.3 Defense in depth

There is not a single solution to the security vulnerabilities and weaknesses in automotive systems. What is needed is an extensive approach providing multiple layers of security, also known as “defense in depth” [33]. A comprehensive approach to securing a vehicle’s systems should include, at the very least, better network segmentation, locking down of external interfaces, controller and ECU authentication and authorization, and data encryption.

The diagram shown below in Fig. 13 offers a conceptual model for applying a defense-in-depth approach to secure and protect CAN communications. The diagram depicts and illustrates the flow of data through multiple layers of security, as a CAN controller (ECU) prepares a CAN packet, i.e., CAN message for transmission onto the CAN bus. See Fig. 13.
Figure 13. Defense in depth approach to secure CAN communication [33].

The above model has several layers of security so that CAN data would still be protected if an attacker were somehow able to compromise and exploit one of the security controls. Through this defense-in-depth approach, the CAN bus is protected and secured against even the most determined attacker [33]. Alternatively, Ethernet has shown significant capacity as one possible solution to replacing CAN with more fundamentally secure infrastructure [34].
3.4 Improvement of Scania immobilization procedure

Immobilization approach is a method or mechanism by which the start of vehicle is prevented if any of validation processes between specified ECUs in immobilizer system fails. Therefore, the vulnerabilities in immobilization approach enables attackers to start the vehicle despite of not possessing the right ignition key (RFID chip), by bypassing all validation rounds in the immobilizer system.

It is important to notice that CAN bus vulnerabilities depicted earlier in previous section, sets up and facilitates this type of security attack on immobilizer.

In this section, I have first investigated and discovered current Scania EV/HEV immobilization approaches by reading documents on different security layers of EV/HEV immobilizer systems and illustrated the advantages and disadvantages of the immobilization approach that current Scania EV/HEV use.

In the final step, I have proposed two unique and original immobilization approaches and concepts for both Scania EV and HEV which not only eliminate current vulnerabilities in immobilization approach of EV/HEV but also eliminate the chances of bypassing the validation stages to bypass the immobilizer system and start the vehicle.

3.4.1 Current immobilization approach in EV

EV possess electrical machines (electrical motors) rather than ICE to move the EV. Furthermore, instead of exploiting fuel, EV run on batteries or fuel cells to supply electrical power to electrical machine. The DC power supplied for inverter can be derived from a batteries or fuel cells. Electrical machine ECU is used to adjust the final AC output voltage and frequency of the inverter which will ultimately determine the torque and speed of the electrical motor operating under its mechanical load.

The main stages to immobilization of modern EV is the same as in conventional vehicles. The common main stages are as following.

1. Key validation (Validation between key transponder and Central ECU)
2. Power ECU validation (Validation between Central ECU and Electrical machine ECU)
However, in electrical vehicles, Electrical machine ECU is validated against Central ECU while in conventional vehicles it is Engine ECU which is validated against Central ECU. If either of key validation or Electrical machine ECU validation does not happen successfully, Electrical machine ECU engages a clutch in automatic transmission to neutral gear in order to prevent the vehicle from moving even if Electrical machine ECU allows power supply to inverter and start of electrical machine. The overall schematic of ECUs in EV illustrates how different ECUs are connected when immobilizer operates. See Fig. 14.

![Figure 14. ECUs in EV and their CAN bus connections.](image)

### 3.4.2 Advantages of current EV immobilization approach

Current immobilization approach in purely electrical vehicles has following advantages.

1. Low number of validations (in terms of algorithms simplicity and process time)

2. Validations between company own developed ECUs
3.4.2.1 Low number of validation

There is only one more validation beside Transponder-Central ECU validation, which is Central ECU-Electrical machine ECU validation. The lower number of validations lead to a simpler validation programming algorithms as well as faster performance of immobilizer operation in overall. If there are excessive number of validation procedures in an immobilizer operation, the total processing time of validation stages may exceed the maximum time limit determined for immobilizer to complete its operation and hence the vehicle might not start running when cranked even though the right key is used.

3.4.2.2 Validation between company own developed ECUs

Another advantage of having Central ECU and Electrical machine ECU validating each other is that almost always both of these ECUs’ software is completely developed and programmed by manufacturers of vehicles themselves. Therefore, in case of technical difficulties, bugs and software problems, vehicle manufacturers manage to identify and resolve the issues independently. Moreover, various types of developments, modifications and upgrades can be implemented in Central ECU-Electrical machine ECU validation algorithm by vehicle manufacturers without any issues and external dependencies on product suppliers.

3.4.3 Disadvantages of current EV immobilization approach

In this section the disadvantages of current EV immobilizer are examined. After investigation and evaluation of immobilizer operation in current EV, the drawbacks of current EV immobilizers have been inferred to be as follows.

1. Inadequate number of validations (in terms of immobilizer security)

2. Risky and unreliable immobilization procedure

3.4.3.1 Inadequate number of validations

As mentioned earlier, there is only one more validation beside Transponder-Central ECU validation which is Central ECU-Electrical machine ECU validation. The less validation processes included in immobilizer operation, the lower security level an immobilizer will have. Thus, the number of validation stages in an immobilizer strategy is a trade of between system security, immobilization time and algorithm simplicity.
3.4.3.2 **Unreliable immobilization procedure**

In EV immobilizers, the immobilization is executed by Electrical machine ECU controlling the electrical charge to the transmission solenoids for engaging the required clutch in order to set the gear to neutral. Therefore, the attacker can replace Electrical machine ECU inside EV which is conveniently reachable from driver cabin with desired ECU that the attacker has programmed. Consequently, the programmed ECU sends the required electrical charge to transmission solenoids to change the clutch and gear from neutral to drive and disable the immobilizer.

Attacker can achieve this by supplying the transmission solenoids with required electrical voltage to set the desired clutches and gears. The thief needs to have acceptable knowledge of CAN network and manufacturer automatic transmission electrical structure to accomplish to disable the immobilizer by putting the gear from neutral to drive.

3.4.4 **New proposed immobilization approach for Scania EV**

My immobilizer proposal for EV eliminates the weaknesses existing in current EV immobilizers, i.e., inadequate number of validation processes within immobilizer operation and unreliable and risky immobilization procedure. Moreover, proposed immobilizer ameliorate and enhances the security level of EV immobilizers to a significantly high extent. My proposal immobilizer is achieved by:

1. Addition of one more validation round to current EV immobilizer operation
2. Alteration and modification of immobilization strategy

The additional validation would be between Electrical machine ECU and Motor Generator Unit (MGU). MGU is the ECU responsible for controlling inverter inside EV. Electrical machine ECU-MGU validation takes place after Central ECU-Electrical machine ECU validation. The concept is that given the wrong key is used, the Transponder-Central ECU validation fails. Therefore, all subsequent validation processes (Central ECU-Electrical machine ECU and Electrical machine ECU-MGU) fail as well. When Electrical machine ECU-MGU validation fails, MGU requests 0V (no electrical charge) from DC power supply (battery or fuel cells) to the input of inverter and hence there will be no AC voltage or current going to three phase electrical AC motor to make it work and run EV.
Thus, instead of Electrical machine ECU requesting transmission unit (including gearbox) to set the desired clutch to neutral gear by transmitting electrical charge to transmission solenoids, Electrical machine ECU requests MGU to supply inverter with no DC power. Otherwise, if the correct key is used, all validation processes will be successful including Electrical machine ECU-MGU. Consequently, Electrical machine ECU requests MGU to provide required DC power to the input of inverter to apply required torque and speed to the electrical motor and in turn the wheels. Following figures demonstrate the differences in validation processes between current and proposed immobilizer strategy. See Fig. 15 and Fig. 16.

Figure 15. Validation process in current EV immobilizer after Key-Central ECU validation.
3.4.5 Current immobilization approach in Scania HEV

As the name implies, hybrid electrical vehicles (HEV) exploit both ICE and electrical machine to run the vehicle. Therefore, HEV also make use of Engine ECU and Electrical machine ECU as two ECUs that control ICE and electrical machine respectively. In current HEV, the immobilization operation is executed by performing following stages.

1. Key validation (Validation between key transponder and Central ECU)

2. Power ECU validation (Validation between Central ECU and Engine ECU)

Thus, HEV immobilizer performs the same procedure as immobilizer in conventional vehicles, in other words, there is no validation process between Central ECU and Electrical machine ECU as it is in EV. The following figure demonstrates the overall schematic of ECUs in HEV and their CAN bus connections. Observe Fig. 17.
3.4.6 Disadvantages of current HEV immobilization approach

The most eminent and prominent weakness identified in current HEV immobilizers is lack of validation operation between Central ECU and Electrical machine ECU for electrical system in HEV. The immobilizer function in HEV has been designed and established in a way that when the key is inserted and toggled, there will be no validation process in electrical side of HEV for recognition of correct key utilization. In other words, if the right key is exercised to turn on the HEV, shortly after the validation procedure between Transponder-Central ECU and Central ECU-Engine ECU is done successfully, a specific CAN signal is set to “Ready” and will be sent from Central ECU to Electrical machine ECU, allowing Electrical machine ECU to request required voltage to inverter and in turn run the electrical motor if chosen by the driver. However, this particular CAN signal is set to “Not Ready” and sent to Electrical machine ECU by Central ECU if the validation between the key Transponder-Central ECU or Central ECU-Engine ECU is unsuccessful, which in turn results in declining permission to Electrical machine ECU to run inverter and electrical motor and HEV.
This introduces a weakness and flaw in HEV immobilizer which can be exploited by attacker to turn on the electrical motor and run HEV on electric mode. The attacker can achieve this by using any key that can be toggled to U15, which is the state that the key has in starter lock immediately before cranking the vehicle. After toggling the key to U15, the immobilizer blocks the fuel and starter motor circuit and Central ECU sets the specific CAN signal to “Not Ready” and sends it to Electrical machine ECU. However, since the only safety measure to immobilize the electrical part of HEV is by sending a specified CAN message set to “Not Ready” to Electrical machine ECU, the attacker can connect to the CAN bus, manipulate the CAN message to “Ready” and sends it to Electrical machine ECU, and consequently run the electrical motor and thus HEV.

3.4.7 New proposed immobilization approach for Scania HEV

My proposed immobilizer strategy for HEV applies my new immobilizer concept proposed for EV into current HEV immobilizer system. This would eliminate current HEV immobilizers most serious weakness which is lack of validation process in electrical system (electrical side) of HEV. Additionally, proposed immobilizer would considerably elevate the security of HEV immobilizers. In order to accomplish my proposed immobilizer, two validation procedures namely, Central ECU-Electrical machine ECU and Electrical machine ECU-MGU are included, implemented and executed in HEV immobilizer operation.

The concept is that if the wrong key is utilized, Transponder-Central ECU validation fails, so do Central ECU-Engine ECU, Central ECU-Electrical machine ECU and consequently Electrical machine ECU-MGU validations. This not only makes Engine ECU block fuel and starter motor to ICE, but also it deprives inverter from DC power supply so that no AC voltage or current could be produced from inverter output to run electrical motor. Therefore, neither ICE nor electrical motor can be manipulated by the attacker.

Differences in validation processes between current and proposed HEV immobilizer can be observed in Fig. 18 and Fig. 19.
Figure 18. Validation process in current HEV immobilizer after Key-Central ECU validation.
Figure 19. Validation processes in proposed HEV immobilizer after Key-Central ECU validation.
4 Discussion

In this thesis project, main focus and concentration has been placed on finding a reasonable, practical approach to efficiently increase the immobilizer security of EV/HEV and conventional vehicles. Therefore, the security of Scania vehicles immobilizers have been investigated and consequently, immobilizer security level of Scania EV/HEV and conventional vehicles have been successfully improved by my proposals from two perspectives and aspects.

1. Immobilizer RFID chip
2. Immobilization procedure

4.1 Immobilizer RFID chip

Discovering Scania RFID encryption algorithm and encryption key bits are the only elements attackers need, to duplicate Scania correct RFID and run the Scania vehicles whenever desired. In this thesis work I have discovered and illustrated Scania RFID chip vulnerabilities and weaknesses and I have also justified that it is possible for attackers with some engineering skills to crack and recover Scania RFID encryption algorithm and encryption key bits.

Replacing Scania current immobilizer RFID with proposed RFID that has AES-128 as its encryption algorithm makes it impossible for attackers to find AES-128 RFID encryption key bits even by using super-fast and modern computers and having knowledge of structure of AES encryption algorithm and having taken two challenge-response sequence from the correct AES-128 RFID, since there will be $2^{128}$ combinations of encryption bits to scan through.

However, replacing Scania current immobilizer RFID with my proposed AES-128 RFID may be problematic in two respects from a commercial point of view.

First, due to high complexity and security of AES-128 RFID encryption algorithm, the required circuitry for implementation of AES RFID will result in enhanced manufacturing expenses.

Secondly, there is the backwards compatibility issue to address. In other words, in order to replace Scania current immobilizer RFID with AES-128 RFID, overall immobilizer system architecture of Scania vehicles might be changed and modified so that AES-128 RFID is compatible with components in immobilizer system.

Nevertheless, in the long-term, the best approach for establishing an efficient and strong immobilizer system would be utilization of a solid, well-modeled encryption protocol based on industry-standard algorithms with sufficient encryption key lengths such as AES-128 encryption algorithm.
The importance of this thesis work has intensified since AES encryption algorithm has been authorized to protect and secure classified and unclassified national security systems and information. In 2003, U.S National Security Agency (NSA) took the unprecedented step of approving a public-domain encryption algorithm, AES, for classified information encryption and processing. Prior to this milestone, all encryption algorithms approved and authorized by the NSA for classified data encryption and processing were, themselves, classified and secret.

Therefore, the strength of any secure and good encryption algorithm is not enhanced by holding the design as secret. In fact, a public domain encryption standard is subject to continuous, careful and expert attacks. Any breakthroughs will most probably be available to users as well as attackers at the same time.

AES encryption algorithm has been designed to be secure and protected against differential and linear attacks, therefore any threat from these attacks is minimal. Despite impressive initial results, algebraic attacks have not made sufficient progress to be feasible. Hybrid algebraic/SAT solver attacks might yield results, however these attacks have not yet been comprehensively studied. A breakthrough is uncertain, nevertheless caution is still advised. AES encryption algorithm is vulnerable to a related key attack when utilized in a hash function structure and is not recommended for these applications. Furthermore, due to the large encryption key bits combinations and high computational complexity, the brute-force attacks are not threatening the security of AES.

Nonetheless, side channel attacks pose a very real danger and menace in the military and government communications domain. Research on side channel attacks of AES implementations has made sufficient progress to necessitate serious consideration by implementers.

The system designers should consider to control the incidental leakage of information in the physical implementation of not only the encryption system but throughout the entire equipment. For fielded systems, physical access to the equipment and its peripherals (batteries, headsets, etc.) should be observed and watched. Any of these could be exploited as a secret and covert entry point by the attacker for monitoring a range of parameters.

The next five to ten years of encryption attacks will probably not break AES encryption algorithm, however it may weaken AES security enough that a new standard encryption algorithm will have to be developed. Hence, it is not far-fetched for a new AES-2 encryption algorithm development effort to start no later than 2020.
temporary and interim solutions such as enhanced round or a multiple encryption versions of AES can also be taken into account. Besides identifying an appropriate replacement, a major challenge would be logistics. The only risk alleviation and mitigation for either of these is to plan in advance as if a breakthrough is certain and undeniable. It has been determined that research on encryption attacks is making progress against AES. Further caution is recommended since that progress is occurring in the public domain. Results show that AES encryption algorithm could be potentially vulnerable to different side channel attacks. Nevertheless, appropriate countermeasures are available which, when properly implemented, can eliminate these vulnerabilities and weaknesses at the equipment level. Other methods and techniques such as algebraic attacks, hybrid attacks, etc., are making steady progress, however no breakthroughs have been announced.

4.2 Immobilization procedure

Correct immobilization procedure is crucial if the attackers want to bypass the Key-Central ECU validation and manipulate the immobilizer system to run the EV/HEV. In HEV, this manipulation can be accomplished by sending a CAN signal to Electrical machine ECU to run the electrical motor and consequently HEV. Additionally, in EV, this system manipulation could be achieved by breaking into EV, accessing Electrical machine ECU in driver cabin conveniently and replacing it with a programmed ECU or manipulating electrical charge to be applied to transmission solenoids in order to set the desired clutch to achieve drive gear and run the vehicle.

The proposed immobilization procedure in this thesis work, eliminates aforementioned threats and manipulation opportunities by immobilizing EV/HEV through MGU rather than transmission unit (including gear box).

In EV current immobilization procedure, if wrong key is used, Electrical machine ECU sends a signal (CAN message) engaging a clutch in automatic transmission to neutral gear in order to prevent the vehicle from moving. However, once the attacker is inside the vehicle, battery supply and Electrical machine ECU can be accessed, manipulated or replaced conveniently and CAN message could be broadcasted through vehicle internal CAN network, hence making it possible for attacker to disable the immobilizer.
However, Electrical machine ECU-MGU validation described in my proposed EV immobilizer, prevents attacker to manipulate and bypass the immobilizer even by replacing Electrical machine ECU with his/her own programmed ECU and sending engineered CAN messages to set the gear to drive mode or manipulating battery supply. Since as long as the Electrical machine ECU-MGU validation fails MGU makes sure that no DC power is supplied into inverter’s input to run the electrical machine.

In HEV, the proposed immobilizer would implement the same immobilization procedure as proposed in EV, hence the attacker cannot manipulate the CAN signal to Electrical machine ECU in order to run the electrical motor and HEV because there will be Central ECU-Electrical machine ECU and Electrical machine ECU-MGU validations involved.

Therefore, the only option to steal HEV/EV and run away with it is to break into the vehicle and replace MGU and inverter with the attacker’s new programmed ECU and inverter or finding the correct individual 128-bit encryption bits of particular HEV/EV RFID chip. In both cases, the attacks would be highly far-fetched to be feasible and they are considerably time consuming.

Nevertheless, there is always a tradeoff between security level and time, cost and system complexity. Each validation process adds its own validation time to the total immobilizer operational time. Although in my proposed immobilization procedures, the validations added will not cause immobilizer total operational time to exceed its allowed time constraints, it should be noted to take the operating time of immobilizer system into account when increasing validation rounds and security layers. Moreover, each of additional validation processes require their own separate programming software, hence the complexity of the immobilizer software increases.

The only drawback to my proposed immobilization procedures is that, the required software for Electrical machine ECU-MGU validation developed by Scania needs to be transferred to the supplier of MGU to be implemented in their MGU products. Therefore, Electrical machine ECU-MGU validation algorithm causes Scania to have some dependencies on supplier of MGU.

Therefore, in case of software changes such as developments, upgrades, bug fixes and maintenance in the validation process between Electrical machine ECU and MGU, the external supplier also needs to modify the program written for their MGU products to adapt to software changes done in Scania.
5 Conclusions

The vulnerabilities and weaknesses I have demonstrated in Scania current immobilizer RFID are ultimately due to simple encryption algorithm and more importantly inadequate encryption key bits that Scania current RFID has.

It is illustrated from this thesis work that the most important factors for determining the security level of an RFID encryption algorithm chip are the complexity of the encryption algorithm itself and encryption key bit length used by that encryption algorithm. Thus, RFID encryption algorithms are considered to be strongest and most secure, when they employ and use more complicated encryption algorithms with adequate encryption key bit length which have been acknowledged as encryption algorithm standards by certified industry security authorities.

It is concluded that replacing Scania current RFID chip with AES-128 RFID chip, makes it impossible for attackers to find the encryption key bits even by using super-fast and modern computers, having knowledge of structure of AES-128 encryption algorithm and acquiring two challenge-response messages from the actual correct RFID chip, since there will be $2^{128}$ combination of encryption key bits to scan through in order to recover the correct encryption key bits. Impossibility of finding AES-128 RFID encryption key bits makes it impractical to duplicate individual vehicles correct transponder key, i.e., RFID and compromise the immobilizer and vehicle.

It is also illustrated in this thesis report that while there are some theoretical attacks against AES encryption algorithm, they are all infeasible to execute. Even though the computing and calculation power of computers doubles every one and half years it would still take decades before AES encryption algorithm becomes computationally insecure. There are no considerable security threats against AES encryption algorithm but it is possible that a poor and deficient implementation of AES encryption algorithm may allow side channel attacks. Thus, it is very important that software developers take these types of security attacks into account when implementing AES encryption systems.

In this thesis project, I have studied and investigated AES encryption algorithm and its performance, analyzed its security in terms of time security, Avalanche effect, and Strict Avalanche Criterion (SAC) and therefore concluded that not only AES-128 encryption algorithm has shortest encryption and decryption time among well-known encryption algorithms such as DES and RSA but also it is one of the most secured encryption algorithms at present time and it is secure and safe enough for all data security needs.
This thesis project also indicates and elaborates that a major obstacle to the development of secure automobiles is the archaic CAN bus technology that lies at the core of almost every modern vehicle. Because of the significant limitations of CAN, automakers will be forced to implement “Band-Aid” fixes for CAN until a fundamental reconstruction and overhaul of vehicle networking architecture occurs. Ideally, security should be designed and implemented into vehicle systems from the ground up. Security should never be considered as an afterthought, nor should security features and measures be applied reactively. Ethernet has shown promise as one possible solution to replacing CAN with more fundamentally secure infrastructure.

It is concluded from this thesis work that insufficient number of validation processes as well as insecure and unreliable immobilization procedures have been analyzed to be the downsides and weaknesses of current EV immobilizers. Stated weaknesses have been compensated for and turned into strength in my proposed EV immobilization procedure in this thesis work by introducing appropriate validation processes.

Another conclusion can be drawn by my inspection and investigation of current HEV immobilizers that lack of validation process for immobilization of electrical part of HEV is current HEV immobilizers main and most critical disadvantage. Mentioned HEV weakness can be ameliorated and improved by integrating my proposed EV immobilization procedure into HEV immobilizer system.

The only downside to my proposed immobilization procedures can be counted to be sharing part of Electrical machine ECU-MGU validation algorithm with MGU supplier to be implemented in their MGU products when produced.

Nevertheless, as the result of this thesis project my proposed RFID (AES-128 encryption algorithm) and immobilization procedures will be implemented in Scania vehicles in near future and will increase the security of Scania immobilizers significantly.

Finally, it can be concluded that there is always a tradeoff between immobilizer security level and immobilizer operational time, cost and system complexity (concerning hardware and software). More secure immobilizers call for more sophisticated immobilizer algorithms and structures, hence necessitating more cost and immobilizer process (operation) time. Following figure illustrates the tradeoff relation between security level, cost, operational time and complexity of an immobilizer. See Fig. 20.
There are various encryption algorithms and immobilization procedures available nowadays and they continue to improve and develop with time. Choice of immobilizers however, depends on the applications and requirements those applications need to fulfill.

Information security and similar field of studies continue to progress and advance. There will be more secure and faster immobilizer systems but one should consider how cost efficient an immobilizer is comparing to the overall value of objects protected by it. Following figure depicts an example of security design criteria of an immobilizer. See Fig. 21.
It can be realized from Fig. 21, the overlapping area by 3 primitive circles illustrates a security system requiring a pin code, a physical key and a biometric information to grant access to the desired system, hence considered a high security level system.

We can already observe smart phones with finger print security, thus it is not unreasonable in any case to predict that moving towards more advanced technologies and going through severe economic and financial crisis will call for significantly stronger security systems in future to assure the security and safety of invaluable and priceless materials and information.

Finally, future works and spin-off projects could entail further investigation and research on Asymmetric encryption algorithms, cellular networks and biometric verifications as latent prospective immobilizer technologies.
References


