



Exposé

zu meiner Bachelorarbeit

„Verschlüsselung des Controller Area Network mit
kryptografischen Mitteln“

Jannis Priesnitz

Referent: Prof. Moore

Coreferent: Prof. Wiedling

3. Mai 2015

Inhaltsverzeichnis

1	Einleitung	3
1.1	Motivation	3
2	Das Unternehmen	3
2.1	Unternehmensbereiche (Divisionen)	3
2.2	Geschäftseinheit Instrumentation and HMI	4
2.3	Bereich Core Development Software	4
2.4	CDS Gruppe Flashbootloader	5
2.5	Produkte	5
2.6	Mein Tätigkeitsbereich	5
2.7	organisatorische Einbettung	6
3	Das Projekt	6
3.1	Allgemeine Beschreibung	6
3.2	Meine Aufgabe	6
3.3	Ziele	6
3.4	Eingesetzte Technologien	6
3.5	Anforderungen	7
3.6	Konzepte und Lösungsansätze	7
3.7	Aktueller Stand	7
3.8	Bewertung des Ergebnisses	7
3.9	Ausblick	7
4	Evaluation der Praxisphase	7
4.1	Das Unternehmen	7
4.2	Lessons Learned	7
4.3	Persönliche Einschätzung des Lernerfolgs	7

1 Einleitung

in meiner Praxisphase...

1.1 Motivation

In meinem Studium hatte ich die Gelegenheit einige Vorlesungen im Bereich der technischen Informatik zu Belegen, die mir durch ihre Nähe zur Hardware und Komplexität besonders gefallen haben.

2 Das Unternehmen

Die Continental Automotive AG ist ein Konzern der Automobilzuliefererbranche mit 190000 Mitarbeitern, an über 200 Standorten und 53 Ländern. Der Hauptsitz befindet sich in Hannover. Neben dem ehemaligen Kerngeschäft, der Reifenproduktion, ist Continental einer der größten Automobilzulieferer weltweit. Zu den Kunden gehören neben allen großen deutschen Automobilherstellern weltweit viele namhafte Autokonzerne.

2.1 Unternehmensbereiche (Divisionen)

Die Continental Automotive AG unterteilt sich in fünf Divisionen, die ich hier kurz vorstellen möchte.

Chassis & Safety Die Division Chassis and Safety entwickelt Fahrsicherheitssysteme, wie elektronische und hydraulische Bremssysteme, Sensorsysteme, sowie passive Sicherheitssysteme (z.B. Airbags) und Fahrassistenzsysteme (z.B. ABS)

Powertrain Die Division Powertrain beschäftigt sich mit Lösungen rund um den Antriebsstrang von Fahrzeugen. Dazu gehören Komponenten für Motoren, Getriebe und Kraftstoffversorgung, sowie mit dem Thema der Elektromobilität.

Tires Die Division Tires ist mit der Entwicklung von Reifen für PKW und LKW befasst.

ContiTech Die Division ContiTech spezialisiert sich auf Kautschuk und Kunststofftechnologie abseits der Reifen und hat zur Aufgabe Federungssysteme, Beförderungssysteme, Antriebsriemen, Membranstoffe, und außerdem Flüssigkeitstechnologien zu entwickeln.

Interior Die Division Interior, der ich während der Praxisphase angehörte, fasst sämtliche Aktivitäten die das Darstellen und Auswerten von Informationen im Fahrzeug zusammen. Dabei steht die Schnittstelle zwischen Mensch und Maschine im Vordergrund. Geschäftsbereiche der Division sind Instrumentation and Driver HMI, in dem er um die optische und grafische Aufbereitung von Informationen geht, Infotainment and Connectivity, in der Infotainmentsystem entwickelt werden, Body and Security, die sich mit Schließsystemen, sowie die Verfügbarkeit der Funktionen im Auto sicherstellt und Commercial Vehicles & Aftermarket die sich um spezifische Anforderungen im Bereich von Nutzfahrzeugen und Vertrieb kümmert.

2.2 Geschäftseinheit Instrumentation and HMI

Zentrale Aufgaben

2.3 Bereich Core Development Software

Der Geschäftsbereiche "Core Development Software (CDS)" ist die zentrale, technologische Autorität im Geschäftseinheit Instrumentation & Driver HMI. Die zentrale Aufgabe besteht darin, die technologische Führerschaft des Geschäftsbereiches durch hohe Softwarequalität weiter auszuweiten. Dies geschieht durch Entwicklung bereits bestehender und neuer Softwarekomponenten und Plattformen, Forschung an neuen Technologien, Qualitätssicherung und Support beim Kunden. Ziel ist es dem OEM eine einheitliche, sichere, fortschrittliche skalierbare Plattform nach seinen Anforderungen zur Verfügung zu stellen, sodass diese mit einheitlichen Prozessen beim Kunden weiterentwickelt werden kann. Das CDS umfasst die Technologien Grafik, HMI, Sound, Betriebssystem, Netzwerk, Treiber, Diagnose und Flash / Bootloader, der ich angehöre.

2.4 CDS Gruppe Flashbootloader

Die Flashbootloader Gruppe beschäftigt sich mit der Entwicklung eines einheitlichen plattform- und technologieunabhängigen Flashprozesses und der Bereitstellung eines einfachen Systems zum Flashen von Systemen und Anwendungen für die Anwendungsentwicklung. Außerdem wird eine End-of-Line Diagnose bereitgestellt, die eine einfache Analyse des abgeschlossenen Flashprozesses zulässt. Weiter werden Software Pakete für Speichertechnologien für andere Teams bereitgestellt.

2.5 Produkte

Wie bereits im Punkt Unternehmensbereich beschrieben, entwickelt und fertigt Continental sehr viele verschiedene Komponenten und ganze Systeme für die Automobilindustrie. Besonders möchte dabei auf die Entwicklung von Kombiinstrumenten, Head-up Displays und ähnlichen informationstechnischen Komponenten eingehen, die von der Business Unit Instrumentation & Driver HMI übernommen wird. Dies geschieht am Standort Babenhausen in Verbindung mit den Standorten Singapur, Timisoara (Rumänien) und ferner Guadalajara entwickelt und in Babenhausen gefertigt werden.

2.6 Mein Tätigkeitsbereich

Meine Praxisphase absolviere ich in der **Devision „Interior“** im **Bereich „Instrumentation & Driver HMI“**, welcher sich mit der Entwicklung von modernen Kombiinstrumenten, Head-up Displays und Steuerungseinheiten im Cockpit eines Autos beschäftigt.

Die Einheit „Core Development Software (CDS)“ entwickelt eine Basis für die Anwendungsentwicklung durch einheitliche Technologien, Standards und Lösungen, die das Durchführen von Softwareprojekt unter einheitlichen Standards und Prozessen und Plattformen unterstützt. Außerdem werden neue Technologien erforscht und bestehende verbessert.

Die Gruppe „Flash/Bootloader“ schließlich entwickelt Flashloader Systeme, die für das aufspielen und das starten des Systems verantwortlich sind, sowie Packaging- und Diagnosesysteme in Verbindung mit Flashspeichern. Ziel ist es einen einheitlichen, einfachen und sicheren Flashprozess sowohl in der Fertigung, als auch beim Endkunden zu gewährleisten und Fehlfunktionen schnell zu diagnostizieren, sowie eine lange Lebensdauer der Flashspeicherbausteine zu erreichen.

Die Continental Automotive AG entwickelt und baut am Standort Babenhause Kombiinstrumente, Head-up Displays (HUDs) und ähnliche informationstechnische Komponenten im Bereich von automotive embedded Systems für zahlreiche Automobilhersteller weltweit. Dabei wird nahezu jedes Bauteil und jede Softwarekomponente selbst entwickelt und produziert.

2.7 organisatorische Einbettung

3 Das Projekt

CANKrypto blabla

3.1 Allgemeine Beschreibung

3.2 Meine Aufgabe

Meine Aufgabe ist es ein Konzept für eine **sichere Kommunikation über das Controller Area Network (CAN)** zu erstellen. Dazu soll ein bestehendes CAN-Demoprogramm umfassend umgebaut werden, kryptografische Verfahren und Parameter ausgewählt werden und diese in das CAN-Setup integriert werden. Außerdem soll die Software auf verschiedene Hardwar- und Betriebssystemen integriert und umfassende Performancetests durchgeführt werden.

3.3 Ziele

Ziel des Konzeptes ist es die Machbarkeit der sicheren Kommunikation über das CAN Protokoll zu beurteilen. Dazu sollen kryptografische Mittel nach aktuellem Stand der Technik ausgewählt und ein Vorschlag für ein Kommunikationsprotokoll

gemacht werden, das eine für die Anwendungsschicht transparente Kommunikation gewährleistet. Die gewählten Ansätze sollen in Software umgesetzt werden und hinsichtlich Performance, Speicherverbrauch und Portabilität geprüft werden.

3.4 Eingesetzte Technologien

C Visual Studio CryptoPP, CryptLib, OpenSSL

3.5 Anforderungen

3.6 Konzepte und Lösungsansätze

wurden komplett von mir entwickelt

3.7 Aktueller Stand

Prototyp Messungen

3.8 Bewertung des Ergebnisses

- Viel geschafft viel muss noch getan werden

3.9 Ausblick

Auch wenn dies ein Abschlussbericht ist, möchte ich kurz auf meine weiteren Tätigkeiten im Rahmen der noch verbleibenden Zeit in der Praxisphase geben. Außerdem möchte ich noch kurz einen generellen Ausblick zu der von mir bearbeiteten Thematik geben.

4 Evaluation der Praxisphase

4.1 Das Unternehmen

4.2 Lessons Learned

Crypto API schneller wählen+ direkt c entwickeln

4.3 Persönliche Einschätzung des Lernerfolgs