Report on Encryption Technologies for BMS Safety and Security

D3.3

www.incobat-project.eu

Confidentiality	CO	**Deliverable Type**	R
Project	INCOBAT	**Project Number**	608988

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 608988

1 Publishable Executive Summary

Cars are becoming more and more computers on wheels as an increasing amount of functions is being controlled by embedded control units (ECUs). There are vehicle internal communication networks connecting these ECUs and there are different communication interfaces for various purposes that enable external access to the car. Examples are the onboard diagnosis to support maintenance or Bluetooth, WLAN and GSM that enable the car to communicate with mobile devices, other cars or central service points. Consequently security becomes an issue for modern cars and intrusion to the IT infrastructure of a car can become a serious threat if for example safety relevant functions like electronic brake control or steering are manipulated. Hence, safe and reliable operation requires safety and security.

Needless to mention that safety is an essential characteristic of battery management systems (BMS). Security is of similar importance for BMS because of the connections to the vehicle internal network for exchange of information like battery status or commands to control the battery. Integration with the smart grid requires external connections e.g. to identify the car when it connects to the supply net for charging or to provide energy. Thus, BMS is in principle accessible via various communication interfaces of the car to the external world. It faces therefore also security threats and some of them may cause safety issues.

This deliverable examines existing approaches for secure vehicle IT architectures and its potential application to battery management systems of electrified vehicles. In particular, possible security related features and functions and potential threats or misuse will be described. Further, several hardware-based security approaches will be investigated that might be applied to EVs in the context of BMS as well as its wider safety or cyber security implications.

For that, results from recent projects and research activities, mainly results of the projects EVITA and OVERSEE, for cost effective implementations of cyber-security for a BMS were examined, i.e. TCG-TPM, EVITA-HSM and HIS-SHE. Main focus will be the investigation of hardware capabilities of modern CCUs to support such security mechanisms. Following, the security capabilities provided by the Infineon AURIX™ controller will be looked at which will be the basis for the INCOBAT BMS ECU. Figure 1 shows the architecture of the AURIX controller from security point of view. It offers a secure platform which is separated from the rest of the microcontroller by a firewall. Major characteristics are the high flexibility and programmability. The controller features will be investigated whether they are suited to meet the requirements of a future-proof automotive trusted computing platform.

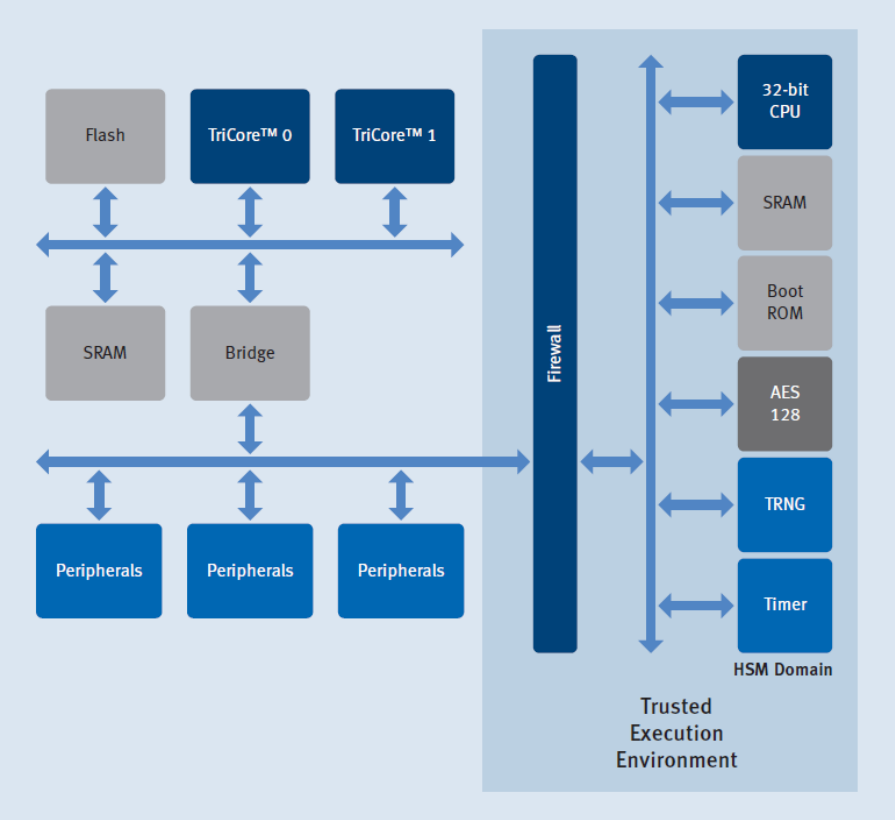

Figure 2: Overview AURIX hardware security module

In a first step results and proposed technical solutions based on EVITA and OVERSEE project were analyzed. Next, the obtained results are mapped to the needs of the BMS application like the security use cases shown in Table 1. The analysis results can be mapped to the hazard and risk analysis and in the following to the requirements of the INCOBAT BMS. Then a comparison to the capabilities of the AURIX HSM was done. SHE HIS and EVITA Medium standards are fulfilled by the AURIX HSM and some additional features are provided. The use cases and the security capabilities can be used to identify solutions which are relevant to the INCOBAT BMS.

Table 2: Use cases BMS security

Category	ID	Short	Description	Priority
Communication External Networks	BMS-UC-01	External communication	The car receives data or a message by a C2X service via a vehicle-external communication network.	C
Nomadic Device Interfaces	BMS-UC-11	Data exchange or applications nomadic devices	The car exchanges data with nomadic/mobile devices, connected by the user (USB Sticks, MP3 …) or installs/runs applications from those devices. Only listed for completeness here as this UC should be covered by an appropriate ECU (e.g. the head unit)	C
3rd party ECUs	BMS-UC-41	Communication with built-in or replaced ECUs by a 3rd party device	Communication to/from the battery pack or to/from other ECUs of the OEM or a supplier. Assumed that some kind of certification will take place so less significant.	B
Aftermarket ECU	BMS-UC-21	Replacement of an in-vehicle ECU	Replacement of an built-in ECU (not the BMS ECU) e.g. due to malfunction; in general this requires also the flashing of the ECU at the garage	A
	BMS-UC-22	Replacement of the BMS ECU	Replacement of the built-in BMS ECU e.g. due to malfunction; in general this requires also the flashing of the ECU at the garage	A
	BMS-UC-23	Replacement of the battery	Replacement of the battery due to malfunction or ageing. Some approaches for EVs consider battery replacement as alternative to charging of the on-board battery.	A
Diagnosis	BMS-UC-31	Diagnosis of the BMS ECU	On-Board Diagnosis or Off-Board Diagnosis of the BMS-ECU, e.g. via OBD, where Off-Board diagnosis is done with an off-vehicle system (e.g. diagnosis tool) by connecting the diagnosis tool to the On-Board Diagnosis system	A
	BMS-UC-32	Flashing	Flashing of the BMS-ECU via a OBD connection	A
	BMS-UC-33	Remote diagnosis or flashing	Remote (wireless) diagnosis, parameter update or flashing of the BMS ECU; Only listed for completeness here remote connections should be handled by an appropriate ECU outside the BMS	C

Priority value range: A = very important, B = important, C = less important