Functional Safety and Cybersecurity aspects of Over the Air Updates

Presenter Name : Riya Shah-a[1], Tanya Agarwal-b[2]

[1] Mahindra Electric, Email ID : SHAH.RIYA@MahindraElectric.com
[2] Mahindra Electric, Email ID : AGARWAL.TANYA@MahindraElectric.com

This paper addresses the functional safety and cybersecurity aspect of Over the Air (OTA) updates. Over the last two decades, cell phone manufacturers have been regularly sending updates on their user's phones to fix a bug or upgrade the system. Similar trends have been observed in the automotive industry wherein, over the past decade, OTA updates were provided remotely using Firmware and Software (FOTA/SOTA). Amongst its competitors, Tesla topped the list by sending 380+ OTA updates to its drivers in 6 years. The top 5 OEMs across the globe are not far behind and vying to expand the OTA update market. The OTA implementation promises to reduce the cost of the recalls by 15%, which in turn will lower the operational cost by $35 billion. Apart from monetary and resource benefits, OTA also serves to make automotive components more secure and safe. For instance, if the government regulations change or vulnerability thresholds of a cyber-attack lowers, an OTA update can ensure that the component is upgraded to meet the regulation or mitigate the hazard/threat.

These updates on safety and security applications bring with them the risk of safety goal violation or security breach. Therefore, it is necessary to evaluate and resolve 1) the safety aspects of OTA updates independent of security concerns, 2) the safety impact of cyber-attacks to rate security risks, and 3) the impact of safety measures on security ratings and vice-versa. Depending on the different use cases and frameworks, the complexity of the solution varies. Our framework includes an internet-connected gateway unit in charge of managing updates to OTA clients as received from the cloud server. The focus of this paper is on evaluating the hazards and threats for both the telematics unit and OTA clients of the framework. Based on the results of integrated hazard/threat analysis and risk management, the presenter derived functional safety and functional security requirements. The scope of the paper is limited to include the SW update and exempts data collection and diagnostics part of OTA from the analysis.

The authors used Hazard and Operability Analysis (HAZOP) activity to facilitate HARA for the telematics unit and OTA clients. The Hazard Analysis and Risk Assessment (HARA) and Threat and Operability Analysis (THROP) results served as a pre-requisite for subsequent Threat Analysis and Risk Assessment (TARA) evaluation. To rate and control the security risks, cybersecurity standards such as ISO 27001 and SAE J3061 served as the guidelines. For safety risks, ISO 26262 examples did the job. To ensure zero safety and security issues within the OTA feature, our analysis showed that its regular governance needs to be established. In the automotive organization, this governance is possible only when hazard analysis is extended to include relevant threats from cyber-attackers. Due to our integrated approach, we were able to define security-specific control measures for safety-critical elements. In conclusion, using our OTA example within an electric powertrain, we intend to share the best practices which can be adopted for better synergy between system safety and system cyber-security engineering.

Keywords: Functional Safety, Cyber Security, Electric Vehicles, Over the Air Update, System Engineering