\chapter{Functional Architecture with Safety Measures}

\label{Chapter4}

\noindent From Chapter \ref{CHAP3} it follows that the ALC system reaches an ASIL D level, which leads to a safety critical system. During the functional safety assessment of an automotive system design it can be chosen to reduce the ASIL levels via ASIL decomposition. ASIL decomposition is a method to assign ASILs to redundant requirements. The redundant requirements can be used to improve the integrity of the system. In this case the FSRs originating from the safety goals are decomposed into redundant and sub requirements that ensure the achievement of the ‘parent’ FSR. The decomposed FSRs are tested afterwards to ensure that the system is working correctly.\newline

\noindent The main rule for this decomposition is that the redundant requirements are allocated to different components of the system. If one component fails to satisfy a particular FSR, the other component can still do so, which improves the system integrity. Important to mention is that the ASIL decomposition can be applied to any requirement at any stage in the design process. The ASIL decomposition can be used to reduce the ASIL level of a safety goal via the rules shown in Table. \ref{ASILdecomposition}. According to \cite{ugly}, the highest decomposed ASIL are assigned to the sub requirements based safety mechanism. Adding redundant safety mechanisms to the system will lead to an equal ASIL assignment to the decomposed FSRs.\newline

\begin{table}[h]

\centering

\caption{ASIL Decomposition \cite{ugly}}

\label{ASILdecomposition}

\begin{tabular}{|c|c|}

\hline

\textbf{ASIL before Decomposition} & \textbf{ASIL after Decomposition} \\ \hline

ASIL D Requirement & \begin{tabular}[c]{@{}l@{}}ASIL C(D) Requirement + Asil A(D) Requirement\\ or\\ ASIL B(D) Requirement + Asil B(D) Requirement\\ or\\ ASIL D(D) Requirement + Asil QM(D) Requirement\end{tabular} \\ \hline

ASIL C Requirement & \begin{tabular}[c]{@{}l@{}}ASIL B(C) Requirement + Asil A(C) Requirement\\ or\\ ASIL C(C) Requirement + Asil QM(C) Requirement\end{tabular} \\ \hline

ASIL B Requirement & \begin{tabular}[c]{@{}l@{}}ASIL A(B) Requirement + Asil A(B) Requirement\\ or\\ ASIL B(B) Requirement + Asil A(B) Requirement\end{tabular} \\ \hline

ASIL A Requirement & ASIL A(A) Requirement + Asil QM(A) \\ \hline

\end{tabular}

\end{table}

\section{Decomposition of FSR’s for ALC}

\noindent The first step in the ASIL decomposition is to determine the safety measures. It can be concluded from Chapter \ref{CHAP3} that the safety goals are related to: wrong/missing input, wrong process or missing output. Therefore, the corresponding safety measures that are required for the decomposition are functions/mechanisms that check the:

\begin{itemize}  
\item arrival and sending of the data at specific components/functions  
\item correctness of the received/calculated data by means of redundancy or predictions  
\item correctness of the decisions made by the supervisors  
\end{itemize}

\noindent The updated functional architecture with safety mechanism is provided in Appendix \ref{App\_DFSR}. Each safety mechanism adds new FSRs to the system. Most of the Decomposed Functional Safety Requirements (DFSRs) are safety measure related requirements that are added to the system to check incorrect operation and reach the corresponding safe states. Therefore, most FSR are decomposed into ASIL C(D) + ASIL A(D) requirements. To decompose the ASIL D FSR into two ASIL B (D) DFSRs, redundant safety mechanism should be added. One example of such a redundant safety measure is to use both the Mobileye lane detection system and the own designed lane detection algorithm.\newline

\noindent The ASIL decomposition will now be explained for the excessive steering scenario, previously explained in Chapter \ref{CHAP3}. The ASIL decomposition of this FSR is shown in Fig. \ref{DFSR}. According to FSR 24 in Fig. \ref{DFSR}, ‘’the system shall only apply a limited additional steer torque to prevent excessive steering when ALC is active’’. The according safety mechanism is a filter that limits the output steer torque to a certain value’’. This comes with the functional safety requirement: ‘’the lateral controller output should be limited to avoid excessive steering torques. Since this safety mechanism is sub requirement based an ASIL C(D) is assigned to the safety mechanism related FSR, whereas an ASIL A(D) is assigned to the original FSR.

\noindent It can be concluded from Appendix \ref{App\_DFSR} that the final ASIL level of the system is ASIL C. For future work it may be possible to reduce the ASIL levels further by using decomposition methods like software redundancy or hardware redundancy. Compared to hardware redundancy, the relative costs of software redundancy is much smaller.