

Safety Functions on Commodity Hardware with Diversified Encoding

Martin Süßkraut¹, André Schmitt² and Jörg Kaienburg³

Abstract: Currently, hardware designed and certified for safety-critical systems is one important building block for any safety-critical application. Such hardware provides the detection of execution errors. However, many modern safety-critical applications, like autonomous driving, require features and performance levels that are not available from safety-certified hardware. One solution to this problem is to use hardware that is not certified for safety-critical systems, for example consumer-graded hardware, but that fulfills the feature and performance requirements. Additionally, a software solution provides the detection of execution errors.

This paper introduces such a software solution called “Diversified Encoding with Coded Processing”. Due to its hardware-independence, this solution provides the flexibility to build safety-critical systems from non-safety-critical hardware components. This solution can be automated with a code transformation tool to further increase the flexibility.

Keywords: safety, ISO 26262, software coded processing, software diversification

¹ SIListra Systems GmbH, Königsbrückerstr. 124, 01099, Dresden, martin.suesskraut@silistra-systems.com

² SIListra Systems GmbH, Königsbrückerstr. 124, 01099, Dresden, andre.schmitt@silistra-systems.com

³ SIListra Systems GmbH, Königsbrückerstr. 124, 01099, Dresden, joerg.kaienburg@silistra-systems.com