

Examination of the Validity of Connections between MSILs and ASILs in the Functional Safety Standard for Motor Vehicles

Sei Takahashi and Hideo Nakamura
Nihon University

Makoto Hasegawa
Japan Automobile Research Institute

ABSTRACT

ISO 26262, a functional safety standard for motor vehicles, was published in November 2011. Although motorcycles are not included in the scope of application of the current edition of ISO 26262, it is expected that motorcycles will be included in the next revision. However, it is not appropriate to directly apply automotive safety integrity levels (ASILs) to motorcycles because the situation of usage in practice presumably differs between motorcycles and motor vehicles. In our previous study, we newly defined safety integrity levels for motorcycles (MSILs) and proposed that the levels of MSILs should correspond to levels one step lower than those of ASILs; however, we did not investigate the validity of their connections. Accordingly, in this research, we validated the connections. We defined the difference of levels of SILs between motorcycles and motor vehicles as the difference of target values of random hardware failure rates specified in ISO 26262-5. By taking into account the benefits of economy, convenience, and pleasure, it is considered that motorcycle and motor vehicle users accept the results of traffic accidents as upper limits on tolerable risks. Using recent traffic accident results, we compared accidental risks while riding motorcycles or motor vehicles. We demonstrated that the difference of levels of SILs between motorcycles and motor vehicles and the difference of upper limits on tolerable risk between motorcycles and motor vehicles balance each other. It is considered that this finding justifies setting the levels of MSILs one step lower than the levels of ASILs.

CITATION: Takahashi, S., Nakamura, H., and Hasegawa, M., "Examination of the Validity of Connections between MSILs and ASILs in the Functional Safety Standard for Motor Vehicles," *SAE Int. J. Engines* 9(1):2016.

INTRODUCTION

ISO 26262 (Road vehicles - Functional safety) was published in November 2011 as a functional safety standard for electrical/electronic systems used in motor vehicles. ISO 26262 is based on IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems). ISO 26262 is a sector-specific adaptation of IEC 61508 that applies to the motor vehicle industry. Functional safety refers to the type of safety that is realized when a safety-related system, such as safety equipment, is functioning properly. In ISO 26262, functional safety is defined as the "absence of unreasonable risk due to hazards caused by malfunctioning behaviour of electrical/electronic systems."

A characteristic feature of ISO 26262 is the concept called Automotive Safety Integrity Level (ASIL) for motor vehicles. ASILs define the levels of safety measures required in order to avoid unreasonable remaining risks due to malfunctioning behaviour of items. ASIL includes four levels, ASIL A to ASIL D: ASIL D represents the highest severity, and ASIL A represents the lowest severity.

In the current edition of ISO 26262, passenger cars with a maximum gross vehicle weight up to 3500 kg are included in the scope of application; however, motorcycles are not included in the scope of application. Motor vehicles for which safety integrity levels are investigated in this research refer to "vehicles intended mainly to travel on roads (vehicles with four or more wheels)." Motorcycles refer to- or three-wheeled motor vehicles, not including mopeds."

However, it is not appropriate to directly apply ASILs to motorcycles. In the first place, the situation of usage in practice presumably differs between motorcycles and motor vehicles. It would be excessive to require the same level of safety measures for motorcycles as that for motor vehicles.

In our previous study [2], we newly defined safety integrity levels for motorcycles (MSILs) and investigated their connections with ASILs. We demonstrated that, by considering motorcycle-specific situations, it is appropriate to increase the degree of tolerable risk for motorcycles compared with the case of motor vehicles, and that it is appropriate to reduce the maximum severity for motorcycles compared with motor vehicles. From these results, we demonstrated

that it is appropriate to reduce the adequacy of safety measures required against the risks associated with motorcycles compared with the case of motor vehicles.

Accordingly, in this research, we validated the connections between MSILs and ASILs; specifically, we demonstrated that there are grounds for reducing the adequacy of required safety measures against the risks associated with motorcycles compared with the case of motor vehicles, on the basis of the results of traffic accidents.

In the rest of this article, Section 2 describes our definitions of MSILs that will be introduced in the next revision of ISO 26262, as well as the corresponding relationships between MSILs and ASILs. Section 3 describes a basic concept for investigating the validity of the corresponding relationships between MSILs and ASILs. Section 4 describes an examination of the validity on the basis of the results of traffic accidents. Lastly, concluding remarks will be given in Section 5.

CONNECTIONS BETWEEN MSILS AND ASILS IN ISO 26262

A characteristic feature of ISO 26262 is the concept called ASILs for motor vehicles. Figure 1 shows the Correspondence Diagram between Risk and ASIL (CDRA) in order to explain the concept of ASIL [2]. For each item constituting a safety-related system, hazard analysis and risk assessment are conducted to determine initial risks (Circle-I in Figure 1). The initial risks are classified into corresponding ASILs according to Severity (S) and Frequency. Frequency is determined according to both Exposure (E), representing the probability of occurrence of a driving scenario that could result in a hazardous event, and Controllability (C) for avoiding a hazard. Then, risks are reduced by taking safety measures according to the ASILs such that only tolerable risks (Circle-R in Figure 1) remain. The lengths of red arrows in Figure 1 represent the “degrees of adequacy” of safety measures defined for the individual ASILs. The arrow length is longest for ASIL D, representing the highest safety integrity level.

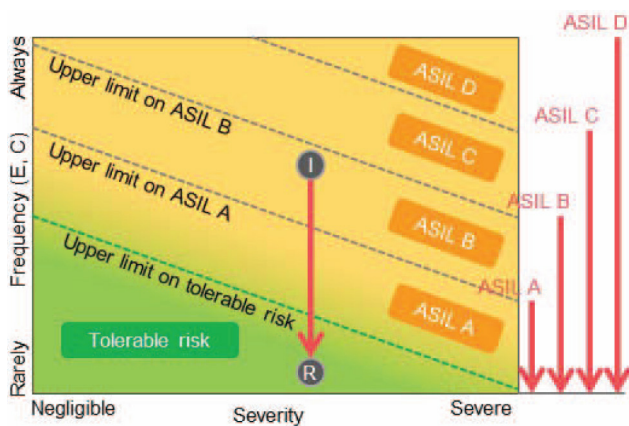


Figure 1. Correspondence Diagram between Risk and ASIL (CDRA) [2].

It is not appropriate to directly apply current ASILs to motorcycles. In the first place, the situation of usage in practice presumably differs between motorcycles and motor vehicles. It would be excessive to require the same level of safety measures for motorcycles as that for motor vehicles.

In our previous study [2], we newly defined MSILs for motorcycles. Figure 2 shows the Correspondence Diagram between Risk and MSIL (CDRM) in order to explain the concept of MSIL. We demonstrated that, by considering motorcycle-specific situations, it is appropriate to increase the degree of tolerable risk for motorcycles compared with the case of motor vehicles (see graph at the upper right side of Figure 2), and that it is appropriate to reduce the maximum severity for motorcycles compared with motor vehicles (see graph at the upper left side of Figure 2), on the CDRA shown in Figure 1 in order to explain the concept of ASILs. This allows the intolerable risk area in the CDRA to be considerably reduced compared with that for motor vehicles. We newly defined four MSILs in this risk area. Upper limits on MSILs A to D in Figure 2 correspond to ASILs shown by red arrows in the right side of the figure. As a result of investigating connections between MSILs and ASILs based on this conceptual diagram, it was revealed that the adequacy of safety measures required against risks associated with motorcycles was less compared with the case of motor vehicles; in other words, we propose that the levels of MSILs should be one step lower than the corresponding levels of ASILs.

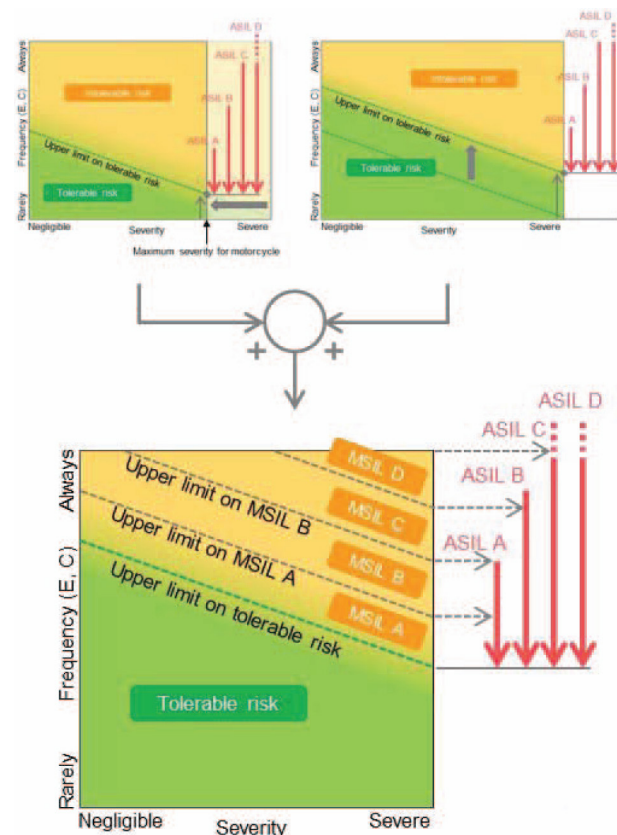


Figure 2. Correspondence Diagram between Risk and MSIL (CDRM) [2].

Table 1 shows the risk matrix used to define our proposed MSILs. The combinations of the individual classes S, E, and C determine the levels of MSIL A to MSIL D, or “QM”. “QM” in Table 1 denotes quality management. In ISO 26262, there are no requirements for QM, and normal quality management levels are required. A hazard is always classified into QM in the case where one of the parameters S, E, and C is S0, E0, or C0. The levels in parentheses represent the corresponding levels of ASILs. This suggests that even in the case where a hazard is classified into MSIL D, it suffices to take the level of safety measures required for ASIL C.

Table 1. Determination of MSILs [2].

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A[QM]
	E4	QM	A[QM]	B[A]
S2	E1	QM	QM	QM
	E2	QM	QM	A[QM]
	E3	QM	A[QM]	B[A]
	E4	A[QM]	B[A]	C[B]
S3	E1	QM	QM	A[QM]
	E2	QM	A[QM]	B[A]
	E3	A[QM]	B[A]	C[B]
	E4	B[A]	C[B]	D[C]

In that study, however, although we demonstrated the conceptual connections between MSILs and ASILs, we did not investigate the validity of the connections.

BASIC IDEA OF VALIDATING CONNECTIONS BETWEEN MSILS AND ASILS

In this section, we propose a basic idea for validating the connections between MSILs and ASILs. The basic idea is to demonstrate that the difference of levels of SILs, which are technical safety indicators, and the upper limits on tolerable risk, which are social safety indicators, between motorcycles and motor vehicles balance each other. There are various aspects for defining an upper limit on tolerable risk, such as economy, convenience, etc. It is considered that, by taking these aspects into account, motorcycle and motor vehicle users accept the results of traffic accidents as upper limits on tolerable risks.

In order to confirm the validity of the connections between MSILs and ASILs shown in Table 1, it is necessary to demonstrate that the difference of levels between MSILs and ASILs in terms of the same initial risks and the difference of the upper limits on tolerable risk between motorcycles and motor vehicles balance each other. Figure 3 shows a risk diagram for explaining this idea. The initial risks (Circle-I in Figure 3) correspond to ASIL D for motor vehicles and MSIL D for motorcycles, respectively. Then, risks are reduced by

taking safety measures according to the corresponding SILs such that only tolerable risks (Circle-RA for motor vehicles and Circle-RM for motorcycles in Figure 3) remain. The difference of levels between ASIL D and MSIL D corresponds to that between ASIL D and ASIL C because MSIL D corresponds to ASIL C according to Table 1. Therefore, in order to show the validity of connections between MSILs and ASILs, it is necessary to demonstrate that the difference of levels of MSIL D (ASIL C) and ASIL D and DoL (Difference of Level in Figure 3), which is the difference of upper limits on tolerable risks between motorcycles and motor vehicles, balance each other.

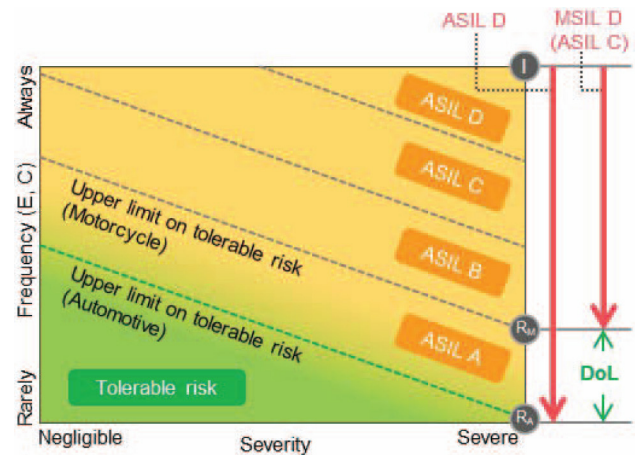


Figure 3. Risk Diagram for Explaining Validation of Connections between MSILs and ASILs.

Next, we will investigate upper limits on tolerable risks. There are various aspects for defining an upper limit on tolerable risk (Table 2). For defining the upper limits on acceptable risks for motorcycles and motor vehicles, it is considered that the risk-benefit factor has the greatest affect among these factors. If the benefit from the objects is large, there is a possibility of increasing the degree of tolerable risk. For instance, benefit includes factors like convenience and pleasure etc. It is considered that, by taking into account the aspects shown in Table 2, motorcycle and motor vehicle users accept the upper limits on tolerable risks. In the following, we compare motorcycles with motor vehicles in terms of some of these factors in determining the level of tolerable risk.

Table 2. Factors in Determining the Level of Acceptable Risk.

Factor	Examples
Regulations	Legal Regulation
Standard	Higher Standard or Standards for Other Fields
Social Factors	Results of Traffic Accidents Wide Adoption of Technology
Economic Limitations	Cost of Risk Reduction
Technological Limitations	Impossibility of Achievement Unknown Failure Rate Unknown Severity
Risk-Benefit	Economy, Convenience
Historical Background	Nation, Safety Culture