機能安全の安全度水準に関する調査研究

日本大学　理工学部　応用情報工学科　准教授　高橋　聖

１．はじめに

鉄道システム，特に列車制御システムには高い安全性が求められている。一方，鉄道システムだけでなく，産業のあらゆる分野で電子化が進み，安全性実現のためにコンピュータが多く使われるようになってきた。このような背景のもと，機能安全に関する国際規格である IEC 61508 が制定されている [(1)]。そして，IEC 61508 をもとに，様々な産業分野で個別に機能安全規格が制定されている。

機能安全に関する規格の中では，システムに対するリクスアセスメントの結果推定された初期リスクに対し，それを許容できるリスクまで低減するための安全方策の手厚さを示した安全度水準がある。

同じ初期リクスであっても，各分野のシステムごとに特有の状況があり，許容できるリスクはそれぞれ異なる。安全方策は大事であるが，過剰な安全方策は製造者，使用者双方に必要以上の負荷を強いることにつながる。したがって，規格等による安全度水準は，各分野のシステムの実情に沿って適正に規定される必要がある。

本調査研究では，他の産業分野，特に乗用車の機能安全に関する国際規格である ISO 26262 に関する文献を中心に，機能安全の安全度水準に関して報告する。

２．ISO 26262 における四輪車と二輪車の安全度水準

ISO 26262（Road vehicles - Functional safety）は，乗用車のための機能安全規格として 2011 年 11 月に制定された [(2)]。本規格の中では，安全関連系システムを構成する各アイテムの危険事象を，Severity，Exposure，Controllability の 3 つの尺度で評価し，乗用車のための安全度水準である ASIL（Automotive Safety Integrity Level）を決定する。

ASIL は ASIL A から ASIL D まで 4 つのレベルがあり，ASIL D が最も厳しいレベルである。現時点では，ISO 26262 の適用範囲は 3500 kg 以下の四輪車のみで，二輪車は含まれない。しかし，次期改定時には二輪車が含まれることが予想されている。

Takahashi ら [(3)] は，ASIL をそのまま二輪車に適用することは妥当ではないと考え，二輪車のための安全度水準である MSIL（Motorcycle Safety Integrity Level）を新たに定義している。そして MSIL と ASIL とのつながりを考察した結果，二輪車のリスクに要求される安全度水準は，乗用車よりも軽減できることを示した。

Takahashi ら [(3)] はまず，ASIL の概念を説明するためのリスクダイアグラムである Correspondence Diagram between Risk and ASIL (CDRA)（図 1）を示した。図 1 中の ASIL の赤矢印の長さは，各 ASIL に規定された安全方策の手厚さの程度を示している。最も厳しい ASIL D の矢印の長さが最も長くなっている。

この CDRA をもとに，2 つの基本的な考えにしたがって，二輪車のための安全度水準を定義している。1 つ目は，二輪車と四輪車の車両質量が異なることから，CDRA 上において，二輪車の最大過酷度は，

乗用車よりも縮小できるとしている。2つ目は，事故時の乗員の保護手段の違いや，事故統計資料による死傷者数の割合が二輪車のほうが大きいことから，CDRA 上において，二輪車の許容できるリスクの上限は，乗用車よりも緩和するとしている。

上述した考え方から，MSIL の概念を説明するためのリスクダイアグラムである Correspondence Diagram between Risk and MSIL (CDRM)（図 2）を示し，CDRM 上に新たに MSIL A から MSIL D を定義している。そして，MSIL と ASIL とのつながりを考察した結果，MSIL の各レベルを，1 レベル低い ASIL に対応づけることを提案している。

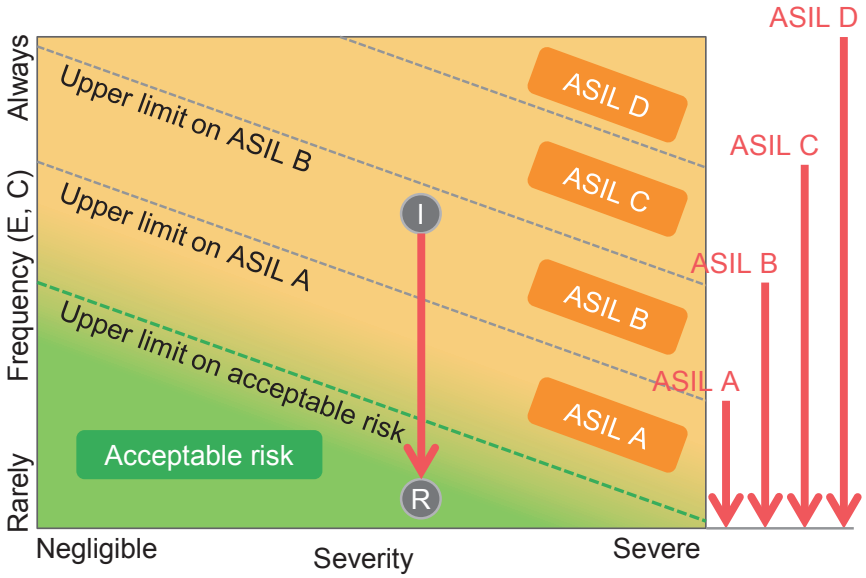

図 1　リスクと ASIL の関連図（CDRA）[3]

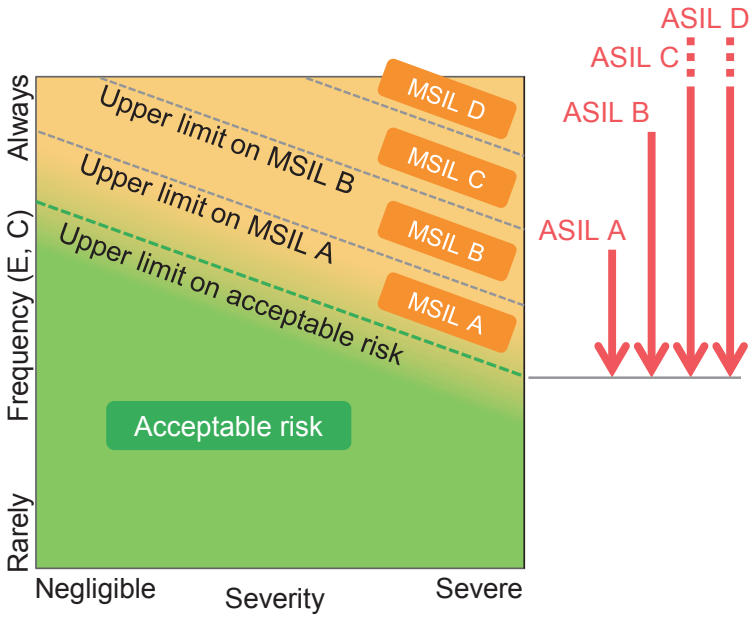

図 2　リスクと MSIL の関連図（CDRM）[3]

３．鉄道および生活支援ロボット分野における安全度水準

乗用車以外の分野として，鉄道および生活支援ロボット分野における安全度水準について調査した。生活支援ロボットは，鉄道や乗用車と同様に人を乗せて移動するものも含まれ，そのための国際安全規格が最近発行されたばかりである。

鉄道分野に関しては，秋田[(4)]が鉄道の事故リスクの許容水準と評価手法について考察している。安全度水準は，許容できるリスクによって異なってくるので，リスクの許容水準は妥当なものに設定する必要がある。そこでは，一般産業を対象とした事故リスクの許容水準の原則である，ALARP，MEM，GAME 等を参考にし，これに日本の鉄道の事故実績を踏まえてリスクの許容水準を提案している。

秋田[(4)]は，鉄道の事故リスクの許容水準等の設定要件を整理し，許容水準と広く受容可能な水準を区別して設定した。そして，鉄道の事故を運転事故と列車事故に区別して，それぞれの許容水準値等を設定している。

生活支援ロボット分野では，2014 年 2 月に国際安全規格 ISO 13482 (Robots and robotic devices - Safety requirements for personal care robots) が発行された[(5)]。ISO 13482 は本文 8 章と A から E の 5 つの Annex で構成されており，第 6 章「Safety-related control system requirements」が機能安全に関連する部分に相当すると考えられる。

本規格の第 6 章では，安全関連制御システム（電気，液圧，空気圧，ソフトウェアを含む）に対する要求事項を示しており，リスクアセスメントにより，適切な Performance Level（PL）または Safety Integrity Level（SIL）を割り当てることを求めている。そして，割り当てられた PL または SIL は，ISO 13849-1（制御システム安全関連部）または IEC 62061（機械類の安全性 － 安全関連の電気・電子・プログラマブル電子制御システムの機能安全）に示された PL または SIL に従うこととしている。ISO 13482 で対象としている生活支援ロボットはまだ販売実績が少なく，事故実績等のデータがない新しいシステムの安全規格の例である。

４．まとめ

他分野の規格，特に乗用車の機能安全に関する国際規格である ISO 26262 に関する文献を中心に，機能安全の安全度水準に関して調査研究した。二輪車と四輪車では，許容できるリスクの上限が異なるため，それに応じて異なるレベルの安全度水準を規定することを提案していた。鉄道分野に関しては，秋田[(4)]が鉄道の事故リスクの許容水準と評価手法について考察している。また，生活支援ロボットの国際安全規格 ISO 13482 (Robots and robotic devices - Safety requirements for personal care robots) が 2014 年 2 月に発行されており[(5)]，まだ市場での実績が少ない生活支援ロボットに対して安全度水準を規定している。システムの安全度水準は，対象分野ごとに適切に割り当てられるべきであり，それは社会的および技術的要因の変化に伴い見直される可能性もありうる。

以上

参考文献

(1) IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems), 2010.
(2) ISO 26262 (Road vehicles - Functional safety), 2011.
(3) S. Takahashi, H. Nakamura and M. Hasegawa, One Approach to Definition of MSILs and Their Connections with ASILs, SAE Technical Paper, 2014-32-0016, 2014.
(4) 秋田雄志“鉄道の事故リスクの許容水準と評価手法に関する研究,”日本大学博士論文, 2006.
(5) ISO 13482:2014 (Robots and robotic devices - Safety requirements for personal care robots), 2014.