第 104 回 SNJ 定例会（オンライン形式）議事録

◎　件　名　　第 104 回 SNJ 定例会（オンライン形式）議事録
◎　日　時　　令和 3 年 12 月 3 日（金）15:00-17:20
◎　出席者　　23 名（非会員含む）

各位

日本大学	中村			労働安全衛生総合研究所	清水
	高橋				北條
					菅
北陽電機				JR 東日本	川野
大同信号	寺田			大同信号	吉富
	阿久根				中野
東京理科大学				海洋研究開発機構	眞砂
海上・港湾・航空技術研究所	柚井			有人宇宙システム	
日本ヒューマンファクター研究所				株式会社コア	
コレムラ技研	是村			西日本電気テック	
村田機械株式会社	今枝			ピルツジャパン	太田
					杉原

Ⅰ　講演「ハザード、リスクの分類と機能安全、SOTIF が対象とする範囲 – 自動運転、AI を通して」（川島）抜粋

- [川島氏は]日本信頼性学会の要素技術安全研究会の主査として、機能安全規格の調査研究、研究成果を国際規格に反映する取り組みを行っている。
- IEC 61511 や IEC 62061 などの機能安全規格や、そこから展開する ISO 10218（産業用ロボット）などの製品規格は、閉じた運用環境（=あらかじめ定義され、制限された運用環境）で対象物が使用されることを前提としている。
- 多くの機能安全規格は、運用環境が閉じたシステムにおける、安全関連系の安全性能限界内のハザード・リスクへの適用を意図しているといえる。
- 生活支援ロボットや、自動車などは、子どもや高齢者、一般消費者など、訓練や許可された人以外も共存する環境（開いた運用環境）で使用されるため、ハザードを限定できない。
- 自動運転車は、開いた運用環境のシステムの一例である。
- 自動運転車では、LiDAR(レーザー光を使用するセンサによる位置・形状・距離検出)やカメラの性能の限界により、雪、対向車のライトなどの影響を受けて、故障せずとも正常検出できない場合がある。
- 信号、標識、道路状況のカメラ画像が不鮮明な場合（色あせたり、一部隠れたりしている)、故障せずとも正常検出できないことがある。
- AI 技術を画像処理に適用する場合、人の期待と異なる予見できない判断をして、画像を誤認する可能性がある。
- 今後、自動運転車やロボットに AI 技術が適用される見込みは高い。
- AI は人の期待と異なる判断をする可能性があり、安全性の検証が困難であるため、現行の機能安全規格 IEC61508-3 Ed.2(2010)では、SIL2 以上は安全技術への適用を推奨していない。
- AI だけで固有安全/本質安全を達成するのは、現時点では困難なため、AI を実装したシステムは、AI の機能安全手段と AI 以外の手段の両者による多重防護層の構築により、安全を確保する。
- システムが故障しなくても、合理的に予見可能な誤使用（製造者が意図しない方法でユーザーがシステムを使用すること）によって生じる危険は想定しなければならない。
- 安全な自動運転のために、安全関連系が故障せずとも（システムが正常でも）意図した安全機能では対応できない事象については、ISO/PAS 21448: 2019 Road Vehicles – **S**afety **o**f **t**he **i**ntended **f**unctionality（通称 **SOTIF**)で対応する。
- SOTIF では、未知の危険なシナリオを許容可能なレベルまで小さくすることを目標とする。
- 未知の危険なシナリオは、各種テストや、系統的な分析などの産業分野でのベストプラクティスで少なくする。
- 2021 年発行の国際規格案 ISO/DIS 21448 では、ISO/PAS 21448 と比較して、残存リスクの評価項目が 12 種類から 16 種類に増加した（追加項目の例：合理的に予見可能な誤使用のテスト)。
- SOTIF は、機能安全が対象としない、安全機能性能限界外のハザード・リスクを可能な限り同定・分析し、除去または許容レベルまで低減するために適用する。
- 安全機能の対象外リスク（残留・残存リスク）については、リスクアセスメントでリスクレベルが許容範囲内であるか判定する。
- リスクアセスメントの品質向上でメタリスク（予見不能リスク）を予見可能にして許容可否を判定する。
- 2018 年 9 月に米国アリゾナ州で発生した自動運転車による死亡事故は、SOTIF 規格を適用することで防げた可能性が高い。

II　質疑応答（抜粋）

- Q1. SOTIF では予見不可能なリスクはできるだけ予見可能にし、未知は既知にしようと言っているが、予見不可能なものも SOTIF は対象としているのか？
- A1. SOTIF は、予見不可能なものも対処としている。予見不可能なものも含めて、残存リスクが許容できるかどうか判断する。技量によって、現在未知のものを既知としていき、未知が既知になったとして、それでも残存リスクが許容できなければ、前提条件を変えるなどして残存リスクが許容できるレベルまで低減する。
- Q2. ご紹介いただいた自動運転車の事故は、SOTIF を適用していれば防げたかもしれないとのことだが、何をしていれば、事故を防げたのか？
- A2. この事故では、**安全機能の不完全性**（対象物の検知結果が幾度も変化し、位置の履歴が引き継がれず、移動経路を正確に予測できなかった）と**合理的に予見できる誤使用**が原因で起こった。仮に、検知機能が働かなくても、運転者が自動運転中に動画を見るというのは、合理的に予見できる誤使用であった。運転者の視線を感知するようなシステムで、事故防止の対応をすることが可能であった。

III 報告事項

・　次回は、2 月 4 日(金)に、第 22 回 SNJ 総会および第 105 回定例会を開催する。開催形式は未定。定例会の講師は北條理恵子氏（労働安全衛生総合研究所）と齊藤智明氏（株式会社 ISID エンジニアリング）を予定。今年は宿泊を伴う総会は行わない。

IV 審議事項

・　1 月初旬に、2 月 4 日の総会および第 105 回定例会を対面、オンラインのいずれで行うか役員で審議する。

以上