第 117 回 SNJ 定例会（ハイブリッド形式）議事録

◎ 件　名　　第 117 回 SNJ 定例会（ハイブリッド形式）議事録

◎ 日　時　　令和 6 年 6 月 14 日（金）15:00-17:30

◎ 出席者　　23 名（非会員含む）

各位

日本大学	中村			G・O・P 株式会社	
	高橋				
大同信号	寺田			北陽電機	
JR 東日本	川野			JR 東日本	羽手原
	野上				藤本
	池谷				槻澤
	岩森				
東京理科大学				有人宇宙システム	
海洋研究開発機構				海上・港湾・航空技術研究所	柚井
株式会社コア				日本ヒューマンファクター研究所	
長岡技術科学大学				コレムラ技研	
西日本電気テック				村田機械株式会社	
しくみデザイン Lab.	齊藤			ナミックス株式会社	
ピルツジャパン	太田				
	杉原				

I　講演「機能安全 IEC 61508 の SIL 割当てと安全関連系の独立性」（川島）抜粋

- 川島氏が主査を務める日本信頼性学会の要素技術安全研究会では、機能安全に関連する規格、法令、要求事項の調査を行い、国際機械への反映に取り組んでいる。
- IEC 61508 シリーズは機能安全の最上位に立つ規格であり、IEC 61508-1:2010 はその一つである。
- IEC 61508-1:2010、7.6.2.5 の中で、安全度水準（以下 SIL）の決定は、低頻度作動要求モードの運用に対しては、安全機能の作動要求における危険側故障の平均確率(PFD_{avg})によって規定すると記されている。
- 同様に、高頻度作動要求または連続モードの運用に対しては、安全機能の危険側故障の平均頻度(PFH)によって規定すると記されている。
- なお、PFH は危険側故障率で近似されるため、今回の発表では危険側故障率とする。
- 同規格の 7.6.2.7 では、SIL の決定にこの規格を使用する際、同時故障などの可能性が要求された安全度に関して十分低いように、多重防護系が独立していることが求められている。
- 多重防護系の独立性を保持できない場合は、同規格の PFD_{avg}、PFH による SIL の表を適用して SIL を決定すると、不適切な SIL が割り当てられる可能性がある。
- このような場合に適切な SIL の決定を可能にする方法として、「リスクメトリク」にもとづく包括的な SIL（H-SIL）決定のための尺度を提案する。
- メトリクとは、ある状態から事象が発生するまでの平均時間。
- リスクメトリクとは、リスクに関連する事象が発生するまでの平均時間。
- 危険事象率とは、危険事象に係るリスクメトリクの逆数であり、すなわち、初期状態から危険事象が発生するまでの平均時間の逆数。
- S-R System とは、電気・電子・プログラマブル電子安全関連系(E/E/PE 安全関連系)。表記が長いため本日の発表ではさらに略して S-R System とする。
- 防護層とは、複数の S-R System において、ある S-R System の不具合が他の安全関連系への作動要求になるシステム構成。
- IEC 61508-1:2010 の 7.6.2.8 には、多重防護系が独立していない場合は、各防護系間の共通原因故障を考慮した SIL を割り当てなければならないと規定されている。
- IEC 61508-1:2010 の A.5.5 によると、 許容リスクを達成するために複数の防護層を用いる場合、システム間及び、システムと作動要求の原因との間に相互関係がある場合がある。
- 同規格では、防護層が他の防護層や作動要求から独立していることが前提となっている。
- 同規格の運用者から、防護層が独立していない場合どうすればよいのかわからないという声が聞かれる。
- この防護層の独立性の必要性を認識していない人や認証機関が見受けられる。
- 独立していることが前提である理由は、S-R System の外部で発生する事象のメトリクが考慮されないためである。
- アイテム外で発生するメトリクの影響を受けない場合は使用できるが、アイテム外で発生するメトリクの影響を受ける場合は、その影響が反映されないので、SIL の割り当てが適切でない可能性が出て来る。
- 多重防護層を持つシステムは一般によく見られるが、独立性が保持できない場合がある。
- 防護層の独立性が保持できる場合、規格の作動要求率と危険側故障率の関係は、右上がりの単調増加となり、割り当てられる SIL が適切である。
- 今回の独立性が保持できていない場合の例では、作動要求と危険事象率の関係が先ほどの表とは全く異なるため、割り当てられる SIL が適切でない。
- S-R System への作動要求と S-R System の修復とが独立していない例として、密閉された、自分で室温調整することが困難な部屋を挙げる。
- 室温調整が困難な部屋で、室内が高温や低温になったときに空調システムが故障した場合に、熱中症や低体温症になるハザードが IEC 61508 で適切に算出されるか検証してみる。
- 非作動要求状態で故障した場合は、修復時間が作動要求の発生に影響される。

- 作動要求率が高いと故障が頻繁に検出され、作動要求の影響を受けない IEC 61508 のグラフの線とは全くちがったカーブになる。
- 作動要求が十分に低い領域においては、作動要求の頻度が危険側故障率の決定的要素になる。作動要求が上がると、単調増加で増えていく。
- 共通原因故障がある場合は、ない場合と比べてあまり下がらない。
- 独立性がない場合は作動要求率に従って単調増加ではなく、複雑なカーブを取る。
- この表が適用できない「複雑な安全関連系」には、作動要求率、共通原因故障など、包括的(holistic)な尺度が必要になる。
- 複雑な S-R System の H-SIL を決定する際、リスク軽減運用モードとリスク制御運用モードに分けて H-SIL を決定する。
- リスク軽減運用モードではリスク軽減比（Risk-Reduction Ratio）を用いる。
- H-SIL では、作動要求率に従って、危険側故障率、SIL の割り当てを行う。
- IEC 61508 は、Ed.3 が 2022 年 9 月 39 日に CD が発行され、今後は 2024 年 9 月に CDV の発行、2025 年 5 月に CDV2 または FDIS の発行が予定されている。
- 本日紹介した、複数の防護層間で共有部を有する場合や、独立性の考慮方法に関する実施例などは、日本が提案しており、IEC 61508-6 Ed.3 Annex B.4 として新設される見込み。

II. 質疑応答（抜粋）Q=質問、A=回答、C=コメント

- C1 国際規格の日本発の提案をするのは素晴らしいことだと思う。１つずつはなるほどと思ったが、設計する前の段階で SIL を決定することについては疑問がある。設計時にシステムの要求事項(SIL3, SIL4 が必要など)を決めるのが妥当ではないかと思った。計算したらこうなったというのではなく、設計時に必要な SIL を決めるべきだと思う。
- Q1 SIL の「割り当て」、SIL の「決定」という用語が使われているが、この２つに意味の違いがあるのか？
- A1 ある目的のために必要な SIL を割り当てる。実際に設計してみてこのシステムでは SIL いくつが達成できると決定する。ほとんどの場合「割り当て」と「決定」は同じ意味で使われている。
- C2 自動車の場合、たとえばエアバッグシステムが壊れた時の被害の程度を考慮して、ASIL（自動車安全水準） D が必要と決める。衝突した時に死亡しないためにさまざまなシステムで防護する。車のさまざまなシステムにそれぞれ ASIL を割り当てる。
- Q2 SIL を割り当てるとはどういう意味か？
- A2 機械安全だと ISO 13849-1 でパフォーマンスレベルを使う。どれくらいの安全性が必要であるか PLr(equired)を決め、実際に満たしている安全性の PL が割り当てられ、要求をみたしているかどうか確認する。
- C3 たとえば、大学のセキュリティシステムの場合、入館できなくするか、各室に入れないようにするかという選択肢がある。
- Q3 システムや部品にどの SIL を割り当てるかと言う意味か？
- C4 ステムを構成するエレメント（メーター、エアバッグなど）に SIL を割り当てる。部品は故障率を算出する。守らなければならない SIL は変わらないが、実現する手段は変わる。規格では機能に SIL を割り当てる。機能はたとえばエアバッグやメーターなどの具体的なシステムで実現する。
- Q4 規格の改訂案を日本から提案されると言う話があった。改訂への反映ということがだが、どのように行うのか？
- A4 佐藤先生が IEC 61508 のエキスパートであり、私（川島氏）も国内委員会のメンバー。佐藤先生は国際会議にも参加するので日本の意見を直接提案できる立場にある。
- Q5 規格に意見を出したい時はどうすればよいのか？
- A5 規格には国内審議団体があるので、団体のメンバーに相談するとよいと思う。
- Q6 今回の提案は、独立性を担保できない場合の提案だと思うが、独立性の定義と担保できていることをどのように確認できるのか？
- A6 独立性が担保できるのは、システム間に依存性がない、共通原因故障が十分少ないなどの場合。
- Q7 独立性が担保できるシステムは少ないのではないかと思うが、、、

- A7 実際そうだと思う。現状、独立性について規格に明確に定義されていない。
- Q8 IEC 61508 の話を久しぶりに聞かせていただき、これには関わらないで置こうと思った。ISO 13849-1 は社内で必須なので理解に役立つことがあればアドバイスいただきたい。
- A8 1980 年頃から比べると自動車事故の死亡者が各段に減っている。機能安全規格は完全ではないが規格に取り組んで、反映された結果でもあると思う。そういう意味では IEC 61508 は機械設計者にとって難しいが、ISO 13849-1 は IEC 61508 よりは導入しやすい規格だと思う。
- C5 自動車会社は ISO 26262 ができたおかげで説明の負担が減り楽になったので、関係者は喜んだ。
- C6 協働ロボットが柵なしで人と一緒に働けることになった後、トヨタ自動者の生産技術者と話したことがあるが、怖くて一緒に作業できないと言われた。今は実績ができたので、協働ロボットは増えてきた。

III 連絡事項

- 次回の定例会は 9 月 13 日（金）に日本大学で開催。講師は有人宇宙システムの野本氏を予定。

IV 審議事項

なし

以上