第 103 回 SNJ 定例会（オンライン形式）議事録

◎　件　名　　第 103 回 SNJ 定例会（オンライン形式）議事録
◎　日　時　　令和 3 年 6 月 4 日（金）15:00-17:05
◎　出席者　　30 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	
	高橋				
北陽電機				JR 東日本	川野
大同信号	寺田			大同信号	阿久根
	中野				石川
	吉富				
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	野本
					酒見
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	
ピルツジャパン	リジベル			ピルツジャパン	杉原
	太田				

I　講演「**レジリエンスエンジニアリングによる新しい冗長設計**」（野本）抜粋

- 深宇宙に行くには重力に逆らって推力を出す必要があり、大量の燃料が必要になる。
- 遠い星までロケットで飛ばすには、燃料をできるだけ軽くしなければならない。
- 深宇宙探査においても、高信頼化、開発コストの削減への要求は年々エスカレートし、推力倍、コスト半減が求められる。
- 安全性 1.5 倍から 2 倍、重さとコストの半減を目標に、この研究を始めた。
- 深宇宙の探査では、想定外の故障に耐える信頼性が必要。
- 2 故障に耐えるだけでは足りず、3 故障、4 故障起こっても耐えられることが必要。
- 従来の設計では、高信頼性に必要なのは、冗長数を増やすことだが、そうするとコストは跳ね上がる。
- これを解決するには、設計をドラスティックに変えなければならない。
- MIT のナンシー・レブソン教授によると、冗長設計はハードウェアのランダム故障には有効だが、現代的な設計ミスや、ソフトのバグなどには有効ではない。
- レブソン教授の著作“SAFEWARE”によると、冗長性はどんどん複雑化して、むしろ事故の原因になりやすい。
- NASA の新型インテリジェント航空機のフライトテスト結果では、冗長設計すればするほど、不具合の原因になりやすいことがわかった。
- 解決策として、安全化の方法にメスを入れ始め、安全のアーキテクチャそのものを変えてしまったら、トータルコストをものすごく下げて、安全性も上げられるかもしれないということに気づいた。
- レジリエンス・エンジニアリングに基づき、自然界の冗長設計をヒントにし、動物や植物の持つしなやかさや、人間のすばらしさに着目した。
- 自然界で実際に生物が何万年もかけて獲得してきた冗長設計を設計の参考にした。
- レジリエンスとは、復元力、回復力、弾力を意味し、困難な状況にもかかわらず、しなやかに適応して生き延びる力。
- 今まで安全性というのは、がっちりしているもの、不動のものというイメージだった。
- 対照的に、レジリエンスは、柔らかさやフレキシビリティ。
- 人間の場合は A 系がだめになったら B 系を使うという設計ではなく、すべてを常に使っている。
- 従来型の冗長設計の弱点は、常に半分以上が未使用資源であること。
- 有人機の場合、3 重系の設計になっており、2/3 は重り。これをなくせば軽くできるし、遠いところまで飛んでいける。
- 切り替えメカニズムがシステムを複雑にし、特にソフトウェア制御のバグの温床になる。
- 人間の右手と左手は違う機能に使用しているため、同じ理由で喪失しにくい。
- 人間の動作では、モードの切り替えはない（左足だけ、右足だけで歩くなど）。
- 人間の関節筋が複数の軸制御に関わっていることにヒントを得て、２つの機能を各軸に持たせ、縦横の合力で動かすアクチュエータを作ることができないか考えた。
- 縦横合力で動かすアクチュエータなら、重さが半分、信頼度が同じになり、どれが壊れても動き続けられる。
- ３つ、４つ、５つのアクチュエータの合力で作れば、さらに信頼性が上がり、重さもどんどん軽減できる。
- 人間の筋肉の例からもわかるように、自然界の冗長設計はオーバーラップしているため、いくつかの要素が損傷したとしても、機能し続けることができるため、強い。
- 新しい冗長設計では、バックアップをなくして、常にすべての機器を使う。

- 新しい冗長設計では、各系に異なる機能、異なるレイヤーを持たせ、冗長切り替えを排除した。
- 人間の足が斜めに生えていることをヒントに、各軸を斜めに、最適な角度で配置した。
- 新しいアーキテクチャでは、スラスタ数 25%減でミッション達成率 100%増となり、ミッション効率 150%増を達成可能となった。
- 新しいアーキテクチャでは、シミュレーションの結果、最悪の外乱の組み合わせに対しても、切り替えなしで、1 系のみの調整で十分対応できることがわかった。
- **遺伝的アルゴリズムを使って**スラスタ配置の**最適化**を行った結果、並進能力で 5 倍を達成し、回転能力も大きなマージンを確保したため、メインエンジンを根こそぎ削除可能となった。
- 新しい冗長設計は、持てる能力を最大限に使えるため、想定外の外乱に強い。
- 特定の系を隔離（オフ）して、永久故障への対応や温存も可能。
- 従来の考え方では、悪いところを見つけて切り替えることが目的だったが、レジリエンス・エンジニアリングでは、最適のパスを探すことが目的。
- レジリエンス設計により最適解を見つけた結果、ミッションと安全のトレードオフから脱却し、**安全になればなるほど、ミッション達成能力も上がる**結果となった。
- 従来の安全設計では、環境はばい菌と見なし、ばい菌の侵入を検知して、クリーンバックアップへの切り替えを行った。
- レジリエンスな安全設計では、環境はばい菌でなく友だちであり、デグレードしながら対応していくものと考える。
- 安全側も、ミッション側も、環境がクリーンでなくても飛び続けたいという同じゴールを目指しているため、レジリエンス設計により、両者のトレードオフの関係を排除できた。
- 従来の安全(Safety I)では、安全は重荷であったが、エリック・ホルナゲル教授の提唱する新しい安全(Safety II)では、安全はパワーであり、変化する環境に対応できる能力である。
- Q1.生物は冗長というより縮退設計ということになるのか？
- A1.その通り。人間の体も縮退になるものと腎臓のように冗長のものもあるように思う。
- Q2.心臓については冗長も縮退も持たせることができなかったのではないか？
- A2.心臓の場合、協調して合力で血を押し出すことは難しい。
- 参加者コメント 1: 冗長系を持たないということで、縮退の話があるが、フェイルセーフの考え方で優美劣化(graceful degradiation)というシステムがあり、100%のものが 80%になるような考え方があった。
- Q3.遺伝的アルゴリズムを使ったスラスター配置とは、どのように行ったのか？
- A3.動物の筋肉の配置を真似して斜めに配置した。0℃から 90℃までどれが最適なのかシミュレーションし、最適な角度を決定した。
- 野本氏コメント: JAXA で伝説になっている島秀雄先生の以下の言葉がある。「新幹線の素晴らしかったところは、新しいコンポーネントは実はない。従来のものを組み合わせることによって、何倍もの信頼性や利便性を達成したことが一番すごいところ。」この新設計では、姿勢制御クラスターを斜めにつけるだけで、同様の効果が出た。
- Q4:遺伝的アルゴリズムは、何を変数として設定しているのか？何を最適化の指標としているのか？
- A4.変数スラスターの位置と取り付け角度。最適化の関数は、最低でも現行の人工衛星の並進推力が出て、姿勢勢力がほぼ同等になること。結果、回転数も 2 倍、3 倍出た。A 系が全部使えなくなっても 2 倍くらいの推力が残った。最終的に 5 倍の並進推力が得られた。
- Q5.最終的にスラスターはどのような配置になったのか？
- A5.最終的に最適解として重心に近いところにきれいに配置されたが、微妙な角度が必要となった。

- 参加者コメント 2: 車の場合は使っていない部品はない。今日の発表を聴講し、車ではレジリエンスの設計が大昔から行われていることを確認できた。
- 参加者コメント 3: 以前担当していたシステムで、冗長設計を用いたことが禍いして(全系ダウンに至り)大きなトラブルを発生させた事がある。冗長設計はハード・ソフトともに複雑化するので、単独系の装置の信頼性を高める方が良い結果になるケースもあると思う。また、話題に出た生物のアナロジーの話であるが、鉄道でも使われている自立分散システムも生物のアナロジーから発想したものである。東京圏の輸送管理システム(ATOS:アトス)では、従来のように中央コンピュータですべての駅をコントロールするのを止め、各駅にダイヤ情報を配信し、駅では自立分散のコンピュータで自律的な制御を行っている（生物の細胞のように、脳からの指令が無くても、周囲環境に応じて自律的な動きをすることをヒントにしている)。これにより、トラブル発生時の影響を局所化したり、段階的なシステム構築が可能となった。
- 参加者コメント 4: 1980 年ごろにどうやったら安全なコンピュータ（高信頼性アーキテクチャ）ができるかという議論があった。今は仕様が与えられれば、誰でもモノを作ることができる。今後、単に製品の認証を取るというのではなく、最適な設計なのか、というところを議論しなければならないのではないかと思う。
- 参加者コメント 5: たくさんのエレメントを使用すれば、いくつかが壊れても他の部分で対応できる。たとえば、脳は一部が損傷しても他の部分で対応する。脳は過去の記憶から最適化し、他の機能にも対応するなど、オーバーライドの機能が備わっている。生命を維持するのに必要な部分は最後まで残る設計になっている。これは、レジリエンスの冗長設計に似ている。

Ⅱ　報告事項

・　次回定例会は、SNJ 創立 20 周年記念講演会と同時開催とし、10 月 8 日(金)に開催予定。新型コロナウイルスの感染状況によっては、オンラインで開催する。講師は調整中。

Ⅲ　審議事項

・　創立 20 周年記念講演会の開催形式、運営などについて、後日役員会で審議する。

以上