6章　安全基準

安全分野における汎用性のあるキーパラメータとして、標記の安全度水準（Safety Integrity Level、 SIL）を掲げ、向こう25年を目途として、その高度化を実現するメカニズムと可能性・限界について議論を行い、本分野の技術がいかに社会に貢献できるかを展望する。まず、安全度水準とは、その概念指標の基準を、システムにおける危険側故障を対象として、検出が可能でない故障の割合を問う、すなわち自己診断性能を問うものである。ここで、危険側とは概念的に安全側の補集合として位置づけられるところであり、安全か危険かわからない場合を含んでいる。

元来、ハードウェア故障の自己診断に対して考察が深められてきたリスク抑制の程度を指標化するための概念で、IEC-61508-1でSFF（Safety Failure Fraction）と定義されるものである[1]。より具体的には、ある回路系において、要素の故障が系にとって安全側かあるいは危険側でもこれを検出できる場合を取り上げ、各要素の故障の組み合わせ集合の中で、その割合がどれほど高いかを指標とするのである[1]。

しかし、その後ソフトウェア機能安全に対しても、上記の概念を反映させるべく、ソフトウェア手法・解析手法の中で、推奨される技術の選定・分類が進んでいる。すなわち、ソフトウェアにおいては、あらかじめ定義される状態空間の中で、コマンドの進行によりどのように状態遷移が展開されるか、不安全な状態に陥らないか、あるいは未定義の状態に陥ることはないか、という観点での妥当性がそれぞれの機能を果たすために設けられた仕様のレベルにおいて検証されるのである。

今後は、その高度化の目標として、ハードウェアにおける性能の向上、およびソフトウェア分野の機能高度化の両面が図られていくと考えられる。まず、ハードウェアにおける安全度水準の向上については、ＦＰＧＡ等による、自己修復や故障回避といった安全機構の容易なハードウェア設計・搭載が可能となり、これに伴って、ともすればコストの増大を連想しがちな安全ハードウェア技術が実装されて行くにちがいない。情報量の観点でも、現状は、セイフティーＰＬＣのような接点情報の安全処理をターゲットとするものが主流であるが、TTP/C 等が航空安全分野から産業機械安全へと進出してくることが予想され、今後は、これらの安全技術が高速化、処理情報の大容量化にも寄与するものと予想される。

他方、ソフトウェア技術では、コンテンツに関する安全度水準の高度化が問われるようになるであろう。具体的な一例をあげると、３Ｄの視覚センサによる環境情報の取得によって、環境地図を作成する場合を考えると、これが安全で信頼できるものなのかどうかがいかに保証されるかという問題がある。あるいは、ナビゲーション医療の分野にも同様の深刻な問題が存在する。この点については、安全な地点をいかに安定に検出し続けるか、

[1]系統故障に関する指標SFFと対をなす指標として、ランダム故障に関する指標PDF（Probability of Failure on Demand）がある。

また、モデル化手法やモデルマッチング技術が精度や確度の観点で妥当であるかどうかが、安全目的で検証されるように、技術革新のベクトルが変化して行かなければならない。

このほかにも、非定常で不確定性の高い外界との相互作用が強まるにつれて、システムが、いかに目標使用に対して妥当な出力を供給し続けるかという問題から、アクティブな環境センシングの必要性や、適応的あるいは学習により制御系の安定性、安全性を保証する制御系設計の必要性が問われるようになる。たとえば、ロボット側の動的なパラメータが精緻に同定できても、その触れる対象である人間の身体部位等、外界のパラメータは不確定で変動しやすい。これらの欠点を補って、いかに確保するかという問題は、確率制御の本領であり、この分野からの今後の多大な貢献が期待される。

さて、今後の技術的限界についてであるが、安全な計測技術については、３次元情報の取得が高速に行われるようになっても、一般物体を含む自然環境のモデリング技術がリアルタイム処理に届かず、これがいつの時代にも技術限界を与えるものと予想される。しかし、後に述べるように、環境の構造化を進めたり、あるいは集合知技術の導入が進めたりするなど、ブレークスルーもないわけではない。

安全な制御技術については、適応制御等がパラメータの推定に時間がかかることが物理的な限界を与える。これは、人間との接触においては、範囲がある程度予測可能であるので、限界はないが、人間の動作範囲が関わる場合には、個人差や疲労度等、不確定さ、変動要素が大となり、問題の対処は困難を増すことになる。

安全技術のセル生産応用

セル生産システムは、組立部品点数が制限される、あるいは大型部品が含まれる場合に、セルを構成しにくい場合がある、といった問題があり、生産の対象に応じて取捨選択二分される生産体系であろう。その中で、コストや秘匿性の観点で部品のモジュール化が進む電子部品の組立て現場では歓迎される生産形態となっている。典型的にたとえば、情報家電等電子部品の組立製造現場は、現状では、労働集約化傾向にあるが、技術ロードマップでは、今後、人間とロボットの分担セル生産形態を経て、完全無人化セル生産システムへと進化すると予想されている[2]。すでに、人間と共存するセル生産の形態は、人間支援あるいは省人化目的で現実に提案されており、安全技術の鋭意導入により、今後しばらくは、分担セル生産指向が強まるものと予想される。ここで、安全技術は、人間とロボットの距離を隔離から隣接へと縮める効果をもつと同時に、時間的な作業効率も向上できる点で重要な位置づけとなる。

ただし、現実的には、生産効率をアップさせるために、安全上必要最低限に抑えたい仕様以上のパワーがロボットに求められる、あるいは、ロボット本体をいくら柔軟な被覆で覆っても、把持する部品が鋭利なものとなることが不可避である、等の理由から、本質安

全化設計技術には現実的なソリューションとして限界がある。したがって、SILに代表される機能安全に依存する技術が、否応なく主流となるであろう。

先の議論に照らせば、生産現場においては、環境の構造化が可能で、対象の人間も健常者であることから、ハードウェア、ソフトウェアの技術限界的限界は考えにくいが、ヒューマンエラーに起因する保守作業等の非定常作業時の重篤な事故の回避をいかに達成するかが問われるようになる。この点で、STAMPやグラフィックシミュレータ技術等の新しいリスク分析技術の展開が期待される。また、人間との共存を許すロボットが導入されるセル生産現場にも、ロボットによる部品の搬送や供給を目的とした移動機構の導入が、今後は鋭意進められるであろう。この分野における安全観点の技術では、ＰＬ対策技術として、産業機械やロボットコントローラへの安全ドライブシステムの導入がまず進められる。並行して、より深刻なヒューマンエラー対策も進められるであろう。具体的には、この分野が構造化された環境を前提としていることから、レーザーレンジセンサや安全ビジョンによる人間検出等、安価でSILの保証された技術の普及・発展がみこまれるほか、やがて、段差有走行環境の安全な移動機構の導入・普及が、よりフレキシビリティの高い製造環境での人間共存化機械の進展を促すことになろう。

[1] たとえば, IEC 61508-1(1998), Functional safety of electrical/ electronic/ programmable electronic safety-related systems; Part 1: General requirements
[2] http://www.nedo.go.jp/roadmap/2008/sys1.pdf, ロボット分野の導入シナリオ